RENATO BOBSIN MACHADO

MÉTODO COMPUTACIONAL PARA ACOMPANHAMENTO E INTERAÇÃO REMOTA EM TEMPO REAL PARA VIDEOCOLONOSCOPIA

Campinas
2013

UNICAMP

UNIVERSIDADE ESTADUAL DE CAMPINAS
Faculdade de Ciências Médicas

RENATO BOBSIN MACHADO

MÉTODO COMPUTACIONAL PARA ACOMPANHAMENTO E INTERAÇÃO REMOTA EM TEMPO REAL PARA VIDEOCOLONOSCOPIA

Orientador: Prof. Dr. Wu Feng Chung

Co-Orientadora: Profa. Dra. Huei Diana Lee

Tese de Doutorado apresentada à Pós-Graduação em Ciências da Cirurgia da Faculdade de Ciências Médicas da Universidade Estadual de Campinas – UNICAMP para a obtenção do Título de Doutor em Ciências.

ESTE EXEMPLAR CORRESPONDE À VERSÃO FINAL DA DISSERTAÇÃO/TESE DEFENDIDA PELO ALUNO **RENATO BOBSIN MACHADO** E ORIENTADO PELO **PROF. DR. WU FENG CHUNG**.

Assinatura do Orientador

Campinas
2013

Ficha catalográfica
Universidade Estadual de Campinas
Biblioteca da Faculdade de Ciências Médicas
Maristella Soares dos Santos - CRB 8/8402

M18m

Machado, Renato Bobsin, 1976-
Método computacional para acompanhamento e interação remota em tempo real para videocolonoscopia / Renato Bobsin Machado. -- Campinas, SP : [s.n.], 2013.

Orientador : Wu Feng Chung.
Coorientador : Huei Diana Lee.
Tese (Doutorado) - Universidade Estadual de Campinas, Faculdade de Ciências Médicas.

1. Colonoscopia. 2. Telemedicina. 3. Acompanhamento de procedimentos médicos em tempo real. 4. Proteção de dados médicos. 5. Acompanhamento remoto de procedimentos médicos. I. Wu, Feng Chung. II. Lee, Huei Diana. III. Universidade Estadual de Campinas. Faculdade de Ciências Médicas. IV. Título.

Informações para Biblioteca Digital

Título em outro idioma: Computational method for remote monitoring and interaction in real time for videocolonoscopic procedures
Palavras-chave em inglês:
Colonoscopy
Telemedicine
Monitoring of medical procedures in real time
Security of medical data
Remote monitoring of medical procedures
Área de concentração: Fisiopatologia Cirúrgica
Titulação: Doutor em Ciências
Banca examinadora:
Wu Feng Chung [Orientador]
Ilka de Fátima Santana Ferreira Boin
Orlando Petrucci Junior
Fabiano Silva
Marcos Sfair Sunye
Data de defesa: 02-10-2013
Programa de Pós-Graduação: Ciências da Cirurgia

BANCA EXAMINADORA DA DEFESA DE DOUTORADO

RENATO BOBSIN MACHADO

Orientador PROF. DR. WU FENG CHUNG

MEMBROS:

1. **PROF. DR. WU FENG CHUNG** _____
2. **PROFA. DRA. ILKA DE FÁTIMA SANTANA FERREIRA BOIN** _____
3. **PROF. DR. ORLANDO PETRUCCI JUNIOR** _____
4. **PROF.DR. FABIANO SILVA** _____
5. **PROF.DR. MARCOS SFAIR SUNYE** _____

Programa de Pós-Graduação em Ciências da Cirurgia da Faculdade de Ciências Médicas da Universidade Estadual de Campinas

Data: 02 de outubro de 2013

DEDICATÓRIA

Aos meus grandes amigos e orientadores,

Wu Feng Chung e Huei Diana Lee.

Aos meus pais,

Martim Menger Machado e Cely Bobsin Machado.

As minhas avós,

Magdalena Brehm Bobsin (in memorian) e Mercedes Menger Machado (in memorian).

AGRADECIMENTO ESPECIAL

A duas pessoas muito especiais às quais a vida me brindou em conhecer: Wu Feng Chung e Huei Diana Lee.

Professor Doutor Wu Feng Chung, educador no sentido mais completo da palavra, idealista que com sua motivação inabalável e de integridade inquestionável vem contribuindo de fato para a construção de um mundo melhor, fazendo brotar em todas as pessoas o que elas possuem de melhor.

Professora Doutora Huei Diana Lee, a qual tive a honra de conhecer ainda na graduação, posteriormente trabalhando conjuntamente no Laboratório de Bioinformática e que tive o prazer de ter como orientadora nesse trabalho de doutoramento. Pessoa íntegra, competente, exemplo de conduta ética e perseverança.

A estas pessoas extraordinárias minha eterna gratidão, orgulho, admiração e amizade.

AGRADECIMENTOS

Ao Prof. Dr. Cláudio Saddy Rodrigues Coy que sempre apoio e incentivou os trabalhos em parceria entre o Laboratório de Bioinformática da UNIOESTE (LABI) e o Serviço de Coloproctologia da Faculdade de Ciências Médicas da UNICAMP.

Ao Prof. Dr. João José Fagundes, exemplo como educador e como ser humano, pessoa completa em conhecimentos técnicos, universais e em princípios.

Ao Prof. Dr. Juvenal Ricardo Navarro Góes (*in memorian*), pelo auxílio e incentivo em todos os momentos. Os seus ensinamentos são transcendentais.

Ao Prof. Dr. Joaquim Murray Bustorff da Silva que acreditou e apoiou a realização deste trabalho de tese.

À Profa. Dra. Ilka de Fátima Santana Ferreira Boin por acreditar e apoiar este trabalho e as demais linhas de pesquisa desenvolvidas entre o LABI e a UNICAMP.

À Profa. Dra. Raquel Franco Leal pelas experiências compartilhadas, pela paciência e pelos grandes ensinamentos no acompanhamento de exames de videocolonoscopia e de cirurgias.

À Dra Maria de Lourdes Setsuko Ayrizono, pelo auxílio e experiências compartilhadas.

À Ana Cristina de Moraes e Willian Adalberto Silva, amigos especiais, pessoas íntegras e grandes exemplos como profissionais e como pessoas.

Ao Prof. Joylan Nunes Maciel pelo trabalho conjunto. Profissional extremamente dedicado e motivado.

AGRADECIMENTOS

Aos grandes amigos Prof. Dr. Fabiano Silva e Profa. Dra. Letícia Mara Peres, os quais foram meus professores na graduação e desde então me incentivaram a trilhar o lindo caminho da qualificação.

Ao Prof. Dr. João Bosco Mangueira Sobral, agradeço pelos ensinamentos, incentivo, integridade, ética e apoio incondicional em todos os momentos de minha vida.

Aos amigos João Ricardo Camargo e Carlos Alberto Knakiewicz (Knaka) por acreditarem na importância da qualificação e por incentivarem a realização deste trabalho de tese.

Ao Prof. Dr. Gustavo Batista do Instituto de Ciências Matemáticas e de Computação da Universidade de São Paulo no campus de São Carlos (ICMC/USP) e ao Prof. Dr. Fabiano Silva da Universidade Federal do Paraná (UFPR) pelo grande apoio e auxílio durante a realização de experimentos.

Ao Centro de Computação Científica e Software Livre (C3SL) do Departamento de Informática da UFPR e ao Laboratório de Inteligência Computacional do ICMC/USP (LABIC) pelo auxílio na execução dos experimentos.

Ao Programa de Pós-graduação em Engenharia de Sistemas Dinâmicos e Energéticos da UNIOESTE (PGESDE) pelo empréstimo de computadores para a avaliação da precisão do método proposto neste trabalho.

À Agência de Inovação da UNICAMP (INOVA), especialmente à Patrícia Franco Leal Gestic, Gabriel Gustavo Guion e Ciro De La Cerda pelo grande apoio na identificação e na confecção de patentes de invenção e de registros de *software*.

AGRADECIMENTOS

Aos profissionais e amigos da Gastrocentro da UNICAMP que me auxiliaram de modo prestativo e sempre com alegria e motivação, em especial: Adilson Cattaneo, Carlos Fernando Papotti, Carolina Nunes Barboza, Luciano Ferretti, Marcelo da Silva Primo, Rosângela Ângelo Vaznella e Stela Cristina Tonini.

À Paula Léia e Renata Machado pela prestatividade e eficiência no tratamento dos assuntos da Pós, e pela amizade.

À Faculdade de Ciências Médicas da UNICAMP que me aceitou no Programa de Pós-Graduação em Ciências da Cirurgia.

As instituições que me apoiaram nesse período: UNIOESTE, UNICAMP e Itaipu Binacional.

À minha namorada Edriana Silva pelo apoio e incentivo em todos os momentos.

Aos professores, pesquisadores e estagiários da família LABI, cuja convivência permitiu o compartilhamento de experiências, conhecimentos universais e, sobretudo princípios.

Aos meus familiares, em especial aos meus pais Martim Menger Machado e Cely Bobsin Machado que não mediram esforços para me dar uma formação sólida.

E a todos que de alguma forma colaboraram para a concretização deste trabalho.

RESUMO

A área computacional aplicada à medicina tem contribuído para aumentar a eficiência no armazenamento, na transmissão e na análise de dados referentes aos pacientes e, consequentemente, na precisão do diagnóstico. Nesse contexto, para ampliar ainda mais estas ações, tornam-se essenciais a formação e a consolidação de redes integradas e colaborativas de apoio à área médica à distância. Outro aspecto fundamental que deve ser considerado no trato de informações pertencentes aos pacientes e profissionais médicos é a segurança, contemplando critérios como integridade, confidencialidade e autenticidade dessas informações.

Neste trabalho, desenvolveu-se um método original em telemedicina para o acompanhamento e a interação remota entre especialistas da área médica, em tempo real, durante a realização de exames videocolonoscópicos. Para a proteção de dados e para a transmissão segura e eficiente das informações referentes aos pacientes e aos exames, propôs-se um método de segurança específico. Esses métodos foram implementados em um sistema computacional aplicando tecnologia *Web* e ferramentas *open source*.

Para aferir o desempenho desse sistema, avaliou-se a taxa Quadros por Segundo (QPS) durante a transmissão de vídeos sem compactação. Este processo se deu em dois ambientes distintos, com diferentes resoluções, sendo o primeiro caracterizado apenas pela rede local e, o segundo, pela rede local juntamente com a Internet, simulando ambientes reais de aplicação do método proposto.

As análises dos resultados desse trabalho permitiram concluir que:

1. O método proposto, implementado no sistema computacional, cumpre os requisitos estabelecidos para transmissão de dados, segurança de informações e interação em tempo real entre os usuários;

2. O método proposto é aplicável para a realização de procedimentos videocolonoscópicos, em redes locais e na Internet.

3. O método de segurança definido neste trabalho prove privacidade para a transmissão de dados, de vídeos e de imagens, assim como para a interação entre os participantes locais e remotos.

ABSTRACT

Computational methods and tools applied to medicine have contributed to increase efficiency in storage, transmission and analysis of data related to patients and, consequently, the accuracy of diagnoses. In this context, to further expand these actions, it became essential the creation and consolidation of integrated and collaborative networks to support the medical area. Another fundamental aspect which must be considered in dealing with information about patients and medical professionals is security, considering criteria such as integrity, confidentiality and authenticity of this information.

In this work, we have developed an original telemedicine method for monitoring and remotely interaction among medical experts, in real time, during the performance of video-colonoscopic procedures. For data protection, secure transmission and efficient use of information related to patients and their examinations, we have proposed a specific security method. Both methods were implemented in a computing system by applying Web technology and open source tools.

In order to assess the performance of this system, we have evaluated the transmission rate in frames per second (FPS) during the streaming of an uncompressed video. We performed our experiments simulating real environments in two different scenarios with distinct resolutions, one being characterized only by the local network and the second considering the local network and the Internet.

The analysis of the results has shown that: (1) the proposed method, implemented in the computational system, meets the requirements for data transmission, information security and real-time interaction among the users; (2) the proposed method is applicable for performing video-colonoscopic procedures, via local networks and the Internet, and; (3) the security method built for this system provides privacy during the transmission of the data, video and images, as well as the interaction between the local and remote participants.

SUMÁRIO

LISTA DE ABREVIATURAS

3D	Três Dimensões
ACR	*American College of Radiology*
ADSL	*Asymmetric Digital Subscriber Line*
AES	*Advanced Encryption Standard*
ANSI	*American National Standards Institute*
ARPA	*Advanced Research Projects Agency*
ARPANET	*Advanced Research Projects Agency Network*
ATA	*American Telemedicine Association*
BD	Base de Dados
BIV	Base de Imagens e Vídeos
C3SL	Centro de Computação Científica e *Software* Livre
CECE	Centro de Engenharias e Ciências Exatas
CG	Central de Gerenciamento
CPF	Cadastro de Pessoas Físicas
CPU	Unidade Central de Processamento
CRM	Conselho Regional de Medicina
DES	*Data Encryption Standard*

DICOM	*Digital Imaging and Communications in Medicine*
DP	Desvio-Padrão
EH	Equipamento Hospitalar
ENIAC	*Electronic Numerical Integrator And Computer*
FDDI	*Fiber Distributed Data Interface*
HD	*Hight Definition*
HIS	*Hospital Information System*
IP	*Internet Protocol*
Km	Quilômetro
LABI	Laboratório de Bioinformática
LABIC	Laboratório de Inteligência Computacional
LAN	*Local Area Networks*
MER	Modelo Entidade Relacionamento
MS	Módulo de Segurança
MSE	Módulo de Segurança Externa
MSI	Módulo de Segurança Interna
MUMPS	*Multi-Programming System*
MVC	*Model-View-Controller*
NEMA	*National Electrical Manufacturers Association*
NIST	*National Institute of Standards and Technology*
PACS	*Picture Archiving and Communication Systems*
PC	*Personal Computers*
QPS	Quadros por Segundo

RES	Registros Eletrônicos de Saúde
RG	Registro Geral
RIS	*Radiology Information System*
RNP	Rede Nacional de Ensino e Pesquisa
RSA	*Rivest, Shamir, Adleman*
SA	Servidor de Aplicações
SGBD	Sistema de Gerenciamento de Banco de Dados
SHA-1	*Secure Hash Algorithm 1*
SPE	Sala de Procedimentos Endoscópicos
SSL	*Secure Socket Layer*
S2TR	Sistema de Telemedicina em Tempo Real
SUS	Sistema Único de Saúde
TCP	*Transmission Control Protocol*
TCP/IP	*Transmission Control Protocol/Internet Protocol*
TLS	*Transport Layer Security*
TRS	*Tip-Ring-Sleeve*
UAIR	Unidade de Acompanhamento e de Interação Remota
UDP	*User Datagram Protocol*
UEL	Unidade de Execução Local
UEM	Universidade Estadual de Maringá
UFAM	Universidade Federal do Amazonas
UFMG	Universidade Federal de Minas Gerais
UFPA	Universidade Federal do Pará

UFPR	Universidade Federal do Paraná
UFRGS	Universidade Federal do Rio Grande do Sul
UFSC	Universidade Federal de Santa Catarina
UNIMED	Sistema Cooperativo de Serviço Médico
UNB	Universidade de Brasilia
UNICAMP	Universidade Estadual de Campinas
UNIOESTE	Universidade Estadual do Oeste do Paraná
USB	*Universal Serial Bus*
USP	Universidade de São Paulo
WIFI	*Wirelles Fidelity*
WWW	*World Wide Web*

LISTA DE TABELAS

LISTA DE FIGURAS

1. INTRODUÇÃO

1.1. CONSIDERAÇÕES GERAIS

As aplicações na área de telemedicina iniciaram-se no Brasil com maior ênfase a partir da década de 90, todavia, o desenvolvimento dessas ações continua de modo bastante tímido.

O Brasil é um país com dimensão continental e decorrente ao fato, a formação e a consolidação de redes integradas e colaborativas de apoio à área médica à distância se torna essencial. Sob esse escopo, benefícios poderão ser alcançados como redução dos custos com transportes e comunicações, disseminação da medicina especializada para regiões remotas do país e possibilidade de aumento de inter-relações e compartilhamento de conhecimento entre pesquisadores e especialistas de instituições de ensino superior e de pesquisa.

Para isso, existem diversos recursos tecnológicos que podem ser aplicados com a finalidade de efetuar as ações da telemedicina como transferência de imagens, áudio e vídeo e, sem dúvida, uma das mais consistentes é a aplicação da arquitetura Internet associada com técnicas de gerenciamento de sessões multimídia e criptográficas. Por meio desse modelo, é possível a transmissão de dados em tempo real e a interação dos pesquisadores por intermédio de comunicação por vídeo, voz e por mensagens de texto (1-4).

Embora a Internet não tenha sido projetada para a transmissão de dados de aplicações em tempo real, o aumento da capacidade de processamento computacional e a expansão da largura de banda possibilitaram o desenvolvimento de processos com recursos multimídia contendo qualidade suficiente para iniciar aplicações para a área médica. Vale ressaltar que essas abordagens geram e consomem fluxos de dados, tal como vídeo e áudio, em tempo real (5-7). Assim sendo, o desenvolvimento de soluções relacionadas a este tema deve observar requisitos fundamentais como a qualidade, a latência e as taxas de transmissão de áudio e vídeo (8-10).

Outro aspecto fundamental que deve ser considerado durante a realização de trabalhos com dados médicos é a segurança dos dados. Desse modo, critérios como integridade, confidencialidade e autenticidade dessas informações devem ser abordados

com relevância máxima (11-13). Dentro dessa linha, diversos modelos vêm sendo propostos e desenvolvidos para alcançar o quesito segurança, no entanto, todos são passíveis de críticas e é necessário o desenvolvimento de métodos que atendam as especificidades das aplicações, sem comprometer o desempenho das mesmas (14-16).

É importante notar que processos tecnológicos originais e inovadores, frequentemente, estão diretamente relacionados com altos custos operacionais, desde o desenvolvimento, a disponibilização e a manutenção do sistema computacional. Em contrapartida, atualmente, pode-se optar por ferramentas computacionais modelo *open source*[1], com o qual acredita-se ser possível alcançar atributos como redução de custos e de customização, além de proporcionar instrumentos computacionais para o desenvolvimento, com qualidade, de processos de segurança (17-19).

A partir da identificação dos requisitos desejáveis, das alternativas tecnológicas e das contribuições que podem ser alcançadas para a área médica, construiu-se, neste trabalho, um sistema em telemedicina para o acompanhamento remoto, em tempo real, de procedimentos médicos por meio da Internet e um método de proteção de dados para a transmissão segura e eficiente das informações referentes aos pacientes e aos médicos por meio de vídeos e de imagens.

Esses métodos foram implementados e aplicados à área de videocolonoscopia, cuja finalidade é promover a discussão antes, durante e após a realização do exame endoscópico utilizando-se de distintas mídias representadas pelo vídeo, pelo áudio, pelo texto e pelas imagens.

As vantagens, dos métodos desenvolvidos neste trabalho, sobre os principais recursos tecnológicos já disponíveis em telemedicina são a construção de bases de dados estruturadas de exames provenientes dos exames endoscópicos, facilitando assim, no processo de análise, de extração de conhecimento e de desenvolvimento de novos modelos de detecção de padrões por meio de Inteligência Artificial. Além disso, estes métodos computacionais desenvolvidos poderão ser aplicados a outros problemas similares e equipamentos médicos, como aparelhos endoscópicos usados para diversos diagnósticos em

[1] Neste trabalho o termo *open source* é caracterizado por plataforma de código aberto e de livre utilização.

outras regiões anatômicas, cirurgias videolaparoscópicas, ultrassonografias, tomografia axial computadorizada, ressonância magnética nuclear, entre outros.

Para auxiliar na melhor compreensão da evolução histórica e da importância de aplicações computacionais para a área médica, nas próximas seções serão abordadas as técnicas e os trabalhos relacionados com as áreas de telemedicina e de métodos de segurança da informação.

1.2. EVOLUÇÃO COMPUTACIONAL E APLICAÇÕES NA ÁREA MÉDICA

O ábaco, aparelho utilizado para efetuar operações aritméticas é considerado o primeiro computador da humanidade (20), mas, apesar de ter surgido aproximadamente a 3000 a.C., a primeira aplicação computacional para a medicina ocorreu somente entre 1920 e 1930, com o desenvolvimento de um sistema de processamento de dados proposto por Herman Hollerith (21). Essa máquina de tabulação consistia na adaptação de cartões perfurados para o processamento de pesquisas relacionadas à saúde, principalmente na área de epidemiologia. No entanto, a real expansão computacional se deu a partir dos anos 40 do século XX com a construção do primeiro computador digital (22).

O período entre 1940 e 1960 foi marcado pelo desenvolvimento de computadores baseados na tecnologia de válvulas. No ano de 1946 foi construído o primeiro computador eletrônico de propósito geral, denominado *Electronic Numerical Integrator And Computer* (ENIAC) (23). Posteriormente, diversas máquinas foram desenvolvidas, merecendo destaque o IBM 650 que foi o primeiro computador produzido e comercializado em larga escala (24).

No ano 1960, Schmeck (25) publicou um trabalho no *New York Times* relatando o armazenamento de registros médicos em fitas ou em outros dispositivos de armazenamento, a partir da digitalização dos mesmos. Na época, aplicou-se o computador IBM 650 para essa finalidade.

Plumb (26), em 1962, utilizou recursos computacionais para a transmissão de impulsos elétricos obtidos por meio de exames cardíacos propagados através de linhas telefônicas. Esses dados eram enviados para um computador central, o qual era responsável pela geração de gráficos para auxiliar na análise das informações.

No ano 1970, Greenes et al. (27) criaram uma linguagem de programação específica para aplicações médicas denominada *Multi-Programming System* (MUMPS). Esta linguagem foi amplamente usada, no entanto, decorrente à arquitetura dos computadores da época, a MUMPS precisava ser reescrita para cada nova geração de computadores.

Collen (28), no ano 1972, foi pioneiro na utilização de sistemas computacionais hospitalares para armazenamento e apresentação de resultados de testes laboratoriais, contribuindo positivamente na melhora da eficiência do gerenciamento e da ordenação dos dados.

A partir do ano 1975, iniciou-se a história dos computadores pessoais com a introdução dos microcomputadores. Essa nova abordagem rompeu com o paradigma até então vigente de computadores centralizados denominados *mainframes*, e deu início ao processo de redução dos tamanhos e ao aumento da capacidade de processamento e armazenamento. O primeiro microcomputador de uso pessoal foi denominado Altair 8800 (29).

Neste mesmo período a área de comunicação de dados teve um importante avanço com a implementação da primeira rede local, em 1976. Essa rede recebeu o nome de Ethernet e permitia a interconexão entre equipamentos, baseado em pacotes, com capacidade de transmissão de 3 Mbps (30). Esta ferramenta passou por diversas melhorias e, atualmente, representa a configuração de rede mais utilizada no mundo, alcançando abrangência de 85 % do mercado no setor de redes locais (1, 31).

Essas inovações da área computacional e de comunicação subsidiaram a expansão de aplicações da informática na área médica, tais como a disseminação de microcomputadores para hospitais e clínicas e o estímulo ao desenvolvimento de *softwares* para a área da saúde (32).

Como exemplos desse fato, Greenes (33) desenvolveu em 1982 um sistema computacional para mensurar, calcular e gerar relatórios relativos a exames de ultrassom obstétrico. Nessa década de 90 destaca-se também pela evolução de aplicações direcionadas ao armazenamento e ao gerenciamento de imagens médicas, denominados *Picture Archiving and Communication System* (PACS). Templeton et al. (34) desenvolveram um protótipo de um sistema PACS para a área de radiologia. De modo complementar, Areson

et al. (35) construíram um PACS, por meio de redes locais, para o controle de bases de imagens da área médica, agregando as características de recuperação e de visualização das mesmas por parte dos usuários do sistema.

Nos anos 90, a área tecnológica foi marcada pela expansão das redes de computadores. O fundamento para esse fato foi à popularização da *Advanced Research Projects Agency Network* (ARPANET) que havia sido concebida na década de 70 para fins exclusivos do Departamento de Defesa dos Estados Unidos da América. Esse contexto estimulou a definição e a construção de redes de pesquisa em diversos países e passou por adaptações dando origem à rede mundial Internet (36).

Em 1991, Berners-Lee e Cailliau (37) propuseram um modelo de gerenciamento de informações e associação de documentos em hipermídia e, a partir de então, a Internet passou a ser utilizada também para serviço de disponibilização de páginas e de aplicações passando a ser denominado *World Wide Web*[2] (WWW) (38). Sob esse cenário, cabe dizer que a expansão de trabalhos computacionais para a área médica ganhou ênfase a partir dos anos 90, estimulado por esse novo cenário tecnológico (39).

Em 1996, Abate et al. (40) definiram um sistema computacional que empregava ferramentas distribuídas por meio da *Web* com finalidade de captura, de armazenamento e de processamento de imagens médicas. O sistema permitia também que os médicos identificassem anormalidades nas imagens por meio de diferenças de formas e medidas geométricas.

Em 2003, Duarte et al. (41) propuseram um sistema computacional de videoconferência para facilitar a emissão de laudos e de diagnósticos de doenças por meio da Internet. A solução proporcionava a análise de exames por diversos médicos em locais distintos, de modo colaborativo.

Argenziano et al (42), em 2006, desenvolveram uma técnica aplicando robótica para a realização de procedimentos cirúrgicos, tal como o reparo da valva mitral e de defeitos relacionados ao septo cardíaco. Este feito foi fundamental para o estabelecimento de uso de conceitos de robô na medicina.

[2] Ao longo do texto o serviço *World Wide Web* será expresso por meio do termo *Web*.

No ano de 2009, Mougiakakou et al. (43) desenvolveram um sistema computacional para o arquivamento e o gerenciamento de imagens de tomografia axial, contemplando mecanismos de suporte ao diagnóstico. Este *software* baseou-se no padrão *Digital Imaging and Communications in Medicine* (DICOM) e apresentava algoritmos de pré-processamento semi-automático para segmentação das imagens e diagnóstico apoiado por computador.

Ford et al. (44), em 2012, construíram um sistema computacional para auxiliar os médicos na interpretação de exames de ultrassom em 3D. O sistema também proporcionava a transmissão dessas imagens pela Internet.

Desse modo, as inovações tecnológicas das últimas duas décadas, e em especial o crescimento acelerado da capacidade de processamento e de armazenamento, a disseminação da Internet e a construção de redes locais com alta velocidade, são fundamentais para a construção de aplicativos com recursos multimídia. Na próxima seção serão abordados trabalhos que utilizam os recursos anteriormente citados para o desenvolvimento da telemedicina.

1.3. TELEMEDICINA

A telemedicina constitui uma das principais e mais promissoras classes de aplicações computacionais direcionadas à área médica (3, 4, 32, 45), e uma das definições mais aceitas é a da *American Telemedicine Association* (ATA) na qual caracteriza a telemedicina como a troca de informações médicas entre lugares distintos por meio da comunicação eletrônica a fim de melhorar o estado de saúde do paciente (46, 47).

A história da telemedicina teve início em meados do século XIX, todavia, o trabalho considerado pioneiro na área foi publicado no ano 1906, cujo tema abordado era transmissão de dados de eletrocardiogramas utilizando-se de linhas telefônicas (48, 49).

No ano de 1924, Costa (50) definiu um código postal criado para a solicitação de medicamentos por telégrafo, sendo que cada palavra do código era composta por cinco letras, permitindo assim, a solicitação de um medicamento específico e a respectiva quantidade.

Gershon-Cohen e Cooley (51) desenvolveram, em 1950, um trabalho pioneiro para transmitir os resultados de exames de Radiologia por fios de rádio ou telefônicos à distância. O trabalho contribuiu para que o diagnóstico fosse realizado por radiologistas experientes de outros centros. O método foi aplicado em distâncias de aproximadamente 45 Km.

A utilização das telecomunicações na medicina iniciou com a primeira ligação de vídeo interativo, a qual foi estabelecida em 1964, nos EUA, entre o *Nebraska Psychiatric Institute* e o *Norfolk State Hospital*, com aproximadamente 180 quilômetros de distância entre as instituições (52).

Nesse mesmo escopo, em 1973, Benschoter et al, (53) propuseram a utilização do processo televisivo para facilitar a realização de consultas, possibilitando a discussão entre especialistas da área de psiquiatria e clínicos gerais. Este método foi desenvolvido por meio de circuitos fechados bidirecionais de transmissão televisiva durante tratamentos psiquiátricos.

Embora tenham sido propostos distintos métodos inovadores, tais ocorrências se deram de modo isolado, e somente a partir da década de 90 é que o desenvolvimento e a expansão se tornaram efetivas e amplamente difundidas. Este fato se sucedeu devido ao rápido avanço das tecnologias de informação e de telecomunicação, ou seja, a instalação definitiva da rede Internet (5).

Nesse contexto, o crescimento e a popularização da Internet ampliaram o alcance das ações referentes à telemedicina e promoveu o desenvolvimento de aplicações baseadas em *Web* como teleconsultas e teleconferências, além da utilização de recursos de multimídia no processo de manipulação de imagens, de vídeos e de áudio (3).

No ano de 1994, Anupam et al. (54) desenvolveram um sistema computacional de imagens médicas baseada em computação paralela e distribuída. A ferramenta foi concebida com um conjunto de características para gerenciamento de sessões colaborativas, direcionadas para rede local.

Gomez et al. (55) propuseram, no ano de 1996, um sistema de telemedicina para a realização de diagnósticos a partir de imagens médicas armazenadas. A ferramenta contemplava adicionalmente recursos de áudio conferência e compartilhamento de janelas.

Em 2000, Sung et al. (56) desenvolveram um protótipo de um sistema colaborativo em telemedicina para o acesso de registros de pacientes entre especialistas da área médica por meio da Internet.

Scharcanski e Machado (57), em 2004, desenvolveram um método computacional para o gerenciamento de imagens médicas, em formato digital, e no ambiente clínico hospitalar. O método consistia em um *Picture Archiving and Communication System* (PACS) e permitia a integração com distintos *Hospital Information System* (HIS) utilizados em hospitais e clínicas.

Decorrente à crescente quantidade de investigações científicas realizadas, outra modalidade de trabalho surgiu, nesse período, com consistência, ou seja, a concessão pública controlada pelo Estado por meio do registro da patente. Assim sendo e sob esse foco, a patente TW400503 (B) (58), protocolada no ano 2000, mostrou que os inventores desenvolveram um método para a interação entre as estações de monitoramento central e estações de monitoração de pacientes, por meio de vídeo. A comunicação com os equipamentos hospitalares era realizada principalmente através de dispositivos seriais como *Universal Serial Bus* (USB) e a abordagem era aplicada para o acompanhamento de dados referentes à esfigmomanômetros, termômetros e registro eletrocardiográficas.

A patente BRPI0603602 (A) (59), concebida no ano de 2006, definiu um método para a interação entre o local de tratamento de pacientes, a central de monitoramento com os componentes servidores computacionais e banco de dados, além do local de monitoramento remoto como consultórios e locais externos de acesso à rede.

Em 2007, um dos trabalhos fundamentais que contribuíram para facilitar e disseminar os serviços de tratamento de imagens médicas foi desenvolvido por Sun et al. (60). O diferencial inovador deste método foi a implementação de distintos algoritmos de processamento de imagens por meio de *software*, rompendo assim, com o paradigma anterior caracterizado pelo desenvolvimento de ferramentas inseridas em *hardware* de alto custo no processamento de imagens médicas.

Christ et al. (61) desenvolveram, em 2009, um sistema computacional em telemedicina para a monitoração remota de sinais vitais de pacientes, em tempo real, tendo

como propósito a utilização em redes corporativas de hospitais. A comunicação com os equipamentos hospitalares foi estabelecida por meio da interface RS232.

Krishna e Lexington (6), em 2011, propuseram um método computacional em telemedicina, denominado *ihasClinic*, para propiciar a interação por meio de áudio e vídeo, em tempo real, entre pacientes, médicos, assistentes sociais e outros profissionais da área da saúde. A abordagem também permite que os pacientes gravem dados e capturem imagens com o intuito de facilitar a discussão com os profissionais da área. Essas informações são armazenadas em um servidor, construindo-se um histórico do paciente.

Silva Filho et al. (7) desenvolveram, em 2012, uma ferramenta computacional distribuída para o gerenciamento e a transmissão de fluxos de vídeo. O sistema foi utilizado para a transmissão de cirurgias aplicando redes de alto desempenho. Com o desenvolvimento de trabalhos na área de telemedicina, subsidiado pelo avanço das técnicas computacionais e de telecomunicações, a transmissão de imagens e de vídeos se tornou possível e consiste em um dos principais requisitos para a realização de exames e de diagnósticos à distância. A partir desse contexto, a telemedicina passou por diferentes propósitos atrelados à medicina, tais como: telecardiologia (62), telerradiologia (63, 64), telecirurgia (65, 66), telemonitoramento (67, 68) e telediagnóstico (41, 43, 69).

As aplicações atuais de telemedicina que possuem processamento de vídeo, de áudio e de imagens médicas através da rede Internet utilizam o modelo *Transmission Control Protocol/Internet Protocol* (TCP/IP) (1, 8-10). Esta arquitetura TCP/IP oferece dois tipos de protocolos base para o transporte de dados representados pelo *User Datagram Protocol* (UDP) e pelo *Transmission Control Protocol* (TCP) (9, 70) e cada protocolo apresenta suas características específicas quanto à aplicabilidade (1).

Na medicina, a informação médica deve ser tratada de maneira confiável e íntegra e, por esse motivo, o protocolo TCP tem sido utilizado em diversos trabalhos e cada vez mais solicitado para a transmissão de dados, nessa área da saúde, devido à robustez e confiabilidade (11-13, 43, 62, 65, 71-73).

Além da escolha do protocolo de transporte a ser aplicado, as soluções em telemedicina que trabalham com fluxos devem definir importantes critérios, tais como:

- Resolução: valor em *pixels* da dimensão vertical e horizontal das imagens que compõe o fluxo de vídeo (74);
- Taxa de *Bits* ou *Bitrate*: valor que indica a quantidade de *bits* por segundo utilizados no envio do fluxo de vídeo, a qual pode ser fixa ou variável (75);
- Compressão e Qualidade de Vídeo: técnica utilizada para reduzir a largura de banda necessária para a transmissão de áudio e vídeo, podendo ser com ou sem perdas (76);
- Quadros por Segundo (QPS): valor que indica a quantidade de imagens por segundo, utilizada para a transmissão e/ou apresentação de vídeos (77).

Em relação às tecnologias atuais para o desenvolvimento de métodos em telemedicina, diversas abordagens têm explorado a utilização de ferramentas baseadas em *software* livre, permitindo assim, a redução de custos, a independência de plataforma e a customização de aplicações computacionais (17, 78-81). Outro aspecto de importante relevância para a definição de soluções computacionais para a área médica consiste na proteção dos dados e na utilização de ferramentas com fortes critérios de segurança para a transmissão de dados (11-13, 32). Na próxima seção, este tema será abordado considerando histórico evolutivo sobre a área de segurança computacional, pois representa subsídio fundamental para o entendimento da abordagem adotada neste trabalho.

1.4. SEGURANÇA COMPUTACIONAL

A segurança computacional está diretamente relacionada à capacidade de codificação dos sinais e é aplicada desde longa data para modificação da representação dos dados transmitidos. Assim sendo, a evolução e o desenvolvimento das técnicas de codificação passaram por marcos históricos importantes como (82):

- Aproximadamente no ano de 1900 a.C. – registro da substituição de parte de hieróglifos no túmulo de Khnumhotep II, caracterizando a primeira documentação da utilização de criptografia;
- Próximo ao ano de 1500 a.C. – registros da aplicação de criptografias em

protocolos de confecção de esmaltes para uso em cerâmicas por meio de aplicação de caracteres com distintos significados;

- No período do ano de 550 a.C. – utilização por escribas Hebreus de cifras de substituição simples pelo alfabeto reverso. Esta técnica, na época, foi conhecida como ATBASH;
- Ano 300 a.C. – citação no livro Arthasastra, escrito na Índia, de diversas cifras que continham recomendações para que os oficiais da espionagem transmitissem ordens aos seus subordinados pela escrita cifrada.

Ainda em período antes de Cristo, um dos métodos criptográficos que se destacou era chamado cifra de César. Nesse modelo de representação de sinais, o Imperador da Roma antiga, Júlio César, utilizava chave criptográfica por meio de deslocamento, sendo o alfabeto tratado como cíclico, de modo que a letra do texto natural era substituída pela terceira letra após a mesma.

Já em 1586 e fundamentado no modelo de criptografia cifra de César, o diplomata francês *Blaise de Vigenère* desenvolveu e publicou uma versão mais complexa. A técnica consistia no deslocamento de caracteres de conjunto de regras de substituição mono alfabéticas constituídas de 26 cifras de César e com variação de deslocamento de 0 a 25. Cada cifra era indicada por uma letra-chave (15, 82).

No século passado, ano 1920, foi construída na Alemanha a primeira máquina de cifrar conhecida como Enigma. Essa máquina realizava a criptografia de mensagens de modo mecânico por meio da substituição polialfabética (36). A partir dos anos 60, com a evolução dos computadores, foi necessária a aplicação de cifras no intuito de proteger os dados computacionais, dando origem à área de segurança da informação (1, 14-16, 36).

Uma década após, em 1973, foi proposto o método *Data Encryption Standard* (DES), o qual se tornou um padrão de criptografia para chaves simétricas. O DES codifica texto aberto em porções de 64 *bits* utilizando uma chave também de 64 *bits*. O algoritmo consiste em embaralhar completamente os dados e a chave de modo que todos os *bits* do texto cifrado dependam de todos os *bits* de dados e da chave com o intuito de formar um texto cifrado sem nenhuma correlação com os dados originais e a chave (83).

Em 1976, Diffie e Hellman (84) apresentaram um algoritmo original e consistia em uma abordagem de comunicação segura envolvendo a realização de troca de chaves. A abordagem contempla a troca de informações sem que haja a utilização de uma chave secreta conhecida com antecedência. Esse algoritmo foi um marco histórico da criptografia, iniciando o desenvolvimento dos atuais sistemas de criptografia de chave pública.

Rivest et al. (85) propuseram, em 1978, um método de criptografia conhecido como RSA face as iniciais dos três pesquisadores que o criaram, ou seja, Rivest, Shamir e Adleman. O método era fundamentado em princípios da teoria dos números por meio da aplicação de chaves de, no mínimo, 1024 *bits*. Este mecanismo definiu a robustez do algoritmo desenvolvido e destacou-se pela quantidade de aplicações práticas em área de segurança computacional.

Em 1982, Mueller-Schloer e Wagner (86) desenvolveram um sistema para escritórios que necessitava de segurança máxima baseado em criptografia. A abordagem consistiu em implementação híbrida de criptografia convencional (DES) e presença de uma chave pública (RSA). O DES era utilizado para a geração de chaves com a finalidade de realização de criptografias de mensagens e de arquivos, enquanto que as próprias chaves do DES eram criptografadas e assinadas por chaves RSA.

Apesar do amplo desenvolvimento em curto espaço de tempo das técnicas de segurança computacional, somente no final dos anos 80 foram propostos os *firewalls*, fruto da necessidade de criar restrição de acesso entre as redes existentes, aplicando políticas de segurança no conjunto de protocolos TCP/IP (1, 8-10). Nesse período, a expansão das redes acadêmicas e militares culminou com a formação da ARPANET e, posteriormente, a Internet, e por meio da popularização dos primeiros computadores e ampliação das redes de comunicação, os ataques por invasores tornaram-se cada vez mais comuns (14-16).

Os *firewalls* são dispositivos de redes de computadores que tem por objetivo aplicarem uma política de segurança a um determinado ponto da rede, realizando filtros e regras de acessos tanto físicas quanto de sessões (36).

Em 1992, Rivest (85) propôs um algoritmo para assinatura digital que se tornou um dos mais populares, denominado *Message-Digest* 5 (MD5) sendo que o preenchimento da mensagem texto era feita com comprimento de 448 *bits* para, posteriormente, este

comprimento da mensagem original ser anexado como número inteiro de 64 *bits* para então gerar uma entrada múltipla de 512.

No ano de 1993, o *National Institute of Standards and Technology* (NIST) desenvolveu o *Secure Hash Algorithm* 1 (SHA-1) (85), que é um método de *hash* para assinatura digital e trabalha com dados de entrada em blocos de 512 *bits* além de ter a capacidade de gerar resumos de 160 *bits*.

Paralelamente ao desenvolvimento dos aplicativos, ocorreu também o avanço da Internet e, de acordo com esse processo, as aplicações *Web* se popularizaram cada vez mais, necessitando assim o aumento das demandas por mecanismos de segurança.

Nesse contexto, em 1994, a empresa Netscape (87) desenvolveu o *Secure Socket Layer* (SSL) (88). Este protocolo foi projetado para fornecer criptografia de dados e autenticação entre cliente e servidor em aplicações *Web* e o início do processo é feito com uma fase de apresentação mútua na qual é definido um algoritmo de criptografia e chaves para realizar a autenticação do servidor para o cliente. O SSL, atualmente após diversos melhoramentos do sistema, é utilizado na implementação de quase todos os *browsers* populares e servidores *Web*, além de se tornar a base para o protocolo de segurança de camada de transporte denominado *Transport Layer Security* (TLS) (1, 14, 15, 38, 89).

Em 2001, o NIST anunciou o sucessor do código DES e foi denominado *Advanced Encryption Standard* (AES) (90). Este modelo computacional consistiu no desenvolvimento de um algoritmo de chave simétrica que processa dados em blocos de 128 *bits* e possibilita o trabalho com chaves de tamanhos variados, tais como 128, 192 e 256. Sob esse escopo, o NIST estimou que os tempos que uma máquina levaria para quebrar o código DES de 56 *bits e* AES de 128 *bits*, seriam de um segundo e aproximadamente 149 trilhões de anos, respectivamente.

No ano de 2002, Juels e Guajardo (16) propuseram uma abordagem para garantir a aleatoriedade na geração de chaves, contrastando com as falhas identificadas em processos envolvendo algoritmos clássicos como o RSA. Este mecanismo foi fundamental para a aplicação tanto para algoritmos criptográficos quanto para outras modalidades de segurança, tornando a identificação única e de difícil invasão ou quebra do sistema por meio de técnicas de criptoanálise.

Na patente de invenção WO/2003/081829 (91) foi definido um sistema de geração de chave digital remoto que inclui um codificador e um decifrador. Nesta invenção também foram aplicados dois sistemas com característica caótica e idênticos, sendo que o codificador utiliza um código de início para os dois sistemas caóticos e, por meio desse mecanismo, ocorre a geração da primeira chave constituída por uma sequência de *bits* aleatórios com a quantidade de *bits* desejada. Com esse procedimento, este componente pode ser aplicado para a criptografia de mensagens texto utilizando-se de qualquer algoritmo criptográfico conhecido.

De acordo com esse tema, na patente US 20050084114 (92) foi definido um método de distribuição de chaves de sessões de conferência utilizado em sistemas criptográficos, enquanto que no registro de patente da invenção EP2120389-A1 (WO2008/113279) (93), apresenta um método para geração de uma chave de sessão e dispositivos de comunicação. A abordagem deste método consistiu na geração de uma chave pública e outra privada, de longo prazo, nas duas partes da comunicação. A solução descrita possui um gerenciador de chaves central que cria e manipula as chaves utilizando algoritmos de mapeamento em conjunto com uma matriz de Fatores de Chaves Públicas e matrizes de Fatores de Chaves Públicas/Privadas.

A patente US7406175-B2 (WO03/090185) (94) descreveu um método que utiliza equipamentos de *hardware* para a geração de chaves secretas. Tal invento define um método de geração das chaves secretas usando números aleatórios a partir de valores dados pelo relógio do computador e armazenados em *hardware*.

Outra invenção, sob registro US7372961-B2 (95), provê uma técnica de geração de chaves em que na ocorrência de qualquer desvio do processo delineado, esta é eliminada durante o processo de seleção. Além disso, também são descritos os principais elementos, a rede de comunicação e dois dispositivos eletrônicos, os quais possuem segurança criptográfica baseadas em *hash* como o SHA-1 (85).

Na patente US7739501-B2 (96) é proposto um método computacional para a geração de chaves criptográficas secretas, denominada rótulo, para uso na troca de informações entre membros de organizações em matrizes e filiais. O programa reside em um computador cujos dados armazenados podem ser lidos somente por dispositivos

mecânicos. Para a criptografia, foi aplicada uma função *hash* de único sentido que utiliza um gerador não determinístico de *bits* aleatórios com o objetivo de produzir uma chave pura e com associação a chaves de leitura-escrita e de escrita, para no final, formar o rótulo final.

Por meio das seções anteriores foi possível contextualizar e evolução das tecnologias computacionais, dos métodos de segurança e de aplicações multidisciplinares aplicadas à área da saúde. Desse modo, verifica-se que as contribuições da computação para a área médica devem ser ampliadas em busca de soluções que cooperam para a melhoria da qualidade de vida das pessoas.

A partir desse contexto, neste trabalho foram desenvolvidos dois métodos e um sistema computacional que promove o acompanhamento e a interação remota entre profissionais da área médica durante a realização de exames videocolonoscópicos.

2. OBJETIVOS

Objetivo Geral:

Propor um método em Telemedicina para o acompanhamento remoto e para a interação entre profissionais da área da saúde, em tempo real, durante a realização de exames videocolonoscópicos.

Objetivos Específicos:

- Desenvolver um sistema computacional para o gerenciamento de dados de exames de videocolonoscopia, e para o acompanhamento desses exames, em tempo real, através de rede local e Internet;
- Implementar um método de segurança para a manutenção da privacidade de dados de texto, de imagens e de vídeos relativos aos exames videocolonoscópicos;
- Facilitar a inter-relação de especialistas de domínio médico em locais geograficamente distintos.

3. HIPÓTESE

Assertivas e Hipótese:

Assertivas:

1. As técnicas computacionais de transmissão de dados podem ser aplicadas na área da medicina;
2. O processo de transmissão de dados médicos exige cuidados máximos em relação à segurança dessas informações.

Hipótese:

O desenvolvimento do método de transmissão de dados de exames provenientes de videocolonoscopia, em tempo real e por via Internet, utilizando-se de métodos criptográficos, amplia a interação entre os profissionais da área da saúde provendo segurança das informações transmitidas.

4. MATERIAIS E MÉTODOS

4.1. MÉTODO COMPUTACIONAL PARA O ACOMPANHAMENTO DE EXAMES DE VIDEOCOLONOSCOPIA EM TEMPO REAL

O delineamento do método computacional, assim como das demais atividades para o desenvolvimento da solução tecnológica deste trabalho, baseou-se nas recomendações e preceitos provenientes da Engenharia de Software (97-99) aplicando-se o processo de desenvolvimento denominado Prototipação (100). Esse processo inclui as etapas de especificação de requisitos, de elaboração do projeto de desenvolvimento do aplicativo, assim como da implementação e dos testes do método computacional.

4.1.1. ESPECIFICAÇÃO DE REQUISITOS

Nesta etapa, os conceitos e as funcionalidades identificados foram fundamentados nas características provenientes dos Sistemas de Informações Hospitalares (HIS) e de Comunicação e Arquivamento de Imagens (PACS) (32, 101, 102).

Inicialmente, o domínio do problema foi analisado e discutido por meio de reuniões com especialistas da área médica que envolveu temas como compreensão do protocolo para a realização de exames de videocolonoscopia (103, 104), conhecimento dos equipamentos além dos mecanismos de comunicação disponibilizados, das diferenças de componentes entre marcas, modelos, resoluções de vídeo, qualidade das imagens geradas, tecnologias de entrada e de saída de vídeos, entre outros.

Após esta fase inicial, e por meio do acompanhamento de procedimentos videocolonoscópicos em conjunto com especialistas da área de domínio médico, os principais requisitos técnicos foram elencados para a construção do sistema computacional, e estão definidos a seguir:

- Acessibilidade ao sistema computacional somente por profissionais cadastrados e com permissão para utilizá-lo;
- Manutenibilidade das informações referentes à:
    - Profissionais da área da saúde;
    - Pacientes, incluindo armazenamento e gerenciamento de informações relativas aos registros históricos dos exames clínicos realizados;

    - Exames dos pacientes, incluindo armazenamento e gerenciamento de dados, de vídeo e de imagens capturadas.
- Implementação de recursos de comunicação do sistema computacional com o videocolonoscópio para a captura e o armazenamento de imagens e de vídeos durante a realização dos exames;
- Desenvolvimento de artefatos de exportação de dados de pacientes e de imagens dos exames para o formato *Digital Imaging and Communications in Medicine* (DICOM) (105);
- Acompanhamento de exames de videocolonoscopia através da Internet, utilizando-se de navegadores (*Web Browsers*) no próprio local de realização do procedimento endoscópico ou remotamente, e em tempo real, por meio de mensagens de texto, voz, vídeo e imagem;
- Definição do modelo computacional de modo a possibilitar a expansão para outras modalidades de exames médicos de imagem realizados por equipamentos diferentes;
- Construção de interface computacional amigável;
- Implementação de funcionalidades para análise dos exames endoscópicos realizados após o término dos mesmos;
- Desenvolvimento de mecanismos de segurança.

Após a definição dos requisitos técnicos e considerando-se as particularidades do domínio do problema, foram analisadas as alternativas tecnológicas e delineado o método computacional.

4.1.2. DELINEAMENTO DA CONSTRUÇÃO DO SISTEMA DE TELEMEDICINA EM TEMPO REAL (S2TR)

Nesta seção serão apresentados os modelos de arquitetura, de dados, de segurança do sistema e de compartilhamento de imagens que compuseram o desenvolvimento do método implementado no S2TR para o acompanhamento e a interação remota, em tempo real, de exames de videocolonoscopia.

4.1.2.1. MODELO DE ARQUITETURA

A partir do estudo do domínio específico e da definição de requisitos funcionais, foi construído o modelo arquitetural composto pelos seguintes componentes (Figura 1):

- Sala de Procedimentos Endoscópicos (SPE): local de realização dos procedimentos endoscópicos, situada, neste trabalho, na Gastrocentro da Universidade Estadual de Campinas/UNICAMP, e apresenta os seguintes componentes (Figura 2):
    - Equipamento Hospitalar (EH): equipamento utilizado para a realização do exame endoscópico e representado pelo videocolonoscópio de marca Fuginon, modelo VP-4400 (Figura 3);
    - Unidade de Execução Local (UEL): componente de comunicação entre o computador e o videocolonoscópio responsável pela aquisição e encaminhamento do vídeo para o Servidor de Aplicações (SA) e presente no Central de Gerenciamento (CG).
- Unidades de Acompanhamento e de Interação Remota (UAIR): local com componentes de *hardware* e de *software* disponibilizados para profissionais participantes autorizados no acompanhamento dos exames realizados com o videocolonoscópio (Figura 4);
- Central de Gerenciamento (CG): local de gerenciamento dos recursos computacionais utilizados para a realização do exame, do acompanhamento e da interação local e remota entre os participantes, tanto na SPE quanto nas UAIR. A Central de Gerenciamento é composta por:
    - Servidor de Aplicações (SA);
    - Banco de Dados (BD);
    - Base de Imagens e Vídeos (BIV);
    - Módulo de Segurança (MS).

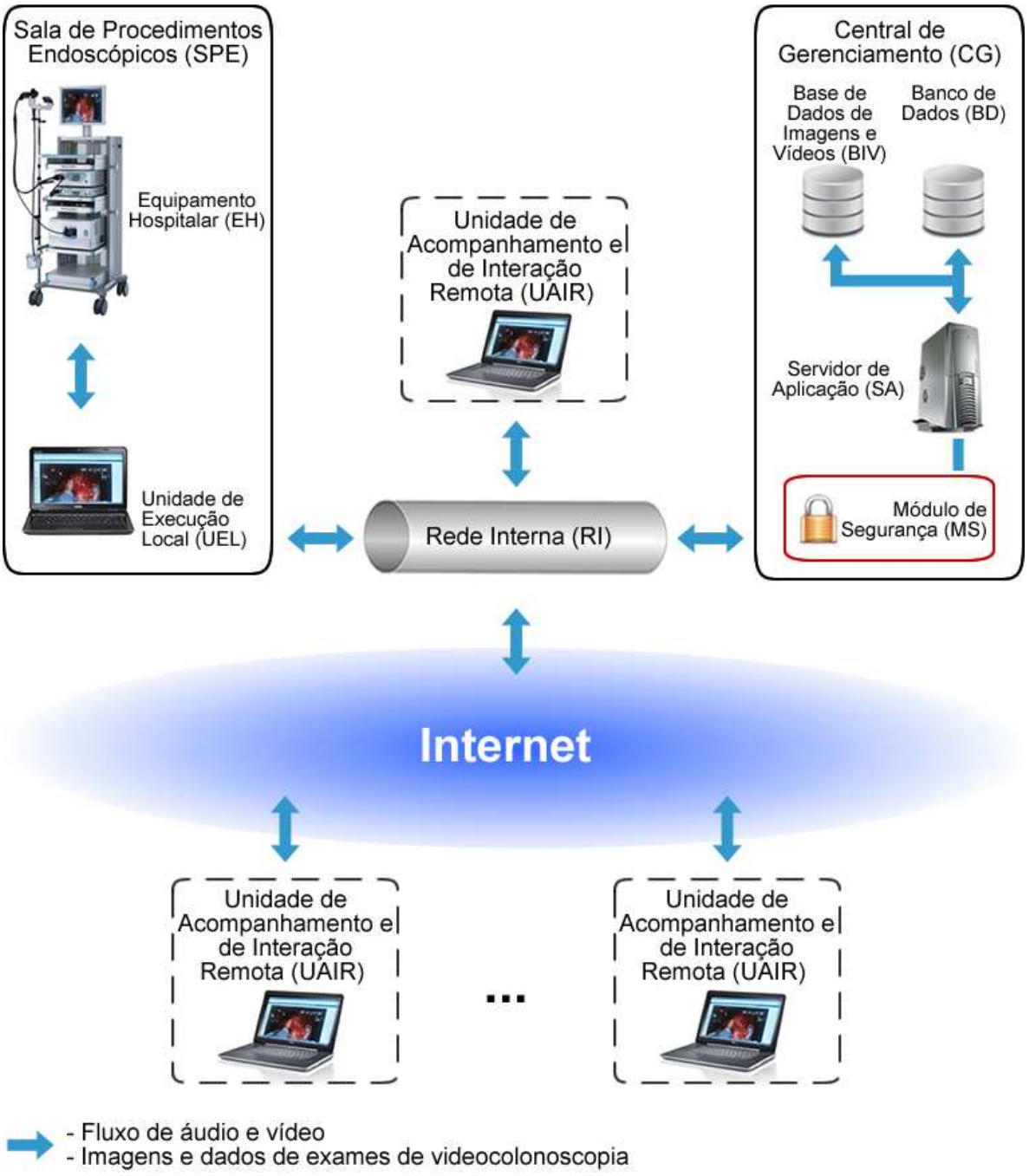

Figura 1. Modelo de Arquitetura do Método em Telemedicina para o Acompanhamento de Exames de Videocolonoscopia.

Figura 2. Sala de Procedimentos Endoscópicos na Gastrocentro da UNICAMP.

Figura 3. Equipamento Hospitalar: Videocolonoscópio, Marca Fuginon, Modelo 4400.

Figura 4: UAIR no Laboratório de Bioinformática da UNIOESTE.

- Rede Interna (RI): dispositivos de *hardware* e de *software* utilizados para comunicação e transmissão de dados, vídeos, imagens e áudio em área interna à instituição na qual os exames videoendoscópicos são realizados;
- Rede Externa (RE) ou Internet: redes de comunicação de dados externos à instituição, utilizadas pelas UAIRs.

4.1.2.2. MODELO DE DADOS

O projeto do modelo de dados foi construído por meio do artefato Modelo Entidade Relacionamento (MER) usando o Sistema Gerenciador de Banco de Dados (SGDB) MySQL[3] versão 5.1.42. As entidades definidas para a construção deste artefato são:

- Entidade Profissional: responsável pelo registro das informações sobre os profissionais da área da saúde que possuem acesso ao sistema com dados gerais de identificação como nome, Cadastro de Pessoas Físicas (CPF), Registro Geral (RG), data de nascimento, sexo, telefone, endereço, vínculo institucional e

[3] <http://www.mysql.com/>.

informações de autenticação como nome do usuário e senha. Esta entidade, quando utilizada para o registro de médicos, especificamente apresenta campo para cadastro do número de registro do Conselho Regional de Medicina (CRM);

- Entidade Paciente: responde pelo armazenamento dos dados relativos aos pacientes, tais como nome, CPF, RG, data de nascimento, email, sexo, telefone e endereço;
- Entidade Instituição: realiza o armazenamento das informações relativas a endereço, contatos e especialidades da Instituição;
- Entidade Equipamento: contém a identificação dos equipamentos utilizados para a realização dos exames de videocolonoscopia, como marca e modelo;
- Entidade Exame: realiza o inter-relacionamento entre as entidades profissional, paciente, instituição e equipamento, bem como armazena os dados sobre os exames complementares;
- Entidade Laudo: nesta entidade são gerenciados os dados relativos aos laudos dos exames de videocolonoscopia, incluindo identificação do médico responsável e do exame, resultado do exame, indicação de tratamento, observações e data de realização do laudo;
- Entidades Auxiliares: são compostas por banco de dados de cidades, Estados, Países, vínculos institucionais dos profissionais, convênios de saúde, como exemplo, o Sistema Único de Saúde (SUS) e a UNIMED, além das configurações do S2TR.

4.1.2.3. MÓDULO DE SEGURANÇA (MS)

O sistema de segurança proposto neste trabalho é composto por outros dois módulos, a Segurança Interna e a Segurança Externa, as quais são apresentadas a seguir.

Módulo de Segurança Interna (MSI)

O MSI foi desenvolvido de acordo com as seguintes características:

- Aplicação de transmissão de dados entre a UEL, o SA e as UAIR por meio da camada de segurança *Server Socket Layer* (88) do modelo de referência *Transport Control Protocol / Internet Protocol* (TCP/IP) (9, 70);
- Implantação de regras no SA para delimitar os locais autorizados de redes para o acesso ao sistema de acompanhamento remoto de exames. Essa personalização foi realizada por meio de endereços *Internet Protocol* (IPs) (1) ou por domínios da Internet;
- Autenticação por meio do fornecimento de identificação do usuário e, após a validação de uso do sistema, fornecimento de senha, a qual é criptografada por meio do algoritmo *Secure Hash Algorithm* 1 (SHA-1) (85);
- Definição de senhas constituídas, no mínimo, de oito caracteres, e deve conter letra(s) em maiúscula(s), letra(s) em minúscula(s), número(s) e caracter(es) especial(s). As senhas são registradas de modo histórico, não sendo permitida a repetição das mesmas quando se efetuam as alterações;
- Possibilidade de configuração do sistema para que em caso de autenticação com sucesso, email seja enviado para o profissional responsável pela conta com as seguintes informações: horário e localização geográfica em que a autenticação foi realizada no sistema com armazenamento de histórico mantido na base de dados;
- Permissão de, no máximo, duas tentativas sem sucesso num período de 24 horas. Caso o usuário não consiga obter êxito, a conta é bloqueada e o sistema envia email de notificação para o responsável da conta com as seguintes informações: aviso sobre o bloqueio da conta, descrição das tentativas de senhas digitadas incorretamente, horário e local geográfico em que ocorreram as tentativas de acesso;
- Reversão do bloqueio da conta realizada pela solicitação de um código ao sistema, o qual é fornecido por email para o usuário que teve a sua conta

bloqueada. Posteriormente ao processo, o usuário deve digitar esse código no sistema e cadastrar uma nova senha.

Módulo de Segurança Externa (MSE)

O MSE é responsável pela interface entre a rede interna e a rede externa ou Internet, sendo as políticas de segurança definidas no MSI. Para a comunicação da rede interna com a rede externa, o MSE foi definido e implementado de acordo com as características abaixo:

- Configurações desenvolvidas por meio de regras de *firewall*, configurando-se o que é aberto e o que é fechado para acesso externo, bem como de lista de locais confiáveis e de lista de locais proibidos;
- Definição e aplicação de ferramentas para detecção de intrusão, de ferramentas para armazenamento e análise de *log* e sistemas de *proxy* pertencentes aos servidores que realizam a interconexão da rede interna com a rede externa.

Para a publicação de *streams*[4] de áudio e de vídeo, foi proposto, no MSE, o método para Geração de Chaves Baseado em Algoritmos Genéticos - **LABI-PUBLISH**, cujo processo consiste na utilização de conceitos relacionados a algoritmos baseados na Teoria da Evolução das Espécies (106, 107) e recursos computacionais para a geração de chaves secretas (15).

Os componentes que fazem parte do **LABI-PUBLISH** são apresentados na Figura 5 e o algoritmo que implementa o método computacional é descrito por meio da Figura 6.

4.1.2.4. MODELO PARA O COMPARTILHAMENTO DE IMAGENS

O modelo para Compartilhamento de Imagens – **LABI/IMAGE/SHARING** foi desenvolvido para a captura e o compartilhamento de imagens relativas aos exames endoscópicos, entre os participantes, tanto locais quanto remotos. Esse modelo é delineado de acordo com os seguintes passos:

[4] Qualquer Fluxo de dados em um sistema computacional. Exemplos de tipos desse fluxo são arquivos, áudio e vídeo.

- Captura da imagem relativa ao procedimento médico em execução pelo Participante A, na UEL ou na UAIR;
- Codificação da imagem para modo texto e formato BASE64 (108);
- Transmissão da imagem codificada pela rede até o SA;
- Armazenamento da imagem pelo SA na BIV em formato JPEG ou BMP (109);
- Notificação da localização, na BIV, da imagem pelo SA ao participante que originalmente capturou a imagem - Participante A;

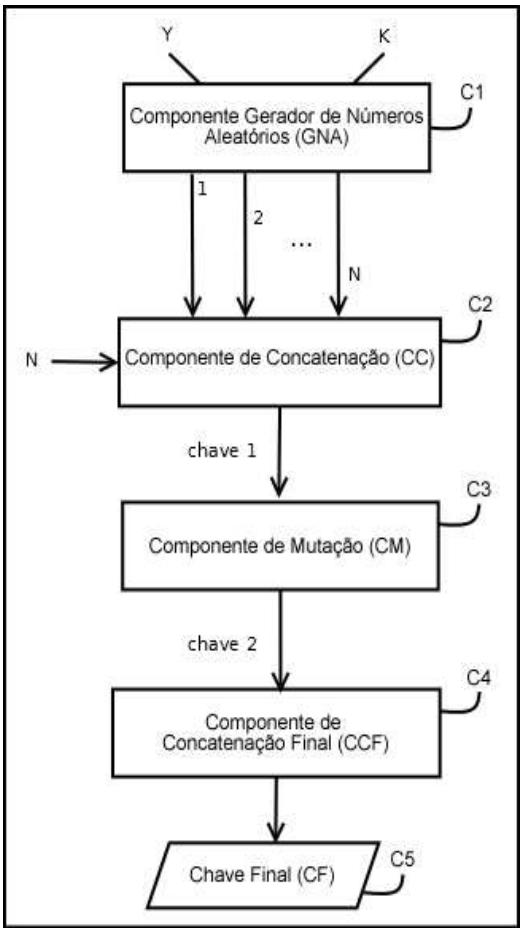

Figura 5: Componentes do Método para a Geração de Chaves Baseado em Algoritmos Genéticos.

Fase 1: Geração da primeira Chave (chave 1)

Nesta fase é gerada a **chave1** por meio da aplicação de componentes aleatórios executando-se os seguintes procedimentos:

1. Gera-se **N** números aleatórios utilizando o Componente Gerador de Números Aleatórios (GNA) (C1). Cada um desses números deve ficar dentro dos limites entre **Y** e **K**. Cada um desses valores numéricos pode conter uma quantidade de caracteres variando entre o número de dígitos de **Y** e o número de dígitos de **K;**

2. O resultado da Fase 1 (**chave 1**) consiste na concatenação dos caracteres gerados pelos **N** números aleatórios, convertidos para formato texto. Esse procedimento é realizado pelo Componente de Concatenação (CC) (C2).

Fase 2: Geração da segunda Chave (chave 2)

Nesta fase gera-se a **chave2** por meio do Componente de Mutação (CM) (C3), o qual utiliza o operador de mutação sobre 50% da **chave1** do seguinte modo:

1. Todos os caracteres da **chave1** são percorridos, de modo que:

   i. Se a posição do caractere na **chave1** for par, esse caractere é adicionado a **chave2**;

   ii. Se a posição do caractere na **chave1** for ímpar será adicionado na **chave2** um caractere ASCCII aleatório.

Fase 3: Geração da Chave Final

A **Chave Final (CF)** (C5) é gerada pelo Componente de Concatenação Final (CCF) (C4), sendo composta pelos seguintes elementos:

i. Hora, minutos, segundos e milissegundos da geração da chave;

ii. chave2.

Parâmetros de Configuração: Esse método pode ser aplicado para distintos propósitos e, por conseguinte, os valores de **N**, **Y** e **K** podem ser personalizados conforme critério de segurança da aplicação. Neste caso, especificamente, foram adotados os valores **N=300**, **Y=0**, **k=9999999999** e operador de mutação de **50%**.

Figura 6: Método para a Geração de Chaves Baseado em Algoritmos Genéticos.

- Envio de mensagem a partir do local, UEL ou UAIR, no qual a imagem foi capturada pelo participante A para todos os outros participantes do procedimento, tanto na UEL quanto na(s) UAIR(s). O conteúdo dessa mensagem é representado pela localização da imagem capturada;
- Realização de *download* da imagem, a partir do SA, pela UEL e pela(s) UAIR(s) e apresentação gráfica para os participantes.

O algoritmo para a captura e o envio das imagens é apresentado na Figura 7 e o algoritmo para a recepção das imagens é descrito na Figura 8.

```
1  //Procedimento para captura de Imagens
2  procedimento capturarImagens ()
3  Início
4     //Captura imagem relativa ao procedimento médico
5     Imagem <- capturaImagem();
6
7     //Processa  imagens capturadas
8     Para cada Imagem Capturada faça
9     Início
10          //Codifica imagem para formato texto, em Base64
11          ImagemB64 <- codificaImagemParaBase64 (Imagem);
12
13         //Envia imagem para o Servidor e o Servidor armazena na Base de Imagens
14          //Servidor retorna o endereço para que os participantes possam fazer download
15          enderecoImagem <- enviaImagemParaServidor (Imagem64);
16
17          //Notificam todos os clientes sobre a nova imagem e seu endereço para download
18          Para cada cliente em Participantes faça
19          Início
20             //Envia mensagem ao Cliente com o endereço da nova imagem para download
21              enviaMensagem (enderecoImagem);
22          Fim
23       Fim
24 Fim Procedimento
```

Figura 7: Algoritmo de Captura e Transmissão de Imagens – Método LABI/IMAGE/SHARING.

```
1  //Procedimento para o recebimento de Imagens
2  //Esse procedimento é executado paralelamente por todos os clientes participantes
3  //Na Unidade de Execução Local e nas Unidades de Acompanhamento e Interação Remota
4  procedimento receberImagem (enderecoImagem)
5  Início
6      //Realiza o download da Imagem em formato texto Base64
7      Imagem64 <- downloadImagem (enderecoImagem);
8
9      //Decodifica a Imagem
10     Imagem <- decodificaImagem (Imagem64);
11
12     //Adiciona a Imagem a caixa de Imagens na tela do Cliente
13     adicionaImagem (Imagem);
14 Fim Procedimento
```

Figura 8: Algoritmo para o Recebimento de Imagens – Método LABI/IMAGE/SHARING.

4.2. ETAPAS DE EXECUÇÃO DO MÉTODO PROPOSTO

O método proposto para o acompanhamento remoto de procedimentos médicos, em tempo real, foi executado em cinco etapas:

- **Etapa 1**: Disponibilização dos Serviços;
- **Etapa 2**: Processo de Autenticação;
- **Etapa 3**: Iniciação da Unidade de Execução Local;
- **Etapa 4**: Acompanhamento Remoto de Procedimentos Médicos;
- **Etapa 5**: Finalização do Procedimento Médico e encerramento do S2TR.

Etapa 1: Disponibilização dos Serviços

A primeira etapa consiste na realização de configurações específicas do sistema de Telemedicina para disponibilizar os serviços necessários às UEL e UAIR. Para isso são realizados processos como:

- Iniciação do Servidor de *Streaming*;
- Iniciação do Servidor de Banco de Dados;
- Iniciação do Servidor de Páginas *Web*;
- Iniciação do Módulo de Segurança (MSE e MSI).

Os procedimentos elencados, anteriormente, são executados de modo automático pelos componentes de *hardware* e *software* do sistema computacional que implementa o método proposto.

Etapa 2: Processo de Autenticação

O processo de autenticação é pré-requisito para o acesso a qualquer funcionalidade e é executado sempre que um usuário se conecta para utilizar o sistema, tanto na UEL quanto na(s) UAIR (s). O algoritmo executado é apresentado na Figura 9.

```
1  Procedimento autenticacao ( Texto login, Texto senha )
2  Inicio
3        Selecione login e senha na base de dados;
4        Se resultado da busca for positivo (encontrado) então faça
5              Instancie um novo objeto Usuário;
6              Adicione o novo objeto Usuário para a lista de Usuários Autenticados;
7              Notifique o usuário sobre o acesso autorizado, caso essa opção esteja ativada;
8        Fim Se
9        Senão
10             Rejeite a conexão;
11             Notifique o usuário sobre o acesso rejeitado;
12       Fim Se
13 Fim Procedimento
```

Figura 9: Algoritmo para a Autenticação de Usuários.

Conforme apresentado na Figura 9, a autenticação consiste em validar a identificação de um usuário (*login*) e a senha correspondente. Para essa validação, os dados de identificação (*login*) e da senha são comparados com as informações armazenados na base de dados de modo criptografado.

Caso o processo de autenticação tenha sucesso, o usuário é adicionado à lista de usuários autenticados e, então, conectado ao sistema. Em contrário, a conexão do usuário ao sistema é rejeitada.

Etapa 3: Iniciação da Unidade de Execução Local (UEL)

Após a execução das Etapas 1 e 2, as seguintes ações são realizadas na UEL:

- Estabelecimento do Protocolo de Comunicação com o Equipamento Endoscópico por meio da utilização de um canal para o recebimento de vídeo como o S-Video ou o vídeo composto;
- Realização da conexão com o SA pelo protocolo de transporte *Transmission Control Protocol* (TCP) (9);
- Iniciação da aquisição de fluxos de vídeo e/ou áudio a partir do equipamento endoscópico, conforme os algoritmos apresentados por meio da Figura 10 e da Figura 11;
- Disponibilização pela UEL de fluxos de vídeo e/ou áudio para o AS. Esse procedimento é realizado conforme os algoritmos apresentados por meio da Figura 12 e da Figura 13.

```
1  Procedimento aquisicaoDeVideo ()
2  Inicio
3        Inicie objeto (objetoVideo) para captura de vídeo;
4        Defina os parâmetros de objetoVideo para a captura do vídeo:
5              - codec de vídeo;
6              - resolução;
7              - número de quadros por segundo;
8              - qualidade desejada;
9              - índice de compactação;
10       Com objetoVideo, inicie a captura de vídeo;
11 Fim Procedimento
```

Figura 10: Algoritmo para a Aquisição de Vídeo.

Conforme apresentado na Figura 10, para a aquisição de vídeo, é iniciado um objeto para essa finalidade e, posteriormente, são realizadas configurações como definição do *codec*[5] de vídeo, da resolução, da taxa de aquisição em quadros por segundo, da qualidade e do índice de compactação. Após esses procedimentos, a captura do vídeo é efetivamente iniciada.

```
1  Procedimento aquisicaoDeAudio ()
2  Inicio
3        Inicie objeto (objetoAudio) para captura de áudio;
4        Defina os parâmetros de objetoAudio para a captura do áudio:
5              - codec de áudio;
6              - qualidade desejada;
7              - níveis de supressão de echo;
8        Com objetoAudio, inicie a captura do áudio;
9  Fim Procedimento
```

Figura 11: Algoritmo para a Aquisição de Áudio.

Na Figura 11 apresentou-se a sequência de procedimentos realizados para a aquisição de áudio, a qual é iniciada com a criação de um objeto específico para configurações como definição do *codec* de áudio, da qualidade e do índice de supressão de *echo*. Após tais mecanismos é que efetivamente ocorre a captura do áudio.

```
1   Procedimento publicacaoDeVideo (Video objetoVideo)
2   Inicio
3        Inicie objeto (objetoStream) para publicação de Stream;
4        Com objetoStream faça
5              Defina um nome de identificação para o Stream;
6              Estabeleça uma conexão com o Servidor de Stream;
7              Aloque um canal de comunicação com o Servidor de Stream;
8              Disponibilize o vídeo (objetoVideo) por meio do canal de
9              comunicação alocado no passo anterior;
10       Fim Com
11  Fim Procedimento
```

Figura 12: Algoritmo para a Publicação de Vídeo.

[5] *Hardware* ou *software* que realiza a codificação ou decodificação de fluxos de dados digitais ou sinais.

```
1  Procedimento publicacaoDeAudio (Audio objetoAudio)
2  Inicio
3      Inicie objeto (objetoStream) para publicação de Stream;
4      Com objetoStream faça
5          Defina um nome de identificação para o Stream;
6          Estabeleça uma conexão com o Servidor de Stream;
7          Aloque um canal de comunicação com o Servidor de Stream;
8          Disponibilize o áudio (objetoAudio) por meio do canal de
9          comunicação alocado no passo anterior;
10     Fim Com
11 Fim Procedimento
```

Figura 13: Algoritmo para a Publicação de Áudio.

Conforme apresentado na Figura 12 e na Figura 13, para a publicação de vídeo e áudio, o objeto é solicitado com a finalidade de estabelecer um canal de *stream* com o SA, e por meio desse processo, é definida uma identificação pelo método **LABI-PUBLISH**. Após o procedimento, estabelece-se uma conexão com o SA para a publicação do *stream* e, por fim, o vídeo e o áudio são disponibilizados por meio deste canal de comunicação.

Etapa 4: Acompanhamento Remoto de Procedimentos Médicos

Por meio das UAIRs é possível acompanhar os exames de videocolonoscopia em tempo real. Para a realização desta etapa foi necessário o desenvolvimento do processo de autenticação no sistema, conforme definido na Etapa 2.

Para cada conexão de nova UAIR no acompanhamento do exame, são executados os procedimentos a seguir:

- Atualização da lista de conexões pelo SA e o envio dessa lista para todas as conexões ativas, tanto UEL quanto UAIR;
- Encaminhamento pelo SA dos dados relativos ao exame em execução para a nova UAIR;
- Estabelecimento, pela nova UAIR, da conexão com o SA e, com isso, passa a receber os fluxos de vídeo e/ou áudio provenientes do exame em execução na UEL;

- Realização de *download* e apresentação das imagens do exame em execução pela nova UAIR.

Etapa 5: Finalização do Procedimento Médico Endoscópico e Encerramento do S2TR

Após o término do procedimento endoscópico, o S2TR realiza as seguintes ações:

- Encerramento da publicação do fluxo de vídeo e/ou áudio da UEL;
- Encerramento do SA e dos canais de comunicação das UAIR relativos ao recebimento de fluxos de áudio e/ou vídeos provenientes do procedimento endoscópico;
- Encerramento da comunicação entre a UEL e o equipamento endoscópico em que o exame foi realizado;
- Término da comunicação entre a UEL e o SA.

4.3. FERRAMENTAS COMPUTACIONAIS UTILIZADAS NO DESENVOLVIMENTO DO S2TR

Para a definição e o desenvolvimento dos requisitos de construção do S2TR, foi necessária a utilização das seguintes ferramentas computacionais:

- Padrão de desenvolvimento *Model-view-controller* (MVC) (110) aplicando:
    - Linguagem de programação Java (111);
    - Servidor de Aplicações JBOSS *Aplication Server* versão 4.2 (112);
    - Servidor de *Streamings* Red5 versão 1.0 RC1 (113);
    - Sistema Gerenciador de Banco de Dados MySQL versão 5.1.42 (114).

Para a apresentação visual dos vídeos e das imagens, assim como a comunicação com os dispositivos de captura de vídeo e áudio e os recursos de acompanhamento remoto de exames endoscópicos, foram utilizados os seguintes aplicativos:

- Linguagem de programação Flex versão 4.0 (115);
- *Framework* Flamingo (116);
- *Framework* de desenvolvimento JBOSS Seam versão 2.1.2 (117).

Na Figura 14 são apresentados os componentes do SA, seguindo a definição em camadas conforme o padrão MVC. Para a função de servidor *Web* utilizou-se o aplicativo *Apache Tomcat* (118).

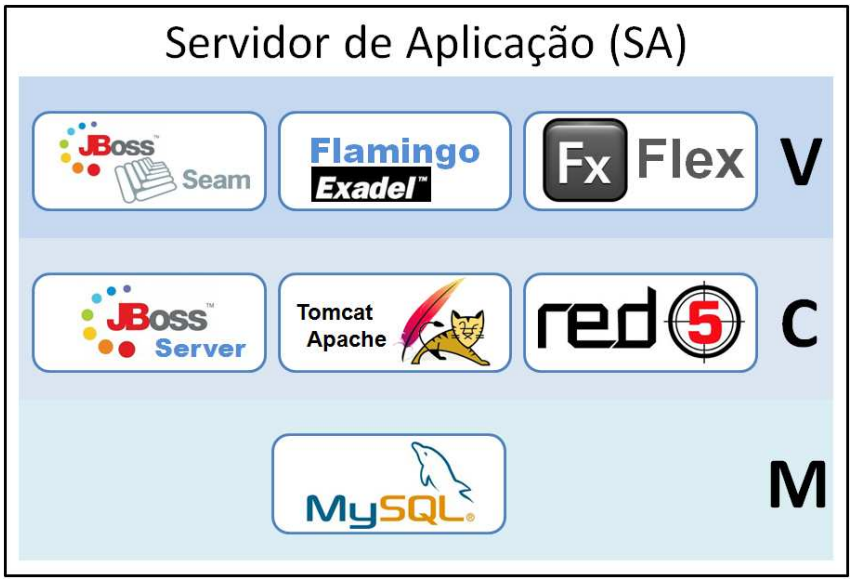

Figura 14: Tecnologias Computacionais Aplicadas no SA conforme Modelo MVC.

4.4. DELINEAMENTO EXPERIMENTAL

4.4.1. LOCAL DE EXPERIMENTAÇÃO

Os experimentos foram realizados na Gastrocentro/UNICAMP, Setor de videocolonoscopia do Serviço de Coloproctologia da Faculdade de Ciências Médicas da Universidade Estadual de Campinas e no Laboratório de Bioinformática da Universidade Estadual do Oeste do Paraná do campus de Foz do Iguaçu (LABI/UNIOESTE). Além destas instituições, ocorreu o auxílio do Centro de Computação Científica e Software Livre do Departamento de Informática da Universidade Federal do Paraná (C3SL/UFPR) e do Laboratório de Inteligência Computacional do Instituto de Ciências Matemáticas e de Computação da Universidade de São Paulo no campus de São Carlos (LABIC/USP).

4.4.2. MATERIAIS UTILIZADOS

Para os experimentos realizados neste trabalho foram utilizados sete computadores e outros equipamentos sendo:

- Um Servidor, na quantidade de um aparelho;
- Um Emissor, na quantidade de um aparelho;
- Cinco Clientes, na quantidade de cinco aparelhos;
- Uma Filmadora Digital JVC Everio GZ HD 520;
- Um *Access Point* TP LINK TL-WA 901ND 54 Mbps, com uma conexão de rede local Gigabit Ethernet 802.3z (31), uma conexão de rede local por meio de uma interface *wireless*[6] padrão 802.11b (120) e conexões com a Internet via os seguintes *links*: RNP[7] 100 Mbps, RNP 1000 Mbps e ADSL[8] 15 Mbps;
- Um vídeo de exame de videocolonoscopia, disponibilizado conforme registro no 2° Tabelionato de Notas de Foz do Iguaçu sob número de protocolo 00046780 (001-000690360) (Anexo I).

A seguir serão apresentadas as configurações de *hardware* e *software* de cada computador.

Configuração de *hardware*:

- **Servidor**: Processador Intel Core 2 Duo CPU E4500 2,20GHz, memória RAM de 4,0 GB, placa de vídeo Intel 82Q963/Q965 Integrated Graphics e placa de rede Broadcom NetXtreme BCM5755 Gigabit Ethernet;
- **Emissor**: Processador Intel Core i7-2630QM CPU 2,00GHz, memória RAM de 6,0 GB, placa de vídeo Intel HD Graphics Family e placa de rede JMicron PCI Express Gigabit Ethernet;
- **Cliente Local ETHERNET**: Processador Intel Core 2 Quad CPU Q9550 2,83GHz, memória RAM de 4,0 GB, placa de vídeo Intel Q45/Q43 Express

[6] O termo *wireless* é amplamente usado como referência à comunicação sem fio.

[7] Rede Nacional de Ensino e Pesquisa.

[8] ADSL (*Asymmetric Digital Subscriber Line)* constitui uma tecnologia de comunicação utilizada para a conexão com a Internet.

Chipset e placa de rede Intel 82567LM-3 Gigabit Ethernet;

- **Cliente Local WIFI**[9]: Processador Intel Core i5-2410M CPU 2,30GHz, memória RAM de 4,0 GB, placa de vídeo Intel HD Graphics e placa de rede Dell Wirelles 1702 b/g/n;
- **Cliente A**: Processador Intel Core i5-3210M CPU 2,50GHz, memória RAM de 4,0 GB, placa de vídeo Intel HD Graphics 4000 e placa de rede JMicron PCI Express Gigabit Ethernet;
- **Cliente B**: Processador Core 2 Duo CPU T8100 2,10GHz, memória RAM de 2,0 GB, placa de vídeo NVIDIA GEForce 8400M GS e placa de rede Marvell Yukon 88E8055-E Gigabit Ethernet;
- **Cliente ADSL**: Processador Intel Core i5-2410M CPU 2,30GHz, memória RAM de 6,0 GB, placa de vídeo Intel HD Graphics e placa de rede Realtek PCIe FE Family Ethernet.

- **Configuração de *software*:**
  - **Servidor**: Sistema operacional Linux Debian Server kernel 2.6.32.-5-amd64 64-bit, *browser* Mozilla Firefox 18.0.2, *plugin Shockwave Flash* 11.5 r502, Java (TM) Platform SE 7 U13 e o servidor de *streams* Red5 1.0 RC 1;
  - **Emissor**: Sistema operacional Microsoft Windows 7 Professional 64-bit SP1, browser Mozilla Firefox 18.0.2, *plugin Shockwave* Flash 11.5 r502, Java(TM) Platform SE 7 U13 e o emulador de câmeras e2eSoft VCam;
  - **Cliente Local ETHERNET**: Sistema operacional Microsoft Windows 7 Professional 32-bit SP1, *browser* Mozilla Firefox 18.0.2, *plugin Shockwave Flash* 11.5 r502 e Java(TM) Platform SE 7 U13;
  - **Cliente Local WIFI**: Sistema operacional Microsoft Windows 7 Home Basic 64-bit SP1, *browser* Mozilla Firefox 18.0.2*, plugin Shockwave* Flash 11.5 r502 e Java(TM) Platform SE 7 U13;
  - **Cliente A**: Sistema operacional Microsoft Windows 7 Home Basic 64-bit SP1, *browser* Mozilla Firefox 18.0.2, *plugin Shockwave Flash* 11.5 r502,

[9] Neste trabalho, os termos *wireless* e WIFI são usados indistintamente.

Java(TM) Platform SE 7 U13 e a ferramenta de controle remoto *TeamViewer* 8.0.16642;

- **Cliente B**: Sistema operacional Microsoft Windows 7 Professional 32-bit SP1, *browser* Mozilla Firefox 18.0.2, *plugin Shockwave Flash* 11.5 r502, Java(TM) Platform SE 7 U13 e a ferramenta de controle remoto *TeamViewer* 8.0.16642;
- **Cliente ADSL**: Sistema operacional Microsoft Windows 7 Professional 64-bit SP1, *browser* Mozilla Firefox 18.0.2, *plugin Shockwave Flash* 11.5 r502, Java(TM) Platform SE 7 U13 e a ferramenta de controle remoto *TeamViewer* 8.0.16642.

Após a definição dos materiais utilizados, nas próximas seções serão apresentados os dois ambientes em que os experimentos foram realizados.

4.4.3. PROCEDIMENTO EXPERIMENTAL PARA A AVALIAÇÃO DE DESEMPENHO

4.4.3.1. DEFINIÇÃO DOS AMBIENTES EXPERIMENTAIS

Os experimentos foram organizados em dois ambientes distintos denominados de Ambiente Institucional e Ambiente Institucional e Internet.

Ambiente Institucional

O Ambiente Institucional consiste em uma rede local, situada no Laboratório de Bioinformática da UNIOESTE Campus Foz do Iguaçu (LABI/UNIOESTE), utilizando a tecnologia Gigabit Ethernet (802.3z) (31) e acesso a Internet de 100 Mbps provido pela Rede Nacional de Ensino e Pesquisa (RNP). Neste ambiente foram aplicados os elementos apresentados na Figura 15.

O vídeo utilizado para o experimento foi gerado por meio da Filmadora Digital JVC Everio GZ HD 520 (Figura 15, componente A). O computador Emissor (Figura 15, componente B) foi responsável pelo envio de áudio e de vídeo para o Servidor (Figura 15, componente D), e este realiza a transmissão desses fluxos para o Cliente Local ETHERNET (Figura 15, componente E) e para o Cliente Local WIFI (Figura 15,

componente G).

A conexão do Cliente Local WIFI é realizada por meio de rede padrão 802.11b (20) com *Access Point TP Link TL-WA 901ND* 54 Mbps (Figura 15, componente F).

O Emissor, o Servidor e o Cliente Local ETHERNET se conectam a rede Gigabit Ethernet (802.3z) (Figura 15, componente C) por meio de cabos *Unshielded Twisted Pair* (UTP) Categoria 6.

Neste ambiente, os experimentos foram realizados usando vídeo e áudio com as seguintes propriedades:

- Resolução 1024 x 768 *pixels*;
- Taxa de 25 Quadros por Segundo (QPS);
- *Bitrate* de vídeo com 13000 Kbps, correspondente a qualidade de imagens geradas pelo videocolonocopio marca Fuginon modelo 4400 com resolução de 1024 x 768 *pixels* e com 25 QPS;
- Qualidade de transmissão 100% e sem utilização de técnicas de compactação;
- *Codec* de vídeo *Sorenson Spark* (120);
- *Codec* de áudio *Speex* (121);
- *Bitrate* de áudio com 34.2 Kbps.

Esse ambiente experimental foi definido com o propósito de analisar o comportamento do método em redes locais.

Ambiente Institucional e Internet

O Ambiente Institucional e Internet é composto pelo Ambiente Institucional, apresentado anteriormente e, adicionalmente, possui três clientes situados na Internet.

Para melhor compreensão, na Figura 16 estão ilustrados os componentes presentes neste ambiente, de modo integral. Os três clientes adicionais são representados por:

- Cliente A (Figura 16, componente K) está situado em uma Instituição que compartilha um link de Internet de 1 Gbps provido pela RNP;

Cliente B (Figura 16, componente L) está localizado em um departamento que compartilha um *link* interno de 100 Mbps e faz parte de uma Instituição que possui um *link* de Internet de 1 Gbps provido pela RNP;

Figura 15: Componentes do Ambiente Institucional.

- Cliente ADSL (Figura 16, componente M) apresenta *link* de Internet residencial ADSL de 15 Mbps provido pela empresa de telefonia GVT[10].

Neste ambiente, os experimentos foram realizados utilizando-se de fluxos de vídeo e de áudio com as seguintes propriedades:

- Resolução 480 x 360 *pixels*;
- Taxa de 25 quadros por segundo (QPS);
- *Bitrate* de vídeo com 6000 Kbps, correspondente a qualidade de imagens geradas pelo videocolonocópio de marca Fuginon modelo 4400 com resolução de 480 x 360 *pixels* e com 25 QPS;
- Qualidade de transmissão 100% e sem utilização de técnicas de compactação;
- *Codec* de vídeo *Sorenson Spark* (120);
- *Codec* de áudio *Speex* (121);
- *Bitrate* de áudio com 34.2 Kbps.

[10]< http://www.gvt.com.br/portal/siebel8/residencial/index.jsp>.

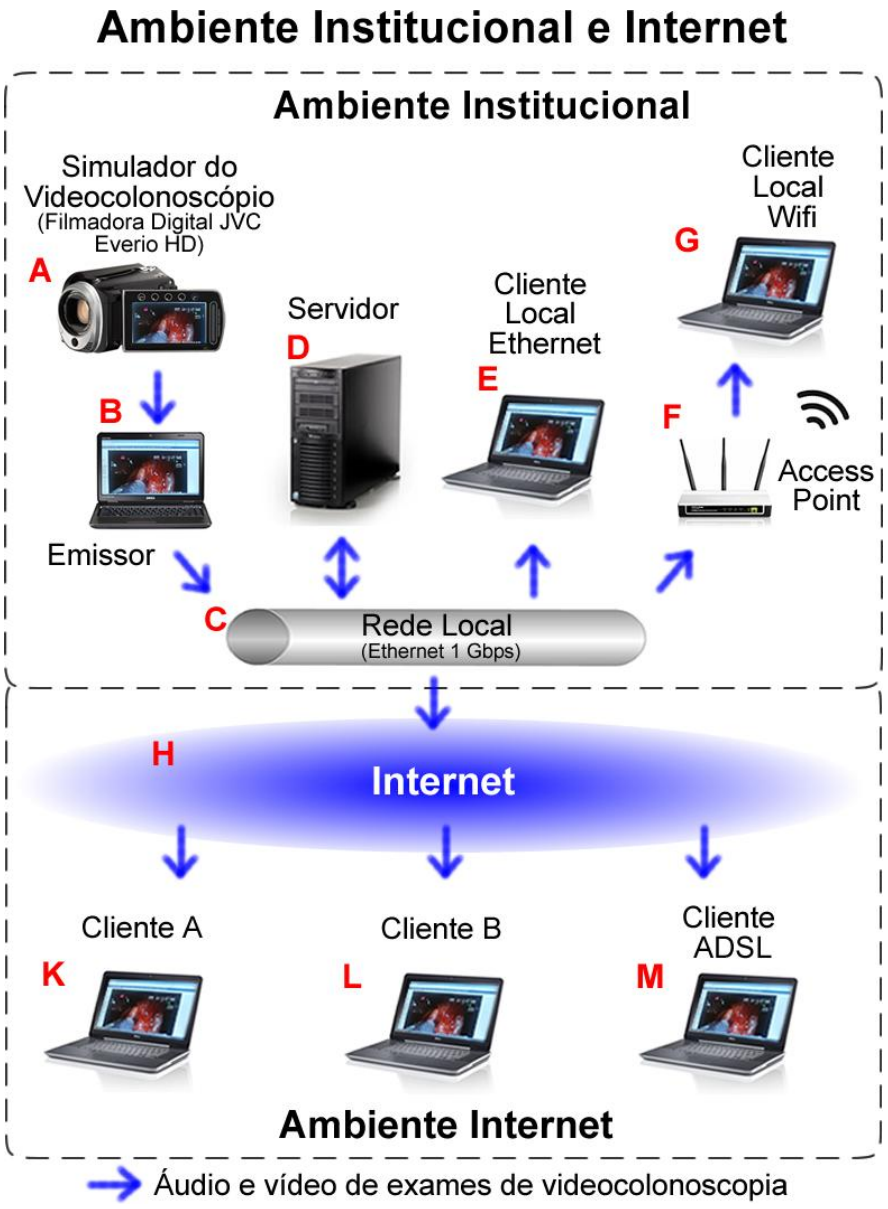

Figura 16: Componentes do Ambiente Institucional e Internet.

4.4.3.2. ETAPAS EXPERIMENTAIS

O delineamento experimental foi estabelecido de acordo com as seguintes etapas:

1. Definição das datas e horários para a realização dos experimentos;
2. Geração dos vídeos a serem utilizados nos experimentos;
3. Desabilitação de processos de *software*;
4. Iniciação do servidor;

5. Configuração do *software* VCam;
6. Iniciação e configuração do Emissor;
7. Iniciação dos clientes;
8. Procedimento de transmissão de áudio e vídeo;
9. Armazenamento dos resultados;
10. Finalização do experimento;
11. Análise estatística.

Etapa 1 - Definição das datas e horários para a realização dos experimentos

Os experimentos foram realizados durante os dias úteis de uma semana, de segunda a sexta feiras, duas vezes por período de acordo com os seguintes horários: 10h00, 11h00, 15h00 e 16h00. Cada experimento teve duração de 30 minutos e os dados referentes à QPS coletados uma vez a cada segundo, totalizando 1800 valores por experimento.

Etapa 2 - Geração dos vídeos utilizados nos experimentos

Para a geração dos vídeos foram realizados os passos abaixo:

- Execução do vídeo do exame de videocolonoscopia no computador Emissor;
- Filmagem e adaptação do filme real de videocolonoscopia por meio da filmadora digital JVC Everio GZ HD 520 às configurações definidas e aplicadas no Ambiente Institucional e no Ambiente Institucional e Internet;
- Cópia dos vídeos gerados pela filmadora no computador Emissor para serem utilizados nos experimentos.

Etapa 3 - Desabilitação de processos de *software*

Nesta etapa, antes de começar a execução dos experimentos, todos os processos que não haviam sido iniciados pelo sistema operacional foram finalizados. Esse procedimento foi realizado em todos os computadores utilizados nos experimentos e, após, iniciou-se o Servidor.

Etapa 4 - Iniciação do servidor

Nessa fase foi definido o endereço Internet Protocol (IP) do Servidor (1, 36). Para os experimentos realizados no Ambiente Institucional aplicou-se o endereçamento demonstrado na Figura 17 (A) e para os experimentos realizados no Ambiente Institucional e Internet ajustou-se o endereçamento apresentado na Figura 17 (B). Essas configurações foram definidas no arquivo **/etc/networtk/interfaces,** sendo necessária prioridade de usuário administrador para realizar a processo.

Depois da definição dos endereçamentos, o servidor de *Streams* Red5 1.0 RC1 (113) foi acionado conforme demonstrado por meio da Figura 18.

Etapa 5 - Configuração do *software* VCam

O *software* VCam foi utilizado como dispositivo de entrada de vídeo, simulando o equipamento videocolonoscópico. Os arquivos de vídeo utilizados foram os definidos na Etapa 2 desta seção, e a tela do *software* VCam, ilustrada por meio da Figura 19.

O processo de adição do vídeo referente ao Ambiente Institucional e ao Ambiente Institucional e Internet estão apresentados nas Figura 20 e Figura 21, respectivamente.

A

```
auto eth0
iface eth0 inet static
        address 192.168.10.100
        netmask 255.255.255.0
        gateway 192.168.10.1
```

B

```
auto eth0
iface eth0 inet static
        address 186.233.12.15
        netmask 255.255.255.128
        gateway 186.233.12.1
```

Figura 17: (A) Configurações IP para o Ambiente Institucional e (B) Configurações IP para o Ambiente Institucional e Internet.

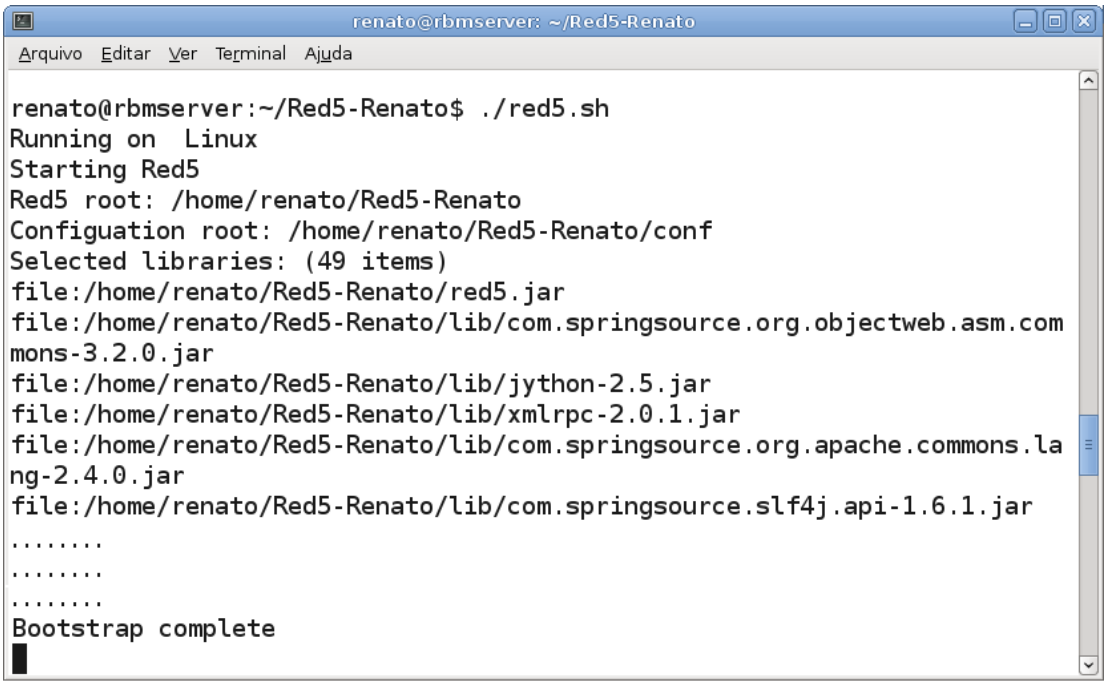

Figura 18: Iniciação do RED5 no Servidor de Aplicação.

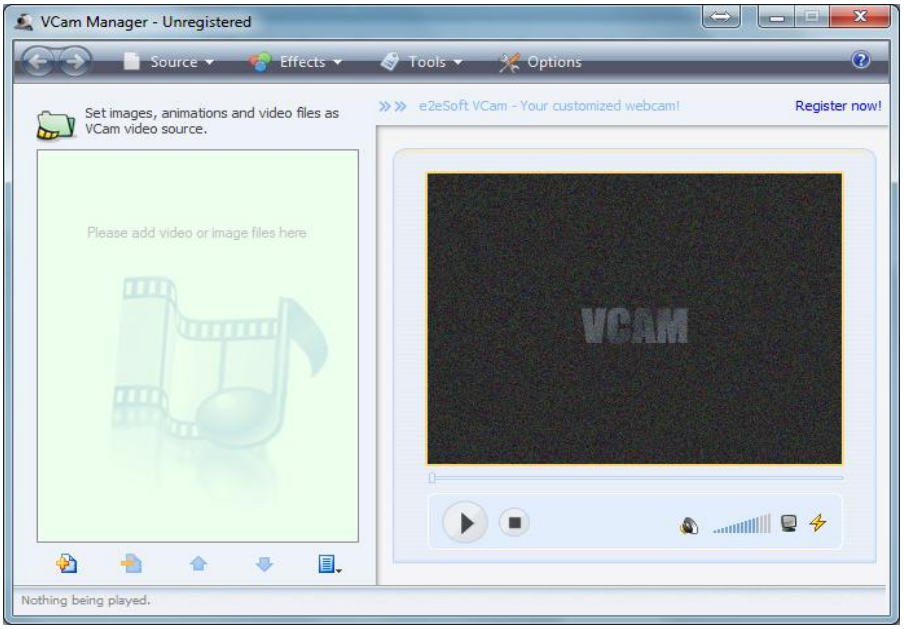

Figura 19: Iniciação do *Software* VCam.

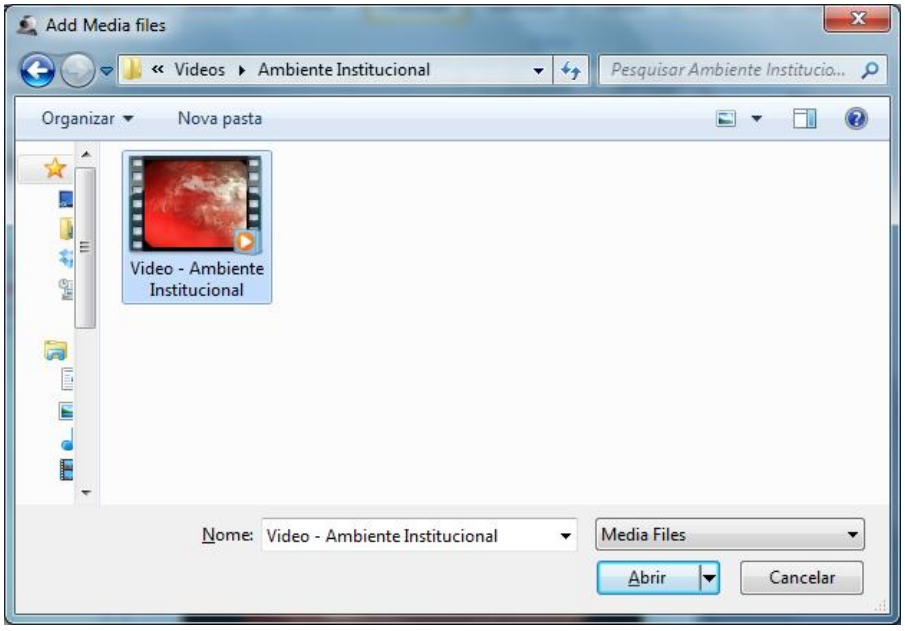

Figura 20: Escolha do Vídeo Referente ao Ambiente Institucional.

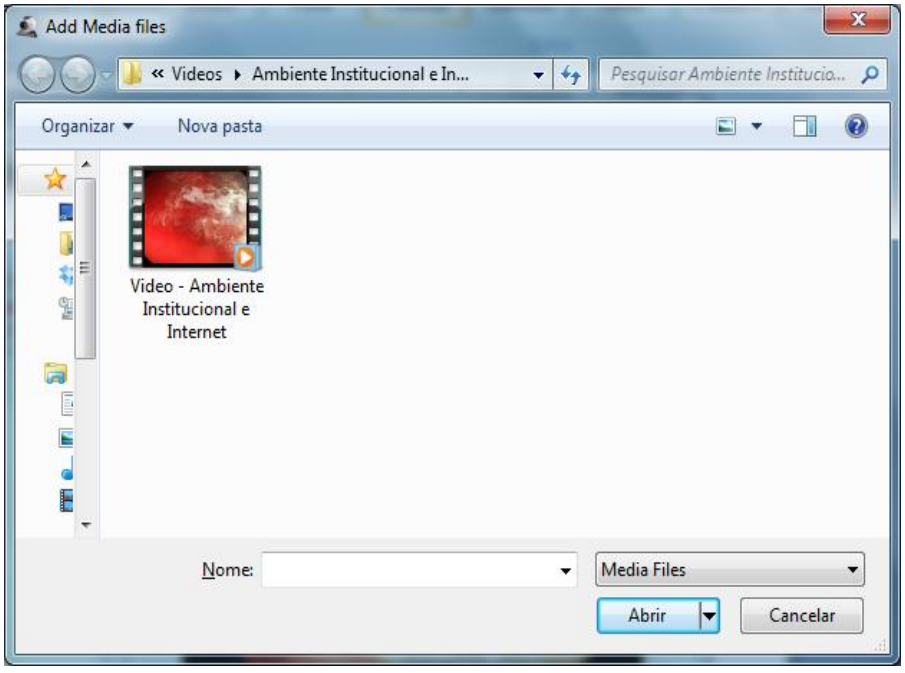

Figura 21: Escolha do Vídeo Referente ao Ambiente Institucional e Internet.

Etapa 6 - Iniciação e configuração do Emissor

O primeiro passo, nesta etapa, foi caracterizado pela configuração do dispositivo de áudio. Para isso, utilizou-se de um cabo de áudio Tip-Ring-Sleeve (TRS) conectado à saída de som do computador auxiliar ao microfone do computador Emissor.

O passo seguinte consistiu em iniciar o navegador Internet Mozilla Firefox versão 18.0.2 com *plugin Shockwave Flash* 11.5 r502 e Java (TM) Platform SE 7 U13.

Após esse processo, foi então acionada a aplicação por meio do endereço **192.168.10.100:5080/Telemedicina/Sistema.html** para o Ambiente Institucional ou do endereço **186.233.12.15:5080/Telemedicina/Sistema.html** para o Ambiente Institucional e Internet. Logo em seguida à entrada da aplicação, os dispositivos de áudio e de vídeo foram definidos acionando-se o botão direito do mouse e selecionando-se a opção menu Configurações (Figura 22).

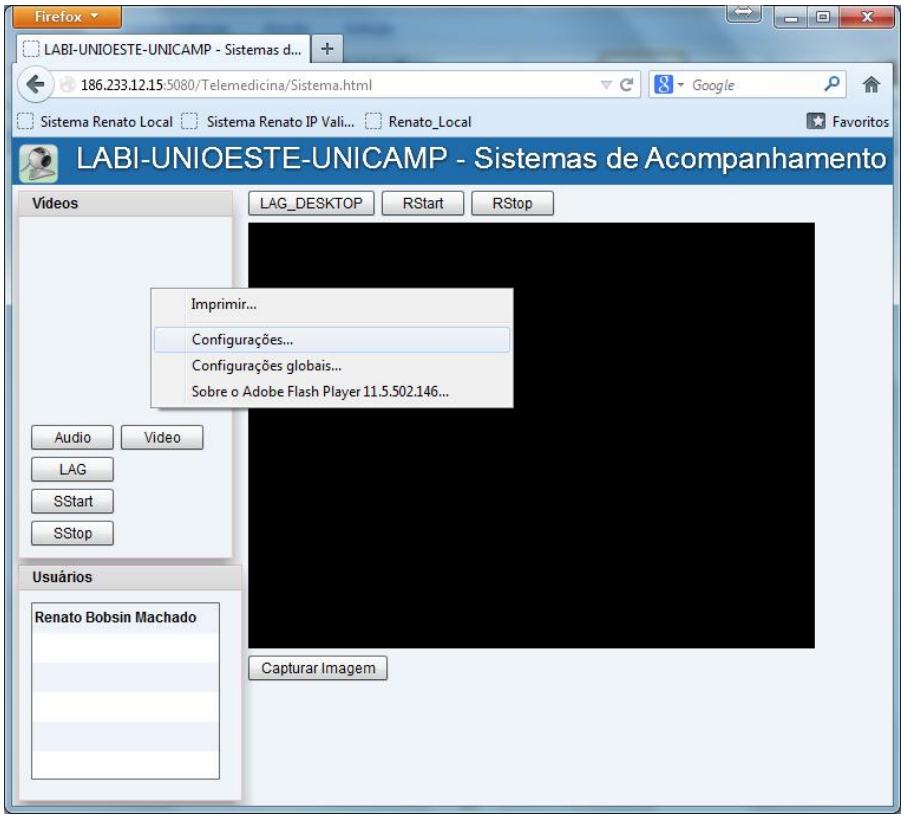

Figura 22: Configuração dos Dispositivos de Vídeo e Áudio.

Etapa 7 - Iniciação dos clientes

No ambiente Institucional foram utilizados os clientes Local ETHERNET e Local WIFI. Já no Ambiente Institucional e Internet, os clientes foram caracterizados pelo Local ETHERNET, Local WIFI, cliente remoto A, cliente remoto B e cliente remoto ADSL. Os clientes remotos foram acessados e configurados remotamente por meio do *software* TeamViewer 8.0[11].

A iniciação da aplicação, em todos os clientes, foi realizada seguindo os mesmos procedimentos definidos para a iniciação do computador Emissor e esta ação está ilustrada na Figura 22.

Etapa 8 - Procedimento de transmissão de áudio e vídeo

Este procedimento consiste em acionar os botões **Áudio** e **Vídeo** no computador Emissor (Figura 22). A partir desse momento, o áudio e o vídeo são enviados pelo Emissor para o Servidor de Aplicação (SA) e deste para todos os outros Clientes.

Com a abertura da aba Configurações, a câmera **e2eSoft VCam,** que corresponde a entrada de vídeo por meio do *software* VCam, foi acionada (Figura 23 - A), assim como a entrada de áudio representada pela seleção do microfone do próprio computador Emissor (Figura 23 - B).

Etapa 9 - Armazenamento dos resultados

Os dados dos experimentos foram armazenados, automaticamente, por 30 minutos. Para salvar esses dados capturados em arquivos texto, foi necessário acionar os botões **SStop** e **RStop** nos computadores Emissor e Clientes, respectivamente. Os dados armazenados representam a taxa de QPS enviada pelo Emissor e recebida em cada cliente.

Etapa 10 - Finalização do experimento

A finalização do experimento consiste no fechamento, no Emissor e em todos os Clientes, do navegador Internet Mozilla Firefox versão 18.0.2.

A B

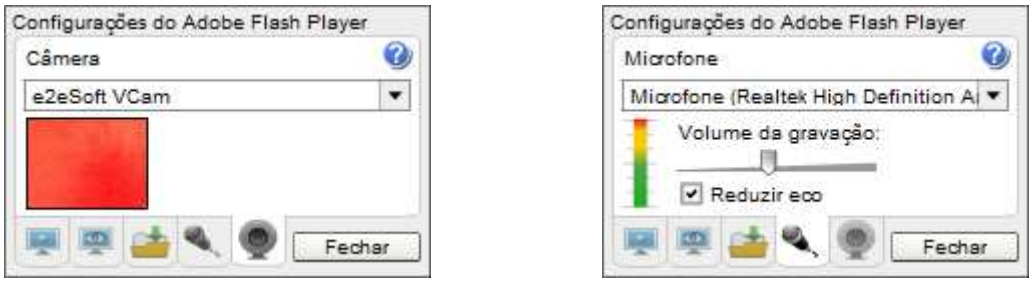

Figura 23: A) Escolha do Dispositivo de Vídeo. B) Escolha do Dispositivo de Áudio.

Etapa 11 - Análise estatística

Conforme o protocolo experimental, todos os dados de QPS obtidos pelo Emissor e pelos Clientes foram submetidos às análises estatísticas descritivas e analíticas. Para todas as análises realizadas fixou-se a rejeição da hipótese de nulidade para o p-valor $\leq 0,05$.

4.4.4. EXPERIMENTAÇÃO PARA A AVALIAÇÃO DE CONECTIVIDADE

Esta categoria de experimentos foi realizada para a validação do sistema computacional, envolvendo a avaliação das funcionalidades implementadas a partir da definição de requisitos. Para isso foi analisado o funcionamento dos processos de cadastro de entidades como Paciente, Profissional, Exames, Laudos e Auxiliares. Também foi verificada a comunicação e a aquisição de vídeos e imagens a partir de um videocolonoscópio *Fuginon* modelo VP-4400 (122) (Figura 24 - A). Para a captura de vídeo, empregou-se uma placa de captura *PixelView PlayTV Xtreme* com interface de vídeo S-Vídeo (Figura 24 - B) conectada ao computador Emissor (Figura 24 - C).

No SA aplicou-se, para o gerenciamento dos fluxos de áudio e de vídeo, o servidor de *Streaming* RED5 1.0 RC 1 (113). As imagens coletadas durante os experimentos foram armazenadas na BIV e os dados gravados na BD. Durante esses experimentos, utilizou-se como objeto para a obtenção de imagens videocolonoscópicas a região palmar da mão do

[11] <http://www.teamviewer.com/pt/index.aspx>.

autor (Figura 24 - D) e aplicada estrutura de rede *wireless* padrão 802.11b de 54 Mbps (120).

A **B** **C**

D

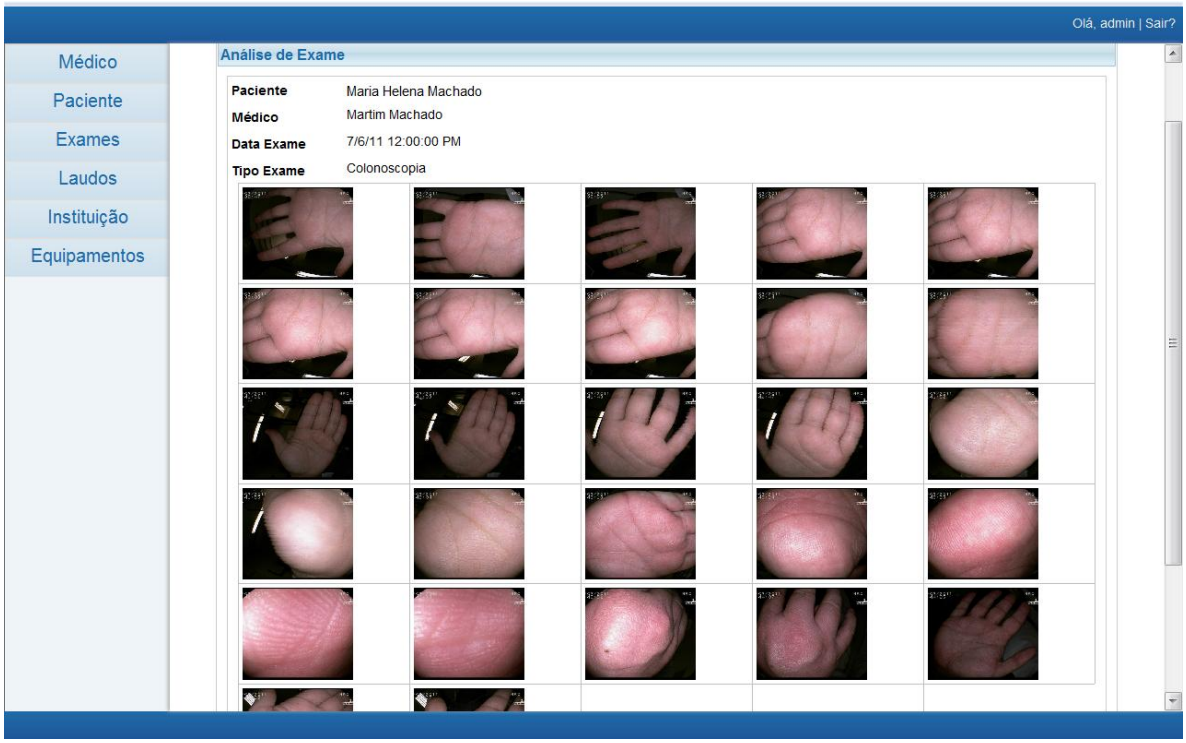

Figura 24: (A) Videocolonoscópio Fuginon 4400; (B) Placa de Captura de Vídeo PixelView PlayTV Xtreme; (C) Computador Core 2 Duo 2.2 GHz e (D) Tela com Imagens Capturadas da Região Palmar da Mão do Autor.

5. PATENTE BR 10 2012 033125 0

MÉTODO EM TELEMEDICINA PARA O ACOMPANHAMENTO REMOTO E EM TEMPO REAL DE PROCEDIMENTOS MÉDICOS

< Uso exclusivo do INPI >

INSTITUTO NACIONAL DA PROPRIEDADE INDUSTRIAL
PROTOCOLO GERAL
Manaíosa
26/12/2012 018120047754
VP21/12/2012
BR 10 2012 033125 0

Espaço reservado ao protocolo | Espaço para etiqueta

DEPÓSITO DE PEDIDO DE PATENTE OU DE CERTIFICADO DE ADIÇÃO

Ao Instituto Nacional da Propriedade Industrial:
O requerente solicita a concessão de um privilégio na natureza e nas condições abaixo indicadas

1. Depositante (71):

1.1 Nome: UNIVERSIDADE ESTADUAL DE CAMPINAS - UNICAMP

1.2 Qualificação PESSOA JURÍDICA DE DIREITO PÚBLICO, AUTARQUIA ESTADUAL

1.3 CNPJ/CPF: 460684250001/33

1.4 Endereço Completo CIDADE UNIVERSITÁRIA "ZEFERINO VAZ"

1.5 CEP: 13083-970 1.6 Telefone (19)35215015 1.7 Fax: (19)35215210

1.8 E-mail: patentes@inova.unicamp.br

☒ continua em folha anexa

2. Natureza: ◉ Invenção ○ Modelo de Utilidade ○ Certificado de Adição

Escreva, obrigatoriamente, e por extenso, a Natureza desejada: INVENÇÃO

3. Título da Invenção ou Modelo de Utilidade ou Certificado de Adição(54):
MÉTODO EM TELEMEDICINA PARA O ACOMPANHAMENTO REMOTO E EM TEMPO REAL DE PROCEDIMENTOS MÉDICOS

☐ continua em folha anexa

4. Pedido de Divisão: do pedido Nº Data de Depósito:

5. Prioridade: ☐ interna ☐ unionista
O depositante reivindica a(s) seguinte(s):

País ou organização de origem	Número de depósito	Data do depósito

6. Inventor (72):

☐ Assinale aqui se o(s) mesmo(s) requer(em) a não divulgação de seu(s) nome(s)

6.1 Nome: WU FENG CHUNG

6.2 Qualificação BRAS,CASADO,PROF. UNIVERSITÁRIO 6.3 CPF: 102.096.488-05

6.4 Endereço completo RUA LONTRA, 26, VILA A, EM FOZ DO IGUACU - PR

6.5 CEP: 85861-120 6.6 Telefone: 45 3521-4824 6.7 Fax:

6.8 E-Mail: wufengchung@gmail.com

☒ continua em folha anexa

608_TELEMEDICINA

INPI Formulário 1.01 – Depósito de Pedido de Patente ou de Certificado de Adição (folha 1/2)

7. Declaração na forma do item 3.2 do Ato Normativo nº 127/97:

☐ 7.1 Declaro que os dados fornecidos no presente formulário são idênticos ao da certidão de depósito ou documento equivalente do pedido cuja prioridade está sendo reivindicada.

☐ em anexo

8. Declaração de divulgação anterior não prejudicial: (Período de Graça):
(art. 12 da LPI e item 2 do AN nº 127/97) ☐ em anexo

9. Procurador (74)

9.1 Nome: FERNANDA LAVRAS COSTALLAT SILVADO

9.2 CNPJ/CPF: 295.166.068-57 9.3 API/OAB: 210.899

9.4 Endereço completo PROCURADORIA GERAL DA UNICAMP , EM CAMPINAS - SP

9.5 CEP: 13083-970 9.6 Telefone: (19)3521.4766 9.7 Fax: 19 3289.2245

9.8 E-Mail: proc-geral@pg.unicamp.br

10. Listagem de sequências Biológicas (documentos anexados) (se houver):

☐ Listagem de sequências em arquivo eletrônico: nº de CDs ou DVDs (original e cópia).

☐ Código de controle alfanumérico no formato de código de barras: fl.

☐ Listagem de sequências em formato impresso: fls.

☐ Declaração de acordo com o artigo da Resolução INPI nº 228/09: fls.

11. Documentos anexados (assinale e indique também o número de folhas):
(Deverá ser indicado o nº total de somente uma das vias de cada documento)

☒	11.1 Guia de Recolhimento	1 fls.	☒	11.5 Relatório descritivo	29	fls.
☒	11.2 Procuração	2 fls.	☒	11.6 Reivindicações	6	fls.
☐	11.3 Documentos de Prioridade	fls.	☒	11.7 Desenhos	3	fls.
☐	11.4 Doc. de contrato de trabalho	fls.	☒	11.8 Resumo	1	fls.
☐	11.9 Outros que não aqueles definidos no campo 11 (especificar)					fls.

12. Total de folhas anexadas (referentes aos campos 10 e 11): 42 fls.

13. Declaro, sob penas da Lei, que todas as informações acima prestadas são completas e verdadeiras.

CAMPINAS, SP, EM 18.12.2012
Local e Data

Assinatura e Carimbo
Fernanda Lavras Costallat Silvado
Procuradora da Universidade Subchefe
Matrícula nº 28.874-2
OAB/SP nº 210.899

INPI Formulário 1.01 – Depósito de Pedido de Patente ou de Certificado de Adição (folha 2/2)

< Uso exclusivo do INPI >

INPI INSTITUTO NACIONAL DA PROPRIEDADE INDUSTRIAL PROTOCOLO GERAL
mariahnm
05/02/2013 018130003552 14:41 DESP
0000221300695956

Espaço reservado ao protocolo

Espaço para etiqueta

PETIÇÃO - RELACIONADA COM PEDIDO, PATENTE OU CERTIFICADO DE ADIÇÃO

Ao Instituto Nacional da Propriedade Industrial:

1. Interessado

1.1 Nome: UNIVERSIDADE ESTADUAL DE CAMPINAS - UNICAMP

1.2 Qualificação: pessoa jurídica de direito público

1.3 CNPJ/CPF: 46068425000133

1.4 Endereço completo: Cidade Universitária "Zeferino Vaz"

1.5 CEP: 13083-970

1.6 Telefone: 19 3521-5015 1.7 Fax: 19 3521-5210 1.8 E-Mail: patentes@inova.unicamp.br

☒ continua em folha anexa

2. Título da Invenção, do Modelo de Utilidade ou Certificado de Adição:

MÉTODO EM TELEMEDICINA PARA O ACOMPANHAMENTO REMOTO E EM TEMPO REAL DE PROCEDIMENTOS MÉDICOS

☐ continua em folha anexa

3. Natureza ◉ 3.1 Invenção ○ 3.2 Certificado de Adição ○ 3.3 Modelo de Utilidade

4. Referência

☒ 4.1 Pedido

☐ 4.2 Patente | 4.3 Nº BR1020120331250 | 4.4 Data: 21.12.2012

5. Procurador (74)

5.1 Nome: FERNANDA LAVRAS COSTALLAT SILVADO

5.2 CNPJ/CPF: 295.166.068-57 5.3 API/OAB: 210.899

5.4 Endereço Completo: PROCURADORIA GERAL DA UNICAMP, CAMPINAS - SP

5.5 CEP: 13083-970

5.6 Telefone: 19 3521-4766 5.7 Fax: 19 3289-4766 5.8 E-mail:proc-geral@pg.unicamp.br

6. Apresentação ou modificação da Listagem de Sequências Biológicas (documentos anexados)(se houver):

☐ Listagem de sequências em arquivo eletrônico: nº de CDs ou DVDs (original e cópia).

☐ Código de controle alfanumérico no formato de código de barras: fls.

☐ Listagem de sequências em formato impresso: fls.

☐ Declaração de acordo com o artigo da Resolução INPI nº 228/09: fls.

INPI **Formulário 1.02 – Petição ou Requerimento, relacionado com pedido, patente ou certificado de adição (folha 1/2)**

7. Apresenta / Requer (continuação)

(Assinale o(s) itens que se aplica(m) ao seu caso):

(deverá ser indicado o nº total de somente uma das vias de cada documento)

		O que se requer / apresenta	folhas
☐	7.1	Modificações no Relatório Descritivo	
☐	7.2	Modificações nas Reivindicações	
☐	7.3	Modificações nos Desenhos	
☐	7.4	Modificações no Resumo	
☐	7.5	Caducidade da Patente/Certificado de Adição	
☐	7.6	Contestação de Caducidade/Nulidade	
☐	7.7	Cópia Oficial do pedido depositado	
☐	7.8	Cumprimento ou Contestação de Exig. RPI , de	
☐	7.9	Desarquivamento, arquivado na RPI , de	
☐	7.10	Documento de Prioridade	
☐	7.11	Exame do pedido com reivindicações	
☐	7.12	Expedição da Carta Patente / Certificado de Adição	
☒	7.13	Guia(s) de Recolhimento (uma para cada serviço)	1
☐	7.14	Manifestação s/ Parecer RPI , de	
☐	7.15	Nulidade do Patente / Certificado de Adição	
☒	7.16	Procuração	1
☐	7.17	Publicação Antecipada	
☐	7.18	Recurso contra o Indeferimento	
☐	7.19	Recurso, (outros)	
☐	7.20	Renúncia da Patente	
☐	7.21	Restauração de pedido / patente	
☐	7.22	Retirada do pedido	
☐	7.23	Subsídios ao Exame Técnico	
☐	7.24	Oferta de Licença	
☒	7.25	Outros que não aqueles definidos no campo 6 (especificar): ORDEM CORRETA DOS INVENTORES - EM DUAS VIAS	01

8. Total de folhas anexadas (referentes aos campos 6 e 7): 3 **fls.**

9. Declaro, sob penas da Lei, que todas as informações acima prestadas são completas e verdadeiras.

CAMPINAS, SP, EM 04 DE FEVEREIRO DE 2013

Local e Data

Assinatura e Carimbo

Fernanda Lavras Costallat Silvado
Procuradora de Universidade Subchefe
Matrícula nº 28.574-2
OAB/SP nº 210.8[illegible]

INPI Formulário 1.02 – Petição ou Requerimento, relacionado com pedido, patente ou certificado de adição (folha 2/2)

1 Continuação dos dados do depositante/interessado:

1.2 Qualificação: UNIVERSIDADE ESTADUAL DE CAMPINAS – UNICAMP, pessoa jurídica de direito público, autarquia estadual devidamente inscrita no CNPJ sob nº 46.068.425/0001-33 e isenta de inscrição estadual.

1.4 Endereço completo: Cidade Universitária "Zeferino Vaz" – Distrito de Barão Geraldo, em Campinas – SP – CEP 13083-970

INOVA, em 04 de Fevereiro de 2013

Ao
INPI – INSTITUTO NACIONAL DA PROPRIEDADE INDUSTRIAL

Em relação ao processo abaixo:

21.12.12 – BR 10 2012 033125 0
MÉTODO EM TELEMEDICINA PARA O ACOMPANHAMENTO REMOTO E EM TEMPO REAL DE PROCEDIMENTOS MÉDICOS
WU FENG CHUNG, CLÁUDIO SADDY RODRIGUES COY, RENATO BOBSIN MACHADO, HUEI DIANA LEE, JOÃO JOSÉ FAGUNDES, ANDRÉ GUSTAVO MALETZKE, CARLOS ANDRÉS FERRERO, RAQUEL FRANCO LEAL, MARIA DE LOURDES SETSUKO AYRIZONO, EVERTON ALVARES CHERMAN e WILLIAN ZALEWSKI
FCM/UNIOESTE

Solicitamos a inserção dos inventores na ordem correta, que é a seguinte: RENATO BOBSIN MACHADO, WU FENG CHUNG, HUEI DIANA LEE, CLÁUDIO SADDY RODRIGUES COY, JOÃO JOSÉ FAGUNDES, JOYLAN NUNES MACIEL, RICHARDSON FLORIANI VOLTOLINI, ANDRÉ GUSTAVO MALETZKE, RAQUEL FRANCO LEAL e MARIA DE LOURDES SETSUKO AYRIZONO.

Atenciosamente

Fernanda Lauras Costallat Silvado
Procuradora de Universidade Subchefe
Matrícula nº 28.574-2
OAB/SP nº 210.899

Rua Roxo Moreira, 1831, Cidade Universitária "Zeferino Vaz" – Distrito de Barão Geraldo - CEP 13083-970 - Campinas - SP
Fone (19)3521-5015 - Fax (19)3521-5210
E-mail: ciro@inova.unicamp.br - http://www.inova.unicamp.br

MÉTODO EM TELEMEDICINA PARA O ACOMPANHAMENTO REMOTO E EM TEMPO REAL DE PROCEDIMENTOS MÉDICOS

Campo da invenção

O presente pedido de patente de invenção se refere a um novo método para o acompanhamento remoto de procedimentos médicos no âmbito da Telemedicina, em tempo real, de modo interativo e iterativo.

Possui aplicabilidade voltada para a realização de exames complementares, cirurgias por videolaparoscopia e demais procedimentos médicos baseados em equipamentos hospitalares.

Fundamentos da invenção

Atualmente, diversos recursos tecnológicos estão disponíveis para hospitais e clínicas, principalmente no que se refere ao registro de informações, em bases de dados, sobre pacientes e sobre exames complementares. No entanto, importantes tarefas para a otimização de processos e para a redução de custos ainda não estão automatizadas ou não são amplamente acessíveis, devido principalmente à falta de recursos computacionais. Como exemplo, pode-se citar a captura, o acompanhamento e a análise de exames e de procedimentos que trabalham com vídeos e imagens, tais como endoscopia, colonoscopia, laparoscopia, entre outros.

Especificamente em relação a aplicações para a área médica, uma importante característica é a adoção de padrões para o armazenamento de imagens. Além disso, há uma carência por recursos tecnológicos que permitam aos médicos e especialistas acompanhar procedimentos médicos e realizar a sua análise remotamente, em tempo real, e de modo interativo e iterativo.

Desse modo, é importante o delineamento de métodos computacionais que possam auxiliar nesses processos. A Telemedicina é definida pela *American Telemedicine Association* – ATA como a utilização da troca de informações médicas entre lugares distintos por meio da comunicação eletrônica a fim de melhorar o estado de saúde do paciente. Já de acordo

com Current Medical Diagnosed & Treatment 2000, Telemedicina é "o uso de informação eletrônica e outras tecnologias de comunicação para proporcionar e dar suporte à saúde quando a distância separa os participantes do processo".

A partir da identificação dessas possibilidades de melhorias e das contribuições que podem ser alcançadas para a área médica, definiu-se, por meio desta invenção, um modelo aplicando recursos tecnológicos para auxiliar no acompanhamento, em tempo real, de procedimentos da área médica.

Atualmente, no estado da técnica, existem diversos trabalhos que se valem do conceito da telemedicina para desenvolver tecnologias que visam auxiliar a atividade médica. No entanto, até o presente momento não foi desenvolvida uma metodologia com a finalidade de viabilizar o acompanhamento e a discussão, em tempo real, sobre procedimentos médicos juntamente com a comunicação de equipamentos médicos baseados em vídeos e imagens.

A titulo de se determinar o estado da técnica e fundamentar o presente pedido de patente de acordo com o item 15.1.2 do Ato normativo 127/97 do INPI, segue abaixo uma relação de patentes e pedidos de patentes e artigos que versam sobre a mesma área do conhecimento do presente pedido de patente.

O pedido de patente US2011106557-A1 consiste em uma ferramenta, denominada de ihasClinic para interação e monitoramento remoto, em tempo real, entre pacientes, profissionais de saúde e outros. É possível armazenar dados e registros dos pacientes no servidor e localmente. Pode também ser usado para agendar ou alterar agendamentos de consultas. A arquitetura desse invento é composta por um servidor central e web browser. No servidor central encontram-se os dados do paciente e por meio de uma página web é possível haver a interação (áudio e vídeo), em tempo real, entre o paciente e o médico, bem como o acesso aos dados. O invento existente não pode ser utilizado para o acompanhamento e a interação de profissionais de saúde para a realização de um procedimento médico em tempo real. Nesse pedido não são tratadas imagens e vídeos provenientes de equipamentos

médicos, tais como o videocolonoscópio. A videoconferência na invenção existente é utilizada para a comunicação entre médicos e pacientes e não para a transmissão de vídeos relativos a procedimentos médicos, em tempo real. Não há mecanismos para a captura e compartilhamento de imagens a partir de qualquer fluxo de vídeo, sendo limitado a cada participante capturar imagens locais e disponibilizá-las para os demais. Em relação ao modo de armazenamento de imagens e dados de pacientes, não são aplicadas padronizações definidas para esta área, como é o caso do formato Dicom. A base de dados não foi projetada, na invenção existente, para a realização futura de análise inteligente de dados. Resumidamente, trata-se de uma tecnologia distinta em relação ao presente pedido, tanto em sua metodologia quanto em sua finalidade.

A patente TW400503(B) apresenta um método para a comunicação entre as estações de monitoramento central e as estações de monitoração de pacientes, encapsulando os dados (vídeo, áudio e dados de equipamentos) em pacotes, podendo utilizar múltiplos tipos de arquiteturas de redes. A comunicação com os equipamentos hospitalares é utilizada por meio de dispositivos seriais, USB, entre outros. Equipamentos normalmente utilizados são medidores de pressão, termômetros e eletrocardiogramas. Tanto no local como na estação remota são utilizados equipamentos de videoconferência, sendo o sistema responsável por separar e enviar os distintos tipos de dados para os destinos corretos. Embora ambas as invenções apliquem recursos de multimídia e de videoconferência, a invenção proposta possui o diferencial de permitir o acompanhamento local e remoto, em tempo real, de procedimentos médicos, principalmente os baseados em vídeos e imagens. Por meio dessa característica da invenção proposta, os profissionais podem realizar uma participação ativa na realização de tais procedimentos, podendo não só se comunicarem, mas também capturarem e compartilharem imagens relativas ao procedimento em execução (método LABI-IMAGE-SHARING, definido na invenção proposta). A parte de videoconferência da invenção existente utiliza equipamentos normalmente aplicados para este fim,

não possuindo recursos para a transmissão de vídeos provenientes de equipamentos médicos, como é o caso da invenção proposta. Outra característica da invenção proposta consiste no armazenamento das imagens provenientes dos procedimentos médicos conforme o padrão Dicom, e na disponibilização de um método para a autenticação e a comunicação segura para a execução de todos os processos e na construção de uma base de exames e imagens para a aplicação futura de métodos de inteligência computacional.

Em relação ao artigo científico SILVA, J. C. F.; VIEIRA, E.; PASSOS, M.; MELO, E. A.; MOTTA, G. H. M. B.; TAVARES, T. A.; SOUZA FILHO, Guido Lemos de. "Uma Ferramenta para Vídeo Colaboração em Saúde". In: *Congreso Argentino de Informática y Salud* 2011, 2011, Córdoba Argentina. Proceedings of CAIS 2011, 2011, este consiste em uma solução computacional para o acompanhamento de cirurgias. No trabalho, têm-se definidas duas salas, sendo uma no local de cirurgia e outra em uma sala de Telemedicina. O objetivo foi permitir a utilização desses recursos para que alunos e residentes pudessem acompanhar e interagir, por meio de áudio e vídeo, durante a cirurgia sem estar na sala onde o procedimento ocorre. No trabalho foram utilizados recursos multimídia de vídeo e áudio. Para isso foi instalada uma câmera na sala de cirurgia e outra na sala de Telemedicina. Os presentes na sala de Telemedicina podiam acompanhar tanto o vídeo da sala de Cirurgia quando vídeos de câmeras internas utilizadas no procedimento cirúrgico. A interatividade entre as duas salas foi definida por meio de áudio e vídeo. Também foram definidas técnicas criptográficas para a transmissão dos fluxos das mídias. Na invenção proposta são disponibilizados recursos para o acompanhamento remoto de procedimentos médicos, incluindo a possibilidade de acompanhamento, em tempo real, de vídeos e imagens provenientes de equipamentos hospitalares. Também são definidos recursos (vídeo, áudio e texto) para a discussão acerca de procedimentos médicos, também em tempo real, entre os participantes presentes no local de execução e em locais remotos. No contexto da invenção proposta podem-se ter múltiplos locais de

acompanhamento. Outra diferença consiste nos mecanismos de interação. Na invenção proposta é possível interagir não somente por áudio e vídeo, mas pode-se também participar ativamente do procedimento médico por meio da captura e compartilhamento de imagens, tanto local quanto remotamente. Além de processos cirúrgicos, a invenção proposta possui mecanismos para o gerenciamento de dados e exames de pacientes, permitindo o armazenamento em formato padronizado pela área médica. Na invenção proposta também foram disponibilizados recursos para a análise posterior dos procedimentos, assim como emissão de laudos e a realização de diagnósticos.

O presente pedido de patente destaca-se do estado da técnica, pois permite o acompanhamento e a discussão, em tempo real, sobre procedimentos médicos, havendo um método de comunicação com equipamentos médicos baseados em vídeos e imagens. Para isso tem-se um ambiente colaborativo que permite acompanhar vídeos de exames durante a sua realização, além do compartilhamento de vídeos, áudio, chat e captura e compartilhamento de imagens, dos equipamentos médicos durante a realização do procedimento, de modo remoto e interativo. Para a realização destes procedimentos os participantes são autenticados e os dados transmitidos são criptografados usando um método baseado em Sistemas Imunológicos Artificiais. A política de segurança foi definida por meio de uma inovação realizada pelo grupo de pesquisa e denominada método LABI-SIA, que será objeto de pedido de patente independente. Os dados e imagens dos exames podem ser exportados para o formato Dicom. Também é alimentada uma base de dados estruturada com o histórico de pacientes e exames, permitindo a aplicação futura de métodos para a análise inteligente de dados.

Os principais diferenciais da tecnologia proposta são: a) Recursos para o acompanhamento tanto local quanto remoto, em tempo real, de procedimentos médicos. Desse modo os participantes podem ter acesso, por meio da Internet, aos fluxos de vídeo, áudio e dados provenientes de equipamentos hospitalares; b) Adicionalmente são disponibilizados recursos que permitem aos participantes, locais e remotos, discutirem acerca do

procedimento médico por meio de recursos multimídia, incluindo vídeo, áudio e texto. Essa interatividade pode ser utilizada tanto durante a realização dos procedimentos médicos quanto após o término dos mesmos; c) Os participantes, local e remotamente, podem participar ativamente durante a realização de procedimentos médicos capturando e compartilhando imagens relativas ao mesmo. Desse modo, os profissionais em qualquer parte do mundo, podem interagir e iteragir, por meio desses recursos tecnológicos. Esse método foi denominado nesta invenção como LABI-IMAGE-SHARING; d) Desenvolvimento de um método específico para a área de segurança, com o objetivo de preservar a privacidade dos dados dos pacientes e dos exames. Esse método, denominado LABI-SIA aplica princípios de Sistemas Imunológicos Artificiais e foram baseados em técnicas de segurança computacional e criptografia; e) Desenvolvimento de um algoritmo para a distribuição segura de fluxos de vídeo e áudio, denominado LABI-PUBLISH.

Breve descrição da invenção

Refere-se o presente pedido de patente de invenção a um novo método computacional sistêmico em telemedicina cuja finalidade é permitir o acompanhamento remoto de procedimentos médicos no âmbito da Telemedicina, em tempo real e de modo interativo e iterativo; permitir que a realização desses procedimentos médicos possam ser realizados em locais onde não se tem a presença de médicos especialistas, sem prejudicar a eficácia do procedimento, e evitando em muitos casos a necessidade de deslocamento de pacientes até cidades distantes que disponham desses especialistas; permitir que médicos especialistas trabalhem, também de modo remoto, na análise e na elaboração de laudos e de diagnósticos, após a realização dos procedimentos médicos.

Para viabilizar o método de acompanhamento remoto, foi estruturado um sistema de telemedicina (Figura 1) constituído de um modelo de interação entre a Sala de Procedimentos Médicos (2_k onde k = 1..p e p = número total de salas de procedimento médico), no qual se encontram os pacientes e a equipe responsável pelo procedimento; e as Unidades de

Acompanhamento e Interação Remota (3_j onde j = 1..m e m = número total de clientes remotos), onde estão presentes médicos, profissionais da área da saúde e/ou pesquisadores. O método de interação foi projetado com o intuito de oferecer recursos para o acompanhamento, o auxílio e a interação remota, em tempo real, durante a realização de tais procedimentos. Para que seja possível essa interatividade são utilizados recursos presentes na Central de Gerenciamento de Procedimentos Médicos (4), incluindo o Servidor de Aplicação (5), o Banco de Dados (6), a Base de Imagens e Vídeos (7), o Módulo de Segurança Interna (8), a Rede Interna (9), o Módulo de Segurança Externa (11) e a Rede Externa (10).

Em termos gerais o método em telemedicina para o acompanhamento remoto, e em tempo real, de procedimentos médicos pode ser definido por meio de sete etapas, as quais são descritas a seguir.

Etapa 1: Disponibilização dos Serviços

A primeira etapa consiste na realização de configurações específicas do sistema de Telemedicina, a fim de disponibilizar os serviços necessários às Unidade(s) de Execução Local (13_i) e à(s) Unidade(s) de Acompanhamento e Interação Remota (3_j). Para isso são realizadas uma série de inicializações/configurações:

1. Inicialização do Servidor de *Streaming*;
2. Inicialização do Servidor de Bando de Dados;
3. Inicialização do Servidor de Páginas Web;
4. Inicialização do Módulo das Políticas de Segurança;
5. Aplicação das Configurações definidas para o Sistema de Telemedicina.

Etapa 2: Processo de Autenticação

O processo de autenticação é pré-requisito para o acesso a qualquer funcionalidade do sistema, e é executado sempre que um usuário se conecta ao sistema, tanto na(s) Unidade(s) de Execução Local (13_i) quanto na(s) Unidade(s) de Acompanhamento e Interação Remota (3_j). O algoritmo executado é apresentado na Figura 2.

Conforme demonstrado na Figura 2, a autenticação consiste em validar a identificação de um usuário (login) e de sua senha. Para essa validação, os dados de identificação (*login*) e senha são comparados com as informações armazenados na base de dados (de modo criptografado). Caso o processo de autenticação tenha sucesso, o usuário é adicionado a lista de usuários autenticados e conectados ao sistema. Em contrário a conexão do usuário ao sistema é rejeitada.

O sucesso no processo de autenticação é pré-requisito para que os usuários tenham acesso as funcionalidades do sistema.

Etapa 3: Inicialização da Unidade de Execução Local

Após a execução das etapas 1 e 2, a Unidade de Execução Local (13_i) realiza as seguintes ações:

1. Estabelece o Protocolo de Comunicação com o Equipamento Médico;
2. Estabelece conexão com o Servidor de Aplicação (5);
3. Inicia a aquisição de fluxos de vídeo e/ou áudio a partir do equipamento médico, conforme os algoritmos apresentados por meio das Figuras 3 e 4.

Conforme apresentado na Figura 3, para a aquisição de vídeo é iniciado um objeto para essa finalidade, e posteriormente são realizadas algumas configurações (definição do *codec* de vídeo, da resolução, da taxa de aquisição em quadros por segundo, da qualidade e do índice de compactação quando aplicável). Após tais definições é efetivamente iniciada a captura do vídeo.

Conforme apresentado na Figura 4, para a aquisição de áudio é iniciado um objeto para essa finalidade, e posteriormente são realizadas algumas configurações (definição do *codec* de áudio, da qualidade e do índice de supressão de *echo*). Após tais definições é efetivamente iniciada a captura do áudio.

4. A Unidade de Execução Local (13_i) disponibiliza esses fluxos de vídeo e/ou áudio para o Servidor de Aplicação (5), conforme os algoritmos apresentados por meio das Figuras 5 e 6.

Conforme apresentado na Figura 5, para a publicação de vídeo é iniciado um objeto para estabelecer uma canal de *stream* com o Servidor de Aplicação (5) (que também é servidor de *Stream*), é definida uma identificação (nome) para esse *stream*, é estabelecida a conexão com o Servidor de Aplicação (5), é alocado um canal de comunicação para a publicação do *stream* e por fim o vídeo é disponibilizado por meio deste canal.

Conforme apresentado na Figura 6, para a publicação de áudio é iniciado um objeto para estabelecer uma canal de *stream* com o Servidor de Aplicação (5) (que também é servidor de *Stream*), é definida uma identificação (nome) para esse *stream*, é estabelecida a conexão com o Servidor de Aplicação (5), é alocado um canal de comunicação para a publicação do *stream* e por fim o áudio é disponibilizado por meio deste canal.

Etapa 4: Acompanhamento Remoto de Procedimentos Médicos

Por meio da(s) Unidade(s) de Acompanhamento e Interação Remota (3_j) é possível acompanhar os procedimentos médicos, em tempo real. Para a realização desta etapa é necessária a realização da autenticação no sistema, conforme definido na Etapa 2.

Para cada nova Unidade de Acompanhamento e Interação Remota (3_j) que se conecta ao sistema, são executados os procedimentos a seguir.

1. O Servidor de Aplicação (5) atualiza a lista de conexões e envia essa lista para todas as conexões ativas, tanto para a Unidade de Execução Local (13_i) quanto para a(s) Unidade(s) de Acompanhamento e Interação Remota (3_j);

2. O Servidor de Aplicação (5) envia os dados relativos ao exame em execução para a nova Unidade de Acompanhamento e Interação Remota (3_j);

3. A nova Unidade de Acompanhamento e Interação Remota (3_j) estabelece uma conexão com o Servidor de Aplicação (5) e passa a receber os fluxos de vídeo e/ou áudio provenientes do exame em execução na Unidade de Execução Local (13_i);

4. A nova Unidade de Acompanhamento e Interação Remota (3_j) faz *download* e apresenta imagens relativas ao exame em execução, caso existam.

Etapa 5: Interatividade Durante a Realização de Procedimentos Médicos

Além do acompanhamento dos procedimentos médicos, a tecnologia proposta disponibiliza mecanismos para que os profissionais interajam, em tempo real, por meio de recursos de vídeo, áudio, mensagens texto; assim como capturando e compartilhando imagens relativas ao procedimento médico em execução. Para ter acesso a esse conjunto de funcionalidades também é necessário que o usuário esteja autenticado, conforme definido na Etapa 2. A seguir são apresentados os mecanismos empregados para cada um desses modos de interatividade.

Interação por meio de Vídeo

Para cada nova Unidade de Acompanhamento e Interação Remota (3_j) que disponibiliza o seu fluxo de vídeo, são executadas as seguintes ações:

1. A nova Unidade de Acompanhamento e Interação Remota (3_j) realiza o processo de aquisição do vídeo e a de sua publicação conforme descrito na Etapa 3, processos 3 e 4;

2. A partir de cada publicação de vídeo realizada, o Servidor de Aplicação (5) atualiza a lista de fluxos de vídeo;

3. O Servidor de Aplicação (5) envia uma mensagem para todas as conexões ativas com a identificação do novo fluxo de vídeo publicado, e com os dados do usuário e da nova Unidade de Acompanhamento e Interação Remota (3_j) que está compartilhando a mídia de vídeo;

4. Todas as Unidades de Acompanhamento e Interação Remota (3_j) e a Unidade de Execução Local (13_i), exceto a nova Unidade de Acompanhamento e Interação Remota (3_j) que está disponibilizando o novo fluxo de vídeo, criam um novo canal de comunicação para receber o novo fluxo de vídeo e passam a obter e apresentar esse vídeo.

Interação por meio de Áudio

Para cada nova Unidade de Acompanhamento e Interação Remota (3_j) que disponibiliza o seu fluxo de áudio, são executadas as seguintes ações:

1. A nova Unidade de Acompanhamento e Interação Remota (3_j) realiza o processo de aquisição do áudio e a sua publicação conforme descrito na Etapa 3, processos 3 e 4;

2. A partir de cada publicação de áudio realizada, o Servidor de Aplicação (5) atualiza a lista de fluxos de áudio;

3. O Servidor de Aplicação (5) envia uma mensagem para todas as conexões ativas com a identificação do novo fluxo de áudio publicado, e com os dados do usuário e da nova Unidade de Acompanhamento e Interação Remota (3_j) que está compartilhando a mídia de áudio;

4. Todas as Unidades de Acompanhamento e Interação Remota (3_j) e a Unidade de Execução Local (13_i), exceto a nova Unidade de Acompanhamento e Interação Remota (3_j) que está disponibilizando o novo fluxo de áudio, criam um novo canal de comunicação para receber o novo fluxo de áudio e passam a obter e reproduzir esse áudio.

Interação por meio de mensagens texto

Todas as Unidades de Acompanhamento e Interação Remota (3_j) e a Unidade de Execução Local (13_i) conectadas ao sistema possuem um mecanismo para a realização de troca de mensagens texto. Para cada mensagem texto enviada, a partir de uma Unidade de Acompanhamento e Interação Remota (3_j) ou da Unidade de Execução Local (13_i), são executados os seguintes procedimentos:

1. A mensagem texto e a identificação do usuário são enviados para o Servidor de Aplicação (5);

2. O Servidor de aplicação (5) encaminha a mensagem texto e a identificação do usuário para todas as Unidades de Acompanhamento e Interação Remota (3_j) ativas e para a Unidade de Execução Local (13_i);

3. Todas as Unidades de Acompanhamento e Interação Remota (3_j) e a Unidade de Execução Local (13_i) recebem e apresentam a mensagem texto e a identificação do usuário.

Interação por meio Imagens relativas ao Procedimento Médico em Execução

Qualquer participante, seja na Unidade de Execução Local (13_i) ou em alguma Unidade de Acompanhamento e Interação Remota (3_j), pode capturar imagens relativas ao procedimento médico em execução, e essas imagens são disponibilizadas, em tempo real, para todos os participantes. Quando uma imagem é capturada na Unidade de Execução Local (13_i) ou em qualquer Unidade de Acompanhamento e Interação Remota (3_j), são executados os seguintes procedimentos:

1. A imagem é transmitida para o Servidor de Aplicação (5);

2. O Servidor de Aplicação (5) armazena essa imagem na Base de Imagens e Vídeos (7);

3. O Servidor de Aplicação (5) comunica a localização da imagem, na Base de Imagens e Vídeos (7), para a conexão que capturou a imagem originalmente, seja na Unidade de Execução Local (13_i) ou na Unidade de Acompanhamento e Interação Remota (3_j);

4. A partir do local onde a imagem foi capturada, Unidade de Execução Local (13_i) ou a Unidade de Acompanhamento e Interação Remota (3_j), é enviada uma mensagem para todas as conexões ativas, ou seja, para as Unidades de Execução Local (13_i) e para as Unidades de Acompanhamento e Interação Remota (3_j) que possuam conexões ativas. O conteúdo dessa mensagem é a localização da imagem capturada na Base de Imagens e Vídeos (7);

5. A Unidade de Execução Local (13_i) e todas as Unidades de Acompanhamento e Interação Remota (3_j) recebem a mensagem, fazem *download* da imagem e a disponibilizam graficamente em uma área da tela destinada para imagens relativas ao procedimento médico em execução.

Etapa 6: Finalização do Procedimento Médico

Após o término do procedimento médico, são realizados os seguintes procedimentos:

1. A Unidade de Execução Local (13_i) encerra a publicação do(s) fluxo(s) de vídeo e/ou áudio;

2. O Servidor de Aplicação (5) comunica todas as Unidades de Acompanhamento e Interação Remota (3_j) ativas para encerrarem os canais de comunicação relativos ao recebimento de fluxos de áudio e/ou vídeo relativos ao procedimento médico;

3. Todas as Unidades de Acompanhamento e Interação Remota (3_j) fecham os canais de comunicação para recebimento de fluxos de vídeo e/ou áudio previamente estabelecidos para o acompanhamento do procedimento médico;

4. A Unidade de Execução Local (13_i) encerra a comunicação com o equipamento médico;

5. A Unidade de Execução Local (13_i) encerra a comunicação com o Servidor de Aplicação (5).

Etapa 7: Análise de Exames, Diagnósticos e Laudos

Além do acompanhamento e interação remota, em tempo real, o método proposto nesta invenção contempla funcionalidades que permitem aos profissionais acessarem remotamente dados relativos a pacientes e aos exames. Essas características podem ser utilizadas por meio das Unidades de Acompanhamento e Interação Remota (3_j) tendo como pré-requisito a autenticação no sistema definida na Etapa 2. Para isso o Servidor de Aplicação disponibiliza os seguintes recursos:

1. Cadastro, visualização e edição de dados de profissionais e pacientes;

2. Visualização de dados e imagens relativas a procedimentos médicos;

3. Criação, visualização e edição de laudos.

Foram desenvolvidos 2 softwares seguindo o modelo Cliente/Servidor. Desse modo ambos estão embarcados no Servidor de Aplicação (5) e são utilizados na Unidade de Execução Local (13) e nas Unidades de Acompanhamento e Interação Remota (3).

Nas invenções existentes e na literatura, os modelos que utilizam recursos multimídia normalmente aplicam somente dois locais, um deles onde o procedimento é realizado e o outro para o acompanhamento remoto. Normalmente esses recursos são aplicados para o paciente conversar com os profissionais da área da saúde, para residentes acompanharem procedimentos médicos, para questões educacionais, entre outros.

Em outras tecnologias, não há nenhuma interação durante a realização dos procedimentos médicos. Esses são realizados e armazenados em uma base de dados e posteriormente os médicos acessam remotamente para a realização de diagnósticos.

Desse modo os grandes diferenciais da invenção proposta são:

- Para um procedimento médico, tem-se o local onde o mesmo é realizado e pode-se ter **n** Unidades de Acompanhamento e Interação Remota. Esse **n** deve ser dimensionado em função dos recursos computacionais disponíveis, como capacidade dos computadores, quantidade de servidores, velocidade da conexão com a Internet, entre outros;
- Os profissionais remotos não somente acompanham, mas podem participar ativamente da realização do procedimento médico, discutindo com outros profissionais tanto locais quanto remotos. Para isso são aplicados recursos de vídeo, áudio e mensagens texto;

- Os profissionais, local e remotamente, além de discutirem, podem capturar imagens relativas aos procedimentos médicos. Essas imagens são automaticamente apresentadas a todos os participantes e também são armazenadas como parte do exame ou procedimento médico. O método para gerenciar essa captura e gerenciamento de imagens foi criado pelo grupo de pesquisa e foi denominado LABI-IMAGE-SHARING, que será pormenorizadamente descrito em pedido de patente independente;
- Após o término do procedimento, os dados e imagens podem ser exportados para o formato Dicom, o que não é realizado pelas soluções existentes, principalmente aplicadas a procedimentos com vídeo, como procedimentos endoscópicos e videolaparoscopia;
- Os dados relativos ao procedimento médico, após a realização dos exames, podem ser analisados e discutidos remotamente, facilitando a realização de análises, laudos e diagnósticos;
- Toda a solução funciona por meio da Internet e ambiente *Web*, sendo necessária apenas a utilização de *Browser* para acessar o sistema;
- Todo o processo de autenticação e transmissão dos dados foi definido por meio de camadas de segurança, com diversos procedimentos para proteger a privacidade dos participantes e dos dados relativos aos procedimentos médicos. Essa política de segurança foi definida criando-se um método denominado LABI-SIA. Nesse método, em todos os acessos com ou sem sucesso, o usuário recebe um relatório por email sobre a tentativa, local de onde tentou, se obteve sucesso ou não, senhas tentadas

erroneamente, e uma foto da pessoa/local onde o sistema está sendo utilizado;

- A base de dados foi definida e projetada para a aplicação futura de técnicas de análise inteligente de dados.
- O método também pode ser aplicado para objetivos educacionais, para que residentes possam acompanhar e interagir com os procedimentos médicos sem a necessidade de estar no local de execução, onde normalmente os espaços são reduzidos. Nesse também permitiria aplicações realizadas pelas tecnologias existentes;

Breve descrição das figuras

A figura 1 demonstra um diagrama de um modelo de arquitetura (porém não se limita a este) da presente invenção sendo constituído por um sistema de Telemedicina (1); salas de procedimento médico (2) sendo cada uma delas constituídas de uma unidade de acompanhamento e interação remota (3), equipamento hospitalar (12) e uma unidade de execução local (13) sendo interligadas por um método de comunicação; uma central de gerenciamento (4) constituída de um banco de dados (6) e uma base de imagens e vídeos (7) conectadas ao Servidor de Aplicação (5) e com o módulo de segurança interna (8); uma rede interna (9); um módulo de segurança externa (11); e uma rede externa (10).

A figura 2 refere-se ao algoritmo de autenticação.

A figura 3 refere-se ao algoritmo para a aquisição de vídeo.

A figura 4 refere-se ao algoritmo para a aquisição de áudio.

A figura 5 refere-se ao algoritmo para a publicação de vídeo.

A figura 6 refere-se ao algoritmo para a publicação de áudio.

Descrição detalhada da invenção

Para alcançar os objetivos descritos na breve descrição da invenção, definiu-se um sistema de telemedicina para o acompanhamento, a monitoração e a interação entre profissionais da área da saúde e/ou

pesquisadores, durante a realização de procedimentos médicos, como por exemplo, exames complementares de videocolonoscopia, endoscopia digestiva alta, cirurgia por meio de videolaparoscopia, entre outros.

O método proposto contempla a interação e a participação ativa de profissionais da área médica, em tempo real e de modo local e remoto, durante a realização de procedimentos médicos. Adicionalmente são disponibilizadas características para facilitar o gerenciamento e o armazenamento padronizado com relação aos dados dos pacientes, exames, vídeos e imagens. Em função da importância desses procedimentos e da necessidade de privacidade em relação às informações, todo o processo de comunicação e troca de informações foi delineado aplicando técnicas de segurança, principalmente métodos criptográficos.

Os componentes que fazem parte da invenção são apresentados na Figura 1, a partir da qual serão descritos os detalhes de seus elementos constituintes e dos métodos aplicados. Embora seja apresentada uma configuração específica, o método pode ser executado de modos diversos em face de personalizações que venham a ser aplicadas, inclusive para a realização e o acompanhamento de experimentos.

Para um entendimento global da arquitetura apresentada por meio da Figura 1, a presente invenção consiste em um sistema de Telemedicina (1) para a realização de procedimentos médicos. Para isso foi definido um modelo de interação entre a Sala de Procedimentos Médicos (2_k onde k = 1..p e p = número total de salas de procedimento médico), no qual se encontram os pacientes e a equipe responsável pelo procedimento; e as Unidades de Acompanhamento e Interação Remota (3_j onde j = 1..m e m = número total de clientes remotos), onde estão presentes médicos, profissionais da área da saúde e/ou pesquisadores. O método de interação foi projetado com o intuito de oferecer recursos para o acompanhamento, o auxílio e a interação remota, em tempo real, durante a realização de tais procedimentos. Para que seja possível essa interatividade são utilizados recursos presentes na Central de Gerenciamento de Procedimentos Médicos (4), incluindo o Servidor de

Aplicação (5), o Banco de Dados (6), a Base de Imagens (7) e o Módulo de Segurança Interna (8).

Conforme ilustrado na Figura 1, no método é definida a presença de diversas Unidades de Acompanhamento e de Interação Remota (3_j). Uma Unidade de Acompanhamento e de Interação Remota (3_j) pode estar localizada dentro da própria Sala de Procedimentos Médicos (2_k), em outros locais da Instituição por meio da comunicação com uma Rede Interna (9) ou em qualquer outro local físico, por meio de uma conexão com a Rede Externa (10) conjuntamente com o Módulo de Segurança Externo (11). Cada Instituição de Saúde poderá também possuir diversas Salas de Procedimentos Médicos (2_k) integradas ao sistema de Telemedicina (1). Toda a solução proposta nesta invenção possui a característica de ser utilizada por meio de sistemas distribuídos, tendo como configuração padrão a aplicação do modelo em ambiente *Web*. Configurações alternativas podem ser aplicadas em função de especificidades e dos recursos computacionais e tecnológicos disponíveis.

Por meio desses componentes e dos métodos aplicados, a presente invenção permite alta flexibilidade para o acompanhamento e a interação, em tempo real, entre profissionais da área médica e/ou pesquisadores, com relação a procedimentos médicos e/ou realização de experimentos, principalmente relacionados à área da saúde. Entre os recursos disponibilizados por essa invenção tem-se o compartilhamento dos seguintes itens:

- dados referentes ao procedimento médico em execução;
- imagens e vídeos capturados na Sala de Procedimentos Médicos (2_k) e/ou nas Unidades de Acompanhamento e Interação Remota (3_j);
- interação entre os participantes por meio de recursos de áudio, vídeo e mensagens texto.

Além das características de tempo real, o presente método permite a recuperação e a análise posterior de exames complementares e/ou procedimentos médicos e/ou experimentos realizados, tornando as atividades mais flexíveis.

A partir dessas definições serão apresentadas as características dos elementos constituintes da Figura 1 e a descrição dos métodos aplicados na presente invenção.

Esta invenção não está limitada aos detalhes de construção apresentados no presente documento, podendo ser realizada por meio de outras configurações alternativas.

Em condição de execução normal, na(s) Sala(s) de Procedimentos Médicos (2_k) encontram-se os pacientes que estão sendo submetidos a determinado procedimento médico, a equipe responsável pelo procedimento, o(s) respectivo(s) Equipamento(s) Hospitalar(s) (12_i) e a(s) Unidade (s) de Execução Local (13_l).

Os Equipamentos Hospitalares (12_i), em condição normal de execução, podem ser destinados a procedimentos médicos, tais como para exames complementares de videocolonoscopia, videoendoscopia, intervenções cirúrgicas por meio de videolaparoscopia, entre outros tipos de exames e procedimentos por vídeo e imagem. De modo alternativo seria possível utilizar outros equipamentos hospitalares para a monitoração de informações sobre pacientes, entre os quais ECG, EEG, temperatura, pressão sanguínea, entre outros. Se aplicados para a realização de experimentos poderiam ser utilizados outros equipamentos hospitalares específicos ou mesmo outras máquinas com outras aplicações, tais como balanças de precisão, entre outros.

A equipe responsável pelo procedimento médico, presente na Sala de Procedimentos Médicos (2_k), poderá utilizar a(s) Unidade(s) de Execução Local (13_l) como auxílio na automatização de algumas tarefas, entre as quais o cadastro e a edição de informações sobre os pacientes, exames complementares e/ou experimentos, e principalmente para a aquisição e a análise de dados, imagens e vídeos provenientes do(s) Equipamento(s) Hospitalare(s) (12_i).

Dentro desse contexto, a(s) Unidade(s) de Execução Local (13_l) é (são) responsável(is) por estabelecer o protocolo de comunicação com o(s) Equipamento(s) Hospitalar(es) (12_i). Considerando o fluxo normal definido

nesta invenção, seriam aplicados Equipamento(s) Hospitalar(es) (12_i) para procedimentos baseados em vídeos e imagens. Como a grande maioria dos Equipamentos Hospitalares (12_i) pertencentes a essa categoria disponibilizam vídeos em formato analógico (vídeo-composto, super-vídeo, entre outros), a(s) Unidade(s) de Execução Local (13_i) possuem a função de capturar esses vídeos, convertê-los para o formato digital e posteriormente encaminhá-los para o Servidor de Aplicação (5), presente na Central de Gerenciamento de Procedimentos Médicos (4). No caso de Equipamento(s) Hospitalar(es) (12_i) que já disponibilizam vídeos em formato digital, a característica de conversão de vídeo analógico para digital não é aplicada.

Em situações alternativas de execução, o(s) Equipamento(s) Hospitalar(es) (12_i) poderiam transmitir outros tipos de dados que não sejam vídeos e/ou imagens. Nessas condições a(s) Unidade(s) de Execução Local (13_i) devem aplicar protocolos de comunicação compatíveis com outros equipamentos específicos, entre os quais o padrão serial, *ethernet*, *wireless*, TCP/IP, entre outros.

A(s) Unidade(s) de Execução Local (13_i) conectam-se ao Servidor de Aplicação (5) presente na de Central de Gerenciamento de Procedimentos Médicos (4). Para isso é utilizada a Rede Interna (9) e é aplicada a política de segurança definida pelo Módulo de Segurança Interna (8). Para a utilização da(s) Unidade(s) de Execução Local (13_i) é necessário realizar um procedimento de autenticação, e para a comunicação entre a(s) Unidade(s) de Execução Local (13_i) e o Servidor de Aplicação (5) é necessário utilizar recursos de criptografia. Esses delineamentos correlatos à segurança foram desenvolvidos pelo grupo de pesquisa e denominado de método LABI-SIA, que será descrito em pedido de patente independente.

A(s) Unidade(s) de Execução Local (13_i) ficam continuamente recebendo vídeos e/ou outros tipos de informações do(s) Equipamento (s) Hospitalar(es) (12_i), e encapsulando esses dados em um protocolo mais adequado e com suporte a mecanismos de segurança (criptografia). Após esse tratamento, ocorre a transmissão desses dados para o Servidor de Aplicação

(5) utilizando a arquitetura de protocolos disponibilizados pela Rede Interna (9). Os protocolos atualmente mais aplicados para esse tipo de transmissão pela *Web* são o *Internet Protocol* – IP – e o *Transport Control Protocol* – TCP.

De acordo com o modelo estabelecido nesta invenção, a(s) Unidade(s) de Execução Local (13_i) também podem receber, do Servidor de Aplicação (5), os fluxos de vídeo e/ou áudio, mensagens em formato texto e imagens em formato texto. Isso ocorre em função do modelo de interação desenvolvido, pois médicos e/ou profissionais presentes na(s) Unidade(s) de Acompanhamento e Interação Remota (3_j) podem disponibilizar seus *streamings* de vídeo e/ou áudio, e interagir durante a realização do procedimento médico e/ou experimental por meio de áudio, vídeo, mensagens texto e ainda capturando e compartilhando imagens. O modelo de compartilhamento de imagens (*LABI-IMAGE-SHARING*) serão descritos pormenorizadamente em patentes específicas.

Como informações médicas requerem sigilo, é fundamental a utilização de critérios rígidos em relação à segurança. Com essa visão, a comunicação e a transmissão de dados em diferentes formatos, entre a(s) Unidade(s) de Execução Local (13_i) e o Servidor de Aplicação (5), é realizada adotando-se políticas fortes de segurança com relação à autenticidade e privacidade.

O foco principal desta invenção foi à aplicação dos métodos para a realização de exames baseados em vídeo e imagens, e também para a interação entre os profissionais por meio de recursos multimídia. Desse modo, foi estabelecido um cuidado especial com relação à publicação dos *streamings* de áudio e vídeo. O método confeccionado para este fim (*LABI-PUBLISH*) será apresentado em pedido de patente específico.

Na(s) Unidade(s) de Acompanhamento e Interação Remota (3_j), em condição normal de execução, poderão estar presentes médicos especialistas, profissionais da área da saúde, pesquisadores e/ou pessoas que tenham relação com o procedimento que está sendo realizado.

Essa(s) Unidade(s) de Acompanhamento e Interação Remota (3_j) podem estar presentes na própria Sala de Procedimentos Médicos (2_k), em qualquer local dentro do Hospital ou Clínica em que o procedimento médico esteja sendo realizado, ou mesmo em qualquer local geográfico que possua uma conexão com qualquer rede interligada, sendo atualmente a Internet a rede mais aplicada para essas finalidades. Em execução normal todas as interações computacionais são realizadas por meio da *Web*, aplicando-se navegadores de Internet. De modo alternativo pode-se aplicar qualquer outra tecnologia que contemple a comunicação em rede.

Inicialmente, a(s) Unidade(s) de Acompanhamento e Interação Remota (3_j) se conectam ao Servidor de Aplicação (5) presente na Central de Gerenciamento de Procedimentos Médicos (4). Para que essa conexão ocorra também é pré-requisito que haja a autenticação de um profissional com direitos de acesso a ferramenta. Quando a(s) Unidade(s) de Acompanhamento e Interação Remota (3_j) estão localizadas dentro do Hospital ou Clínica onde o procedimento está sendo realizado, serão utilizados os recursos disponibilizados pela Rede Interna (9) e será aplicada a política de segurança definida pelo Módulo de Segurança Interna (LABI-SIA). Caso a(s) Unidade(s) de Acompanhamento e Interação Remota (3_j) estejam localizadas fora da Instituição onde o procedimento está sendo realizado, serão utilizados os recursos da Rede Externa (10) e da Rede Interna (9), e serão aplicadas as políticas de segurança definidas pelo Módulo de Segurança Externa (11) e posteriormente pelas regras estabelecidas no Módulo de Segurança Interna (8). Todo esse processo de autenticação e procedimentos de segurança é definido por meio do método LABI-SIA, que será abordado em seção específica.

Após o estabelecimento de conexão com o Servidor de Aplicação (5), a Unidade de Acompanhamento e Interação Remota (3_j) passa a receber os fluxos de dados, vídeos, áudios e imagens relativas ao(s) procedimento(s) que está(ão) sendo realizado(s) na Sala de Procedimento Médico (2_k), em tempo real. Como o Servidor de Aplicação (5) gerencia e disponibiliza esses

recursos para a(s) Unidade(s) de Acompanhamento e Interação Remota (3_j), a mesma pode receber simultaneamente todas essas categorias de fluxos de diferentes Salas de Procedimentos Médicos, e por conseguinte, de distintos Equipamento(s) Hospitalar(es) (12_i).

O Servidor de Aplicação (5) também disponibiliza recursos para a realização de discussões, e para o compartilhando de múltiplas mídias, entre os profissionais ativos em todas as Unidades de Acompanhamento e Interação Remota (3_j). Desse modo, a Unidade de Acompanhamento e Interação Remota (3_j) também receberá, do Servidor de Aplicação (5), os recursos compartilhados por todas as Unidades de Acompanhamento e Interação Remota (3_j). Esses recursos consistem em fluxos de áudio e/ou vídeo, e também no compartilhamento de mensagens texto e de imagens capturadas em qualquer Sala de Procedimentos Médicos (2_k) e/ou Unidades de Acompanhamento e Interação Remota (3_j).

Conforme apresentado anteriormente, a Unidade de Acompanhamento e Interação Remota (3_j) pode também disponibilizar o vídeo e/ou áudio de sua Unidade para os demais participantes, por meio do Servidor de Aplicação (5). Essa publicação dos *streamings* de áudio e vídeo é realizada por meio do método LABI-PUBLISH. Esse método foi concebido, nesta invenção, com o intuito de proteger tais fluxos, enfaticamente os fluxos provenientes de procedimentos médicos, contra acessos e conexões indevidas.

A configuração padrão para organizar esses fluxos é a separação dos procedimentos médicos e participantes em locais distintos, permitindo a interação dos participantes somente em relação ao procedimento de interesse específico, ou seja, ter-se uma única Sala de Procedimentos Médicos (2_k) e diversas Unidades de Acompanhamento e Interação Remota (3_j) para a realização de um único procedimento médico.

Além das ações de tempo real, a(s) Unidade(s) de Acompanhamento e Interação Remota (3_j) permite(m) a análise posterior à realização do procedimento médico. Desse modo é possível acessar dados relativos a qualquer procedimento médico, assim como imagens, áudio, vídeos

e quaisquer outras informações relacionadas a um determinado exame complementar e/ou procedimento, após a realização de tal procedimento.

A partir dessa característica é possível realizar a análise local ou remota, individual ou coletiva, a qualquer tempo e de modo interativo. Outra característica disponibilizada nesta invenção, em relação a exames complementares e outros sistemas convencionais de telemedicina, consiste em permitir a exportação, dos dados relativos ao procedimento e das imagens capturadas, para o formato DICOM.

A Central de Gerenciamento de Procedimentos Médicos (4), por meio do Servidor de Aplicação (5), é responsável pelo controle de acessos, pela recepção e pela distribuição dos fluxos de áudio e vídeo entre as Unidades de Acompanhamento e Interação Remota (3_j) e as Unidades de Execução Local (13_i), pelo armazenamento de dados relativos aos procedimentos médicos no Banco de Dados (6) e por guardar os vídeos e imagens provenientes dos procedimentos médicos na Base de Imagens e Vídeos (7). Adicionalmente na Central de Gerenciamento de Procedimentos Médicos (4) são definidas as políticas de segurança e controle de acesso interno, por meio do Módulo de Segurança Interna (8).

O Banco de Dados (6) é o local onde são armazenados fisicamente os dados relativos aos procedimentos médicos realizados na(s) Sala(s) de Procedimentos Médicos (2_k). A definição do Sistema Gerenciador de Banco de Dados a ser aplicado e da política de administração e gerenciamento do mesmo, devem ser definidos em função das alternativas tecnológicas disponíveis e das particularidades de cada Instituição. O número de servidores de banco de dados poderá variar em função do volume de dados a ser tratado e da quantidade de Salas de Procedimentos Médicos (2_k) que serão utilizadas.

Na Base de Imagens e Vídeos (7) são armazenadas e organizadas as imagens e os vídeos adquiridos e capturados na(s) Sala(s) de Procedimentos Médicos (2_k), durante a realização de exames complementares, experimentos ou qualquer outro procedimento médico.

A quantidade de Servidores de Aplicações (5) pode variar de acordo com o local onde o método é aplicado, e deve ser definida em função do número de Salas de Procedimento Médico (2_k) e de Unidades de Acompanhamento e Interação Remota (3_j).

Os Servidores de Aplicações (5) se comunicam, por meio da rede, com os clientes (Unidades(s) de Execução Local (13_i) e Unidade(s) de Acompanhamento e Interação Remota (3_j)), por meio de protocolos próprios para essa finalidade, podendo-se citar a arquitetura de comunicação mais utilizada atualmente que é a *TCP/IP*.

O(s) Servidor(es) de Aplicações (5) recebem os dados relativos aos pacientes e respectivos procedimentos médicos e os armazenam no Banco de Dados (6). Do mesmo modo o(s) Servidor(es) de Aplicações (5) recepcionam as imagens e os vídeos, capturados na(s) Salas de Procedimento Médico (2_k) e na(s) Unidades de Acompanhamento Remoto (3_j), e os encaminham para a Base de Imagens e Vídeos (7). Posteriormente essas informações históricas podem ser consultadas e recuperadas por meio das Unidades de Execução Local (13_i) e pelas Unidades de Acompanhamento e Integração Remota (3_j). Outra função dos Servidores de Aplicações (5) consiste em converter procedimentos médicos baseados em imagem para o formato DICOM e registrar essas informações no banco de dados (6).

Como mencionado anteriormente, o Servidor de Aplicação (5) é também responsável pelo gerenciamento e pela distribuição de todos os fluxos multimídias entre todos os participantes, os quais usam esses recursos por meio da(s) Unidade(s) de Execução Local (13_i) e da(s) Unidade(s) de Acompanhamento e Interação Remota (3_j). As tecnologias a serem utilizadas para prover esses serviços devem ser selecionadas de acordo com as especificidades de cada instituição. Desse modo, os Servidores de Aplicações (5) são responsáveis pela autenticação, recebimento, distribuição e gerenciamento de todas as sessões multimídia. As tecnologias mais utilizadas atualmente, para essas funções, são *Flash Media Server*, *Red5* e *Wowza Media Server*.

Os serviços disponibilizados pelo(s) Servidor(es) de Aplicações (5), por meio do gerenciamento desses recursos multimídia, constituem uma ferramenta de apoio a médicos, especialistas e pesquisadores para permitir a discussão de exames complementares e de outros procedimentos médicos, por meio da utilização dessas diferentes mídias, entre os quais áudio, vídeo, mensagens texto e compartilhamento de imagens.

Na Rede Interna (9) podem ser utilizados recursos de interconexão diversos. Os mais comuns atualmente são o padrão *Ethernet* e *Wireless*. Com relação à Rede Externa (10) também se pode aplicar qualquer rede disponível, como canais dedicados, redes por cabo, redes ADSL, entre outros.

a) Método para Compartilhamento de Imagens LABI-IMAGE-SHARING

Conforme apresentado na Figura 1, a participação iterativa e interativa entre profissionais da área médica e/ou especialistas e/ou pesquisadores ocorre por meio da(s) Unidade(s) de Execução Local (13_i) e da(s) Unidade(s) de Acompanhamento e Interação Remota (3_j). Nesse contexto, além da utilização de mídias aplicadas convencionalmente em sistemas de videoconferência, agregou-se nessa invenção um mecanismo que permite, a esses profissionais, participarem ativamente da realização de procedimentos médicos por meio da captura e compartilhamento de imagens relativas ao procedimento médico que está sendo realizado.

Para explicitar o método algorítmico desenvolvido, primeiramente apresenta-se o contexto em que o método LABI-IMAGE-SHARING é aplicado. Antes de iniciar o procedimento médico, os participantes presentes na(s) Unidade(s) de Execução Local (13_i) e na(s) Unidade(s) de Acompanhamento e Interação Remota (3_j) são autorizados para utilizar o sistema (autenticação) por meio das políticas definidas no método LABI-SIA. Durante a realização dos procedimentos médicos, a Unidade de Execução Local (13_i) transmite o vídeo para o Servidor de Aplicação (5) e esse realiza a distribuição desse vídeo para todas as Unidades de Acompanhamento e Interação Remota (3_j). Do mesmo modo, opcionalmente as Unidades de Acompanhamento e Interação Remota

(3_j) podem enviar as suas mídias de vídeo e/ou áudio para o Servidor de Aplicação (5) e este é responsável pela distribuição dessas mídias para todas as Unidades de Acompanhamento e Interação Remota (3_j) e para a Unidade de Execução Local (13_i). As imagens capturadas durante o procedimento médico devem ser armazenadas na Base de Imagens e vídeos (7). Todo o processo de transmissão de vídeos e imagens é realizado de modo privativo, aplicando-se técnicas de criptografia, conforme delineado no método LABI-SIA.

A partir desse estado, qualquer participante, seja na Unidade de Execução Local (13_i) ou na(s) Unidade(s) de Acompanhamento e Interação Remota (3_j), pode capturar imagens relativas ao procedimento médico e essas devem ser disponibilizadas, em tempo real, para todos os participantes.

b) Método de Segurança Baseado em Sistemas Imunológicos Artificiais LABI-SIA

O modelo de segurança delineado nesta invenção, LABI-SIA, consiste em um método baseado nos conceitos de Sistemas Imunológicos Artificiais. Desse modo são definidas distintas camadas e aplicações com o intuito de proteger a solução contra ataques.

Módulo de Segurança Externa (11)

Essa parte do método é responsável pela interface entre a rede interna e a rede externa. Desse modo devem ser aplicadas as políticas de segurança mais gerais, e que tenham relação com toda a instituição.

O método LABI-SIA é utilizado no processo de acesso ao sistema, durante a autenticação dos usuários, e em todos os momentos em que há transmissão de dados. Inclui as políticas de criptografia, definição de senhas, bloqueios e recuperação de contas, entre outros.

Módulo de Segurança Interna (8)

O módulo de segurança interna (8) é aplicado para o gerenciamento de acessos e de conexões, tanto provenientes da rede interna (9) quanto de conexões solicitadas por meio da rede externa (10) e previamente autorizadas pelo módulo de segurança externa (11).

A seguir são apresentadas as principais características definidas no Módulo de Segurança Interna (8):

c) Método para Publicação de *Streamings* de Vídeo e Áudio LABI-PUBLISH

O método LABI-PUBLISH foi definido com o intuito de proteger o fluxo de vídeo e áudio contra interceptações e conexões indesejadas. O método é aplicado no invento sempre que é publicado um *streaming*, tanto proveniente de equipamentos hospitalares (12_i) quanto das mídias utilizadas nas Unidades de Acompanhamento e Interação Remota (3_j).

A presente invenção enquadra-se na área de Telemedicina, sendo aplicada principalmente para o acompanhamento de procedimentos médicos e/ou experimentos, tanto local quanto remotamente, em tempo real e de modo interativo e iterativo, por meio de recursos computacionais.

Os principais diferenciais da tecnologia proposta são: a) Recursos para o acompanhamento tanto local quanto remoto, em tempo real, de procedimentos médicos. Desse modo os participantes podem ter acesso, por meio da Internet, aos fluxos de vídeo, áudio e dados provenientes de equipamentos hospitalares; b) Adicionalmente são disponibilizados recursos que permitem aos participantes, locais e remotos, discutirem acerca do procedimento médico por meio de recursos multimídia, incluindo vídeo, áudio e texto. Essa interatividade pode ser utilizada tanto durante a realização dos procedimentos médicos quanto após o término dos mesmos; c) Os participantes, local e remotamente, podem participar ativamente durante a realização de procedimentos médicos capturando e compartilhando imagens relativas ao mesmo. Desse modo, os profissionais em qualquer parte do mundo, podem interagir e iteragir, por meio desses recursos tecnológicos. Esse método foi denominado nesta invenção como LABI-IMAGE-SHARING; d) Desenvolvimento de um método específico para a área de segurança, com o objetivo de preservar a privacidade dos dados dos pacientes e dos exames; e) Desenvolvimento de um algoritmo para a distribuição segura de fluxos de vídeo e áudio, denominado LABI-PUBLISH.

A invenção foi projetada inicialmente para ser aplicada na realização de exames complementares de colonoscopia, endoscopia, cirurgias por videolaparoscopia e demais procedimentos médicos baseados em equipamentos hospitalares que trabalham com vídeos e imagens. O método pode ser aplicado para outros procedimentos e experimentos da área da saúde que necessitem a comunicação com equipamentos hospitalares e o acompanhamento remoto em tempo real. Podem-se citar outras categorias de exames complementares em áreas como radiologia, ultrassonografia, entre outros. A invenção, dentro do contexto da área da saúde, pode também ser aplicada para a realização e discussão de experimentos médicos e para a discussão de casos de pacientes e elaboração de diagnósticos, por meio do acompanhamento e discussão de modo remoto, em tempo real, e também após a realização de procedimentos médicos e/ou experimentos. Além de procedimentos médicos e experimentos, a invenção pode ser utilizada com objetivos educacionais, podendo ser utilizada para a disseminação de conhecimento sobre a execução de distintos procedimentos na área médica. O método também pode ser aplicado em outras áreas do conhecimento que necessitem recursos, em tempo real, para o compartilhamento de mensagens texto, áudio, vídeo e imagens.

REIVINDICAÇÕES

1. Método em telemedicina para o acompanhamento remoto e em tempo real de procedimentos médicos **caracterizado por** compreender as seguintes etapas:
   a. Primeiramente realizam-se as configurações específicas do sistema de Telemedicina de modo a disponibilizar os serviços necessários ás Unidade(s) de Execução Local (13_i) e à(s) Unidade(s) de Acompanhamento e Interação Remota (3_j);
   b. Processa-se a autenticação por intermédio do algoritmo descrito na figura 2;
   c. Estabelece o Protocolo de Comunicação com o Equipamento Médico;
   d. Estabelece conexão com o Servidor de Aplicação (5);
   e. Inicia a aquisição de fluxos de vídeo e/ou áudio a partir do equipamento médico por intermédio dos algoritmos descritos nas figuras 3 e 4;
   f. A Unidade de Execução Local (13_i) disponibiliza esses fluxos de vídeo e/ou áudio para o Servidor de Aplicação (5) por intermédio dos algoritmos descrito nas Figuras 5 e 6;
   g. Promove-se a interação dos profissionais, em tempo real, por meio de recursos de vídeo, áudio, mensagens texto; assim como capturando e compartilhando imagens relativas ao procedimento médico em execução;
   h. A Unidade de Execução Local (13_i) encerra a publicação do(s) fluxo(s) de vídeo e/ou áudio, o Servidor de Aplicação (5) comunica todas as Unidades de Acompanhamento e Interação Remota (3_j) ativas para encerrarem os canais de comunicação relativos ao recebimento de fluxos de áudio e/ou vídeo relativos ao procedimento médico, todas as Unidades de Acompanhamento e Interação Remota (3_j) fecham os canais de comunicação para recebimento de fluxos de

vídeo e/ou áudio previamente estabelecidos, a Unidade de Execução Local (13_i) encerra a comunicação com o equipamento médico, a Unidade de Execução Local (13_i) encerra a comunicação com o Servidor de Aplicação (5);

2. Método em telemedicina para o acompanhamento remoto e em tempo real de procedimentos médicos, de acordo com a reivindicação 1, **caracterizado pelo** fato de, para cada nova Unidade de Acompanhamento e Interação Remota (3_j) que se conecta ao sistema, serem executados os seguintes procedimentos:
    - O Servidor de Aplicação (5) atualiza a lista de conexões e envia essa lista para todas as conexões ativas, tanto para a Unidade de Execução Local (13_i) quanto para a(s) Unidade(s) de Acompanhamento e Interação Remota (3_j);
    - O Servidor de Aplicação (5) envia os dados relativos ao exame em execução para a nova Unidade de Acompanhamento e Interação Remota (3_j);
    - A nova Unidade de Acompanhamento e Interação Remota (3_j) estabelece uma conexão com o Servidor de Aplicação (5) e passa a receber os fluxos de vídeo e/ou áudio provenientes do exame em execução na Unidade de Execução Local (13_i);
    - A nova Unidade de Acompanhamento e Interação Remota (3_j) faz *download* e apresenta imagens relativas ao exame em execução, caso existam.

3. Método em telemedicina para o acompanhamento remoto e em tempo real de procedimentos médicos, de acordo com a reivindicação 1, **caracterizado por** na etapa "a" serem realizadas uma série de inicializações/configurações:
    - Inicialização do Servidor de *Streaming*;
    - Inicialização do Servidor de Bando de Dados;
    - Inicialização do Servidor de Páginas Web;

- Inicialização do Módulo das Políticas de Segurança;
- Aplicação das Configurações definidas para o Sistema de Telemedicina

4. Método em telemedicina para o acompanhamento remoto e em tempo real de procedimentos médicos, de acordo com a reivindicação 2, **caracterizado por**, para cada nova unidade, a interação por vídeo se dar por intermédio das seguintes ações:
    - A nova Unidade de Acompanhamento e Interação Remota (3_j) realiza o processo de aquisição do vídeo e a de sua publicação;
    - A partir de cada publicação de vídeo realizada, o Servidor de Aplicação (5) atualiza a lista de fluxos de vídeo;
    - O Servidor de Aplicação (5) envia uma mensagem para todas as conexões ativas com a identificação do novo fluxo de vídeo publicado, e com os dados do usuário e da nova Unidade de Acompanhamento e Interação Remota (3_j) que está compartilhando a mídia de vídeo;
    - Todas as Unidades de Acompanhamento e Interação Remota (3_j) e a Unidade de Execução Local (13_i), exceto a nova Unidade de Acompanhamento e Interação Remota (3_j) que está disponibilizando o novo fluxo de vídeo, criam um novo canal de comunicação para receber o novo fluxo de vídeo e passam a obter e apresentar esse vídeo.
5. Método em telemedicina para o acompanhamento remoto e em tempo real de procedimentos médicos, de acordo com a reivindicação 2, **caracterizado por,** para cada nova unidade, a interação por áudio se dar por intermédio das seguintes ações:
    - A nova Unidade de Acompanhamento e Interação Remota (3_j) realiza o processo de aquisição do áudio e a sua publicação;
    - A partir de cada publicação de áudio realizada, o Servidor de Aplicação (5) atualiza a lista de fluxos de áudio;

- O Servidor de Aplicação (5) envia uma mensagem para todas as conexões ativas com a identificação do novo fluxo de áudio publicado, e com os dados do usuário e da nova Unidade de Acompanhamento e Interação Remota (3_j) que está compartilhando a mídia de áudio;
- Todas as Unidades de Acompanhamento e Interação Remota (3_j) e a Unidade de Execução Local (13_i), exceto a nova Unidade de Acompanhamento e Interação Remota (3_j) que está disponibilizando o novo fluxo de áudio, criam um novo canal de comunicação para receber o novo fluxo de áudio e passam a obter e reproduzir esse áudio.

6. Método em telemedicina para o acompanhamento remoto e em tempo real de procedimentos médicos, de acordo com a reivindicação 2, **caracterizado por**, para cada nova unidade, a interação por meio de mensagens de texto se dar por intermédio das seguintes ações:
    - A mensagem texto e a identificação do usuário são enviadas para o Servidor de Aplicação (5);
    - O Servidor de aplicação (5) encaminha a mensagem texto e a identificação do usuário para todas as Unidades de Acompanhamento e Interação Remota (3_j) ativas e para a Unidade de Execução Local (13_i);
    - Todas as Unidades de Acompanhamento e Interação Remota (3_j) e a Unidade de Execução Local (13_i) recebem e apresentam a mensagem texto e a identificação do usuário.

7. Método em telemedicina para o acompanhamento remoto e em tempo real de procedimentos médicos, de acordo com a reivindicação 2, **caracterizado por**, para cada nova unidade, a interação por meio de Imagens relativas ao Procedimento Médico em Execução se dar por intermédio das seguintes ações:
    - A imagem é transmitida para o Servidor de Aplicação (5);

- O Servidor de Aplicação (5) armazena essa imagem na Base de Imagens e Vídeos (7);
- O Servidor de Aplicação (5) comunica a localização da imagem, na Base de Imagens e Vídeos (7), para a conexão que capturou a imagem originalmente, seja na Unidade de Execução Local (13_i) ou na Unidade de Acompanhamento e Interação Remota (3_j);
- A partir do local onde a imagem foi capturada, Unidade de Execução Local (13_i) ou a Unidade de Acompanhamento e Interação Remota (3_j), é enviada uma mensagem para todas as conexões ativas, ou seja, para as Unidades de Execução Local (13_i) e para as Unidades de Acompanhamento e Interação Remota (3_j) que possuam conexões ativas. O conteúdo dessa mensagem é a localização da imagem capturada na Base de Imagens e Vídeos (7);
- A Unidade de Execução Local (13_i) e todas as Unidades de Acompanhamento e Interação Remota (3_j) recebem a mensagem, fazem *download* da imagem e a disponibilizam graficamente em uma área da tela destinada para imagens relativas ao procedimento médico em execução.

8. Método em telemedicina para o acompanhamento remoto e em tempo real de procedimentos médicos, de acordo com a reivindicação 1, **caracterizado por** possibilitar a análise dos dados coletados durante o procedimento médico por intermédio de dois programas de computador embarcados no Servidor de Aplicação (5) que são utilizados na Unidade de Execução Local (13) e nas Unidades de Acompanhamento.

9. Método em telemedicina para o acompanhamento remoto e em tempo real de procedimentos médicos, de acordo com a reivindicação 8, **caracterizado por** o Servidor de Aplicação (5) disponibilizar os seguintes recursos:

- Cadastro, visualização e edição de dados de profissionais e pacientes;
- Visualização de dados e imagens relativas a procedimentos médicos;
- Criação, visualização e edição de laudos.

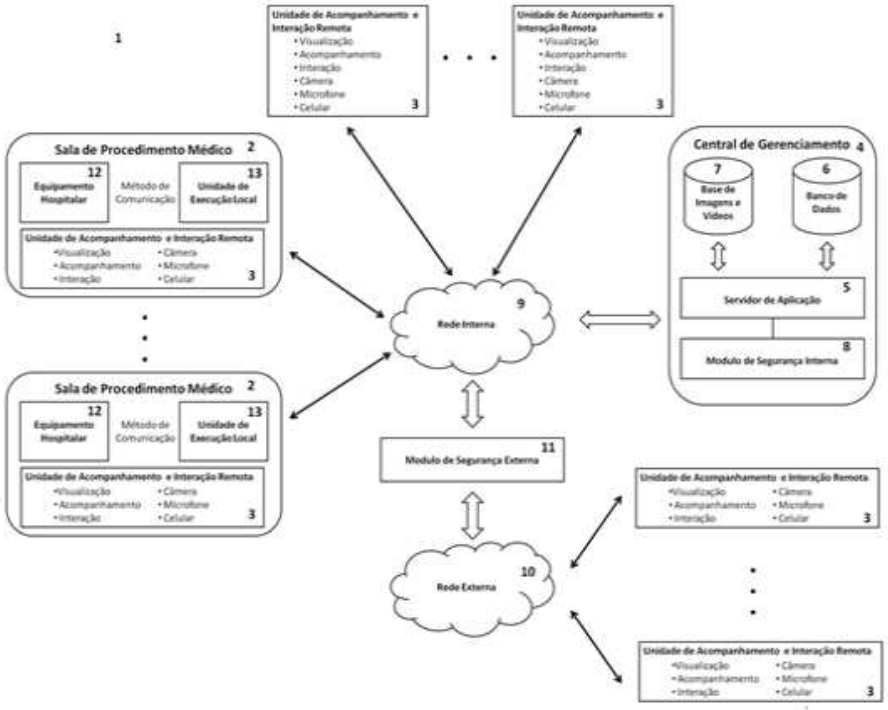

Figura 1

```
Procedimento autenticacao ( Texto login, Texto senha )

Inicio

      Selecione login e senha na base de dados;

      Se resultado da busca for positivo (encontrado) então faça

         Instancie um novo objeto Usuário;

         Adicione o novo objeto Usuário para a lista de Usuários
Autenticados;
```

Figura 2

```
Procedimento aquisicaoDeVideo ()

Inicio

       Inicie objeto (objetoVideo) para captura de vídeo;

       Defina os parâmetros de objetoVideo para a captura do vídeo:

              - codec de vídeo;

              - resolução;

              - número de quadros por segundo;
```

Figura 3

```
Procedimento aquisicaoDeAudio ()

Inicio

       Inicie objeto (objetoAudio) para captura de áudio;

       Defina os parâmetros de objetoAudio para a captura do áudio:

           - codec de áudio;
```

Figura 4

```
Procedimento publicacaoDeVideo (Video objetoVideo)
Inicio
      Inicie objeto (objetoStream) para publicação de Stream;
       Com objetoStream faça
            Defina um nome de identificação para o Stream;
            Estabeleça uma conexão com o Servidor de Stream;
```

Figura 5

```
Procedimento publicacaoDeAudio (Audio objetoAudio)
Inicio
      Inicie objeto (objetoStream) para publicação de Stream;
       Com objetoStream faça
            Defina um nome de identificação para o Stream;
            Estabeleça uma conexão com o Servidor de Stream;
            Alegue um canal de comunicação com o Servidor de Stream;
```

Figura 6

RESUMO

MÉTODO EM TELEMEDICINA PARA O ACOMPANHAMENTO REMOTO E EM TEMPO REAL DE PROCEDIMENTOS MÉDICOS

Refere-se o presente pedido de patente de invenção a um novo método computacional sistêmico em telemedicina cuja finalidade é permitir o acompanhamento remoto de procedimentos médicos no âmbito da Telemedicina, em tempo real e de modo interativo e iterativo; permitir que a realização desses procedimentos médicos possam ser realizados em locais onde não se tem a presença de médicos especialistas, sem prejudicar a eficácia do procedimento, e evitando em muitos casos a necessidade de deslocamento de pacientes até cidades distantes que disponham desses especialistas; permitir que médicos especialistas trabalhem, também de modo remoto, na análise e na elaboração de laudos e de diagnósticos, após a realização dos procedimentos médicos.

6. PATENTE BR 10 2012 033128 4

MÉTODO PARA GERAÇÃO DE CHAVES BASEADO EM ALGORITMOS GENÉTICOS

< Uso exclusivo do INPI >

INPI Manaus 26/12/2012 018120047757 VP21/12/2012

BR 10 2012 033128 4

Espaço reservado ao protocolo

Espaço para etiqueta

DEPÓSITO DE PEDIDO DE PATENTE OU DE CERTIFICADO DE ADIÇÃO

Ao Instituto Nacional da Propriedade Industrial:
O requerente solicita a concessão de um privilégio na natureza e nas condições abaixo indicadas

1. Depositante (71):

1.1 Nome: UNIVERSIDADE ESTADUAL DE CAMPINAS - UNICAMP

1.2 Qualificação PESSOA JURÍDICA DE DIREITO PÚBLICO, AUTARQUIA ESTADUAL

1.3 CNPJ/CPF: 460684250001/33

1.4 Endereço Completo CIDADE UNIVERSITÁRIA "ZEFERINO VAZ"

1.5 CEP: 13083-970 1.6 Telefone (19)35215015 1.7 Fax: (19)35215210

1.8 E-mail: patentes@inova.unicamp.br

☒ continua em folha anexa

2. Natureza: ◉ Invenção ○ Modelo de Utilidade ○ Certificado de Adição

Escreva, obrigatoriamente, e por extenso, a Natureza desejada: INVENÇÃO

3. Título da Invenção ou Modelo de Utilidade ou Certificado de Adição(54):
MÉTODO PARA GERAÇÃO DE CHAVES BASEADO EM ALGORITMOS GENÉTICOS

☐ continua em folha anexa

4. Pedido de Divisão: do pedido Nº Data de Depósito:

5. Prioridade: ☐ interna ☐ unionista

O depositante reivindica a(s) seguinte(s):

País ou organização de origem	Número de depósito	Data do depósito

6. Inventor (72):

☐ Assinale aqui se o(s) mesmo(s) requer(em) a não divulgação de seu(s) nome(s)

6.1 Nome: WU FENG CHUNG

6.2 Qualificação BRAS,CASADO,PROF. UNIVERSITÁRIO 6.3 CPF: 102.096.488-05

6.4 Endereço completo RUA LONTRA, 26, VILA A, EM FOZ DO IGUACU - PR

6.5 CEP: 85861-120 6.6 Telefone: 45 3521-4824 6.7 Fax:

6.8 E-Mail: wufengchung@gmail.com

☒ continua em folha anexa

674_CHAVES

INPI Formulário 1.01 – Depósito de Pedido de Patente ou de Certificado de Adição (folha 1/2)

7. Declaração na forma do item 3.2 do Ato Normativo nº 127/97:

☐ 7.1 Declaro que os dados fornecidos no presente formulário são idênticos ao da certidão de depósito ou documento equivalente do pedido cuja prioridade está sendo reivindicada.

☐ em anexo

8. Declaração de divulgação anterior não prejudicial: (Período de Graça):
(art. 12 da LPI e item 2 do AN nº 127/97) ☐ em anexo

9. Procurador (74)

9.1 Nome: FERNANDA LAVRAS COSTALLAT SILVADO

9.2 CNPJ/CPF: 295.166.068-57 9.3 API/OAB: 210.899

9.4 Endereço completo PROCURADORIA GERAL DA UNICAMP , EM CAMPINAS - SP

9.5 CEP: 13083-970 9.6 Telefone: (19) 3521.4766 9.7 Fax 19 3289.2245

9.8 E-Mail: proc-geral@pg.unicamp.br

10. Listagem de sequências Biológicas (documentos anexados) (se houver):

☐ Listagem de sequências em arquivo eletrônico: nº de CDs ou DVDs (original e cópia).

☐ Código de controle alfanumérico no formato de código de barras: fl.

☐ Listagem de sequências em formato impresso: fls.

☐ Declaração de acordo com o artigo da Resolução INPI nº 228/09: fls.

11. Documentos anexados (assinale e indique também o número de folhas):
(Deverá ser indicado o nº total de somente uma das vias de cada documento)

☒	11.1 Guia de Recolhimento	1 fls.	☒	11.5 Relatório descritivo	18 fls.
☒	11.2 Procuração	2 fls.	☒	11.6 Reivindicações	3 fls.
☐	11.3 Documentos de Prioridade	fls.	☒	11.7 Desenhos	2 fls.
☐	11.4 Doc. de contrato de trabalho	fls.	☒	11.8 Resumo	1 fls.
☐	11.9 Outros que não aqueles definidos no campo 11 (especificar)				fls.

12. Total de folhas anexadas (referentes aos campos 10 e 11): 27 fls.

13. Declaro, sob penas da Lei, que todas as informações acima prestadas são completas e verdadeiras.

CAMPINAS, SP, EM 18.12.2012
Local e Data

Assinatura e Carimbo

Fernanda Lavras Costallat Silvado
Procuradora da Universidade Subchefe
Matrícula nº 20.574-2
OAB/SP nº 210.899

INPI Formulário 1.01 – Depósito de Pedido de Patente ou de Certificado de Adição (folha 2/2)

< Uso exclusivo do INPI >

INPI INSTITUTO NACIONAL DA PROPRIEDADE INDUSTRIAL PROTOCOLO GERAL
mariahmm 018130003657
05/02/2013 14:49 DESP
0000221300696162

Espaço para etiqueta

PETIÇÃO - RELACIONADA COM PEDIDO, PATENTE OU CERTIFICADO DE ADIÇÃO

Ao Instituto Nacional da Propriedade Industrial:

1. Interessado

1.1 Nome: UNIVERSIDADE ESTADUAL DE CAMPINAS - UNICAMP

1.2 Qualificação: pessoa jurídica de direito público

1.3 CNPJ/CPF: 46068425000133

1.4 Endereço completo: Cidade Universitária "Zeferino Vaz"

1.5 CEP: 13083-970

1.6 Telefone: 19 3521-5015 1.7 Fax: 19 3521-5210 1.8 E-Mail: patentes@inova.unicamp.br

☒ continua em folha anexa

2. Título da Invenção, do Modelo de Utilidade ou Certificado de Adição:

MÉTODO PARA GERAÇÃO DE CHAVES BASEADO EM ALGORITMOS GENÉTICOS

☐ continua em folha anexa

3. Natureza ◉ 3.1 Invenção ○ 3.2 Certificado de Adição ○ 3.3 Modelo de Utilidade

4. Referência

☒ 4.1 Pedido

☐ 4.2 Patente | 4.3 Nº BR1020120331284 | 4.4 Data: 21.12.2012

5. Procurador (74)

5.1 Nome: FERNANDA LAVRAS COSTALLAT SILVADO

5.2 CNPJ/CPF: 295.166.068-57 5.3 API/OAB: 210.899

5.4 Endereço Completo: PROCURADORIA GERAL DA UNICAMP, CAMPINAS - SP

5.5 CEP: 13083-970

5.6 Telefone: 19 3521-4766 5.7 Fax: 19 3289-4766 5.8 E-mail:proc-geral@pg.unicamp.br

6. Apresentação ou modificação da Listagem de Sequências Biológicas (documentos anexados)(se houver):

☐ Listagem de sequências em arquivo eletrônico: nº de CDs ou DVDs (original e cópia).

☐ Código de controle alfanumérico no formato de código de barras: fls.

☐ Listagem de sequências em formato impresso: fls.

☐ Declaração de acordo com o artigo da Resolução INPI nº 228/09: fls.

INPI **Formulário 1.02 – Petição ou Requerimento, relacionado com pedido, patente ou certificado de adição (folha 1/2)**

7. **Apresenta / Requer** (continuação)

(Assinale o(s) itens que se aplica(m) ao seu caso):

(deverá ser indicado o nº total de somente uma das vias de cada documento)

		O que se requer / apresenta	folhas
☐	7.1	Modificações no Relatório Descritivo	
☐	7.2	Modificações nas Reivindicações	
☐	7.3	Modificações nos Desenhos	
☐	7.4	Modificações no Resumo	
☐	7.5	Caducidade da Patente/Certificado de Adição	
☐	7.6	Contestação de Caducidade/Nulidade	
☐	7.7	Cópia Oficial do pedido depositado	
☐	7.8	Cumprimento ou Contestação de Exig. RPI , de	
☐	7.9	Desarquivamento, arquivado na RPI , de	
☐	7.10	Documento de Prioridade	
☐	7.11	Exame do pedido com reivindicações	
☐	7.12	Expedição da Carta Patente / Certificado de Adição	
☒	7.13	Guia(s) de Recolhimento (uma para cada serviço)	1
☐	7.14	Manifestação s/ Parecer RPI , de	
☐	7.15	Nulidade do Patente / Certificado de Adição	
☒	7.16	Procuração	1
☐	7.17	Publicação Antecipada	
☐	7.18	Recurso contra o Indeferimento	
☐	7.19	Recurso, (outros)	
☐	7.20	Renúncia da Patente	
☐	7.21	Restauração de pedido / patente	
☐	7.22	Retirada do pedido	
☐	7.23	Subsídios ao Exame Técnico	
☐	7.24	Oferta de Licença	
☒	7.25	Outros que não aqueles definidos no campo 6 (especificar): ORDEM CORRETA DOS INVENTORES - EM DUAS VIAS	01

8. **Total de folhas anexadas (referentes aos campos 6 e 7):** 3 **fls.**

9. **Declaro, sob penas da Lei, que todas as informações acima prestadas são completas e verdadeiras.**

CAMPINAS, SP, EM 04 DE FEVERERO DE 2013

Local e Data

Assinatura e Carimbo

Fernanda Lauras Costallat Silvado
Procuradora de Universidade Subchefe
Matrícula nº 28.574-2
OAB/SP nº 210.803

INPI **Formulário 1.02 – Petição ou Requerimento, relacionado com pedido, patente ou certificado de adição (folha 2/2)**

1 Continuação dos dados do depositante/interessado:

1.2 Qualificação: UNIVERSIDADE ESTADUAL DE CAMPINAS – UNICAMP, pessoa jurídica de direito público, autarquia estadual devidamente inscrita no CNPJ sob nº 46.068.425/0001-33 e isenta de inscrição estadual.

1.4 Endereço completo: Cidade Universitária "Zeferino Vaz" – Distrito de Barão Geraldo, em Campinas – SP – CEP 13083-970

INOVA, em 04 de Fevereiro de 2013

Ao
INPI – INSTITUTO NACIONAL DA PROPRIEDADE INDUSTRIAL

Em relação ao processo abaixo:

21.12.12 – BR 10 2012 033128 4
MÉTODO PARA GERAÇÃO DE CHAVES BASEADO EM ALGORITMOS GENÉTICOS
WU FENG CHUNG, CLÁUDIO SADDY RODRIGUES COY, RENATO BOBSIN MACHADO, HUEI DIANA LEE, JOÃO JOSÉ FAGUNDES, RAQUEL FRANCO LEAL, MARIA DE LOURDES SETSUKO AYRIZONO, EVERTON ALVARES CHERMAN e JOYLAN NUNES MACIEL
FCM/UNIOESTE

Solicitamos a inserção dos inventores na ordem correta, que é a seguinte: RENATO BOBSIN MACHADO, WU FENG CHUNG, HUEI DIANA LEE, CLÁUDIO SADDY RODRIGUES COY, JOÃO JOSÉ FAGUNDES, JOYLAN NUNES MACIEL, RICHARDSON FLORIANI VOLTOLINI, ANDRÉ GUSTAVO MALETZKE, RAQUEL FRANCO LEAL , MARIA DE LOURDES SETSUKO AYRIZONO e EVERTON ALVARES CHERMAN.

Atenciosamente

Fernanda Lauras Costallat Silvado
Procuradora de Universidade Subchefe
Matrícula nº 28.574-7

Rua Roxo Moreira, 1831, Cidade Universitária "Zeferino Vaz" – Distrito de Barão Geraldo - CEP 13083-970 - Campinas - SP
Fone (19)3521-5015 - Fax (19)3521-5210
E-mail: ciro@inova.unicamp.br - http://www.inova.unicamp.br

MÉTODO PARA GERAÇÃO DE CHAVES BASEADO EM ALGORITMOS GENÉTICOS

Campo da invenção

O presente pedido de patente de invenção se refere a um novo método computacional, baseado em *software,* para a geração de chaves secretas que podem ser utilizadas por diferentes aplicações. O método consiste em um algoritmo computacional, inspirado em conceitos da Teoria da Evolução das Espécies, para a geração de chaves secretas, as quais podem ser empregadas na área da criptografia e em sistemas que manipulam dados digitais para aumentar do nível de segurança no acesso as informações, sejam estas compostas por dados, imagens, fluxos de áudio e de vídeo, etc. Essas chaves também podem ser aplicadas para outras finalidades, tais como para geração de senhas, identificação de *streamings*, proteção de arquivos, entre outras.

Fundamentos da invenção

A evolução tecnológica tem estimulado o aumento do uso de recursos computacionais em diversas as áreas do conhecimento. Cada vez mais aplicativos baseados em *softwares* estão sendo utilizados em dispositivos eletrônicos, tais como *tablets*, celulares, relógios, câmeras, equipamentos da área médica, veículos, entre outros. Uma das preocupações que surgem a partir desse cenário é a proteção e segurança de informações e de procedimentos. Associado a essa questão, verifica-se um aumento das violações cibernéticas, envolvendo acesso à informações digitais por meio de interceptações indevidas, permitindo o acesso, a leitura e a cópia não autorizada de dados.

O problema supracitado é mais grave quando os sistemas manipulam informações com caráter sigiloso, as quais têm sido crescentemente transformadas e digitalizadas para o universo computacional. Nesse contexto, uma das áreas que endereçam tal problema é a Segurança da Informação, especificamente em relação a confidencialidade, que consiste em uma

propriedade que limita o acesso a informação para somente aquelas entidades legitimamente autorizadas pelo proprietário da informação (Tanenbaum, 2011).

Desse modo, é importante o delineamento de métodos computacionais que possam contribuir para aumentar o nível de segurança no acesso a essas informações confidenciais. Um dos objetivos da Criptografia é a de garantir confidencialidade e, nesse sentido, diversos modelos de segurança que protegem e aumentam a confidencialidade das informações foram criados. Tais modelos são conhecidos como métodos criptográficos e trabalham com a geração e/ou utilização de chaves criptográficas (ou chaves-secretas) para garantir o acesso as informações protegidas.

Alguns métodos criptográficos oferecem maior nível de segurança e, desse modo, também exigem maior capacidade de processamento para cifrar e/ou decifrar dados por meio da utilização de chaves-secretas. Sendo assim, existem métodos que não podem ser utilizados em qualquer dispositivo eletrônico, com restrições de desempenho e *hardware*, ou seja, principalmente aqueles com menor capacidade de processamento.

A partir da identificação do aumento de problemas relacionados a confidencialidade de informações, e considerando as invenções de métodos criptográficos e de geração de chaves-secretas, definiu-se, por meio desta invenção, um novo método computacional que consiste num algoritmo original para geração de chaves-secretas, de baixo custo de processamento, aplicável para ampliar a o nível de confidencialidade das informações em sistemas baseados em computador. Ao longo do texto os termos chave-secreta e chave serão utilizados com o mesmo significado.

O método proposto neste documento não está limitado a aplicações relacionadas à criptografia, podendo ser utilizada para qualquer tipo de aplicação que necessite uma chave ou identificação com alto grau de segurança. Dentro desse gama de possíveis aplicações pode-se citar a publicação de *streaming*, geração de senhas fortes, proteção de arquivos, geração de chaves para serem utilizadas por algoritmos criptográficos, entre outras.

Atualmente, no estado da técnica, existem diversos trabalhos que se valem do conceito de criptografia e geração de chaves-secretas para desenvolver tecnologias que aumentam a confidencialidade em sistemas computacionais. Neste pedido de patente apresenta-se um método computacional, de baixo custo operacional, que agrega características originais, descritas neste documento, para geração de chaves-secretas únicas e que podem ser aplicadas para distintas finalidades.

A título de se determinar o estado da técnica e fundamentar o presente pedido de patente de acordo com o item 15.1.2 do Ato normativo 127/97 do INPI, segue abaixo uma relação de patentes e pedidos de patentes e artigos que versam sobre a mesma área do conhecimento do presente pedido de patente.

A patente **US7406175-B2 (WO03/090185)** descreve um método que utiliza equipamentos (*hardware*) para a geração de chaves-secretas. A segurança da chave é assegurada prevenindo a utilização de circuitos projetados, ou mesmo de pessoas, que consigam ler e decifrar o valor da chave-secreta. Nessa invenção os circuitos geradores de números aleatórios criam números aleatórios de acordo com diferentes relógios (**CLK1**, **CLK2**, **CLK3**). Um circuito aritmético opera sobre os números aleatórios criados nos geradores para produzir um número aleatório de **N bits** como saída. Este número é adquirido por meio de um seletor de chaves e é armazenado em um registrador a partir de um sinal que habilita a aquisição. Tal processo é gerenciado por contadores de monitoramento de tempo, ou seja, distintos relógios do computador, sendo ao final produzida uma chave em *hardware* que é única e secreta. As chaves secretas geradas por esse invento podem ser aplicadas para criptografia (codificação) ou decodificação em aparelhos equipados com tal gerador e método de geração.

O invento existente aplica componentes arquiteturais e define um método de geração das chaves secretas, usando números aleatórios a partir de valores dados pelo relógio, sendo tais chave-secretas armazenadas em *hardware*. A invenção não realiza a geração das chaves secretas em *software*,

e é totalmente atrelada a utilização de equipamentos de *hardware*, diferenciando-se do presente pedido de patente. A invenção proposta neste documento não trabalha somente com componentes aleatórios, mas também aplica um componente de mutação inspirado na Teoria da Evolução das Espécies, permitindo maior dinamismo na geração de chaves secretas. Outra vantagem da tecnologia proposta consiste em sua implementação ser realizada por meio de *software*, pois, desse modo, a tecnologia pode ser aplicada em distintos dispositivos, de modo independente do *hardware* e de sistema operacional, ampliando sua aplicabilidade. Adicionalmente, a tecnologia proposta não utiliza recursos computacionais que exijam grande poder de processamento, podendo ser executada em qualquer computador atual, assim como em outros dispositivos móveis. Resumidamente, a patente US7406175-B2 trata-se de uma tecnologia distinta em relação ao presente pedido, tanto em seu material quanto ao método aplicado, bem como sua finalidade e aplicabilidade.

Na patente **US7739501-B2** é apresentado um produto que consiste em um programa de computador que realiza a geração de chaves criptográficas secretas, nela denominada rótulo, para uso na troca de informações entre membros de organizações em matrizes e filiais. O programa reside em um computador cujos dados armazenados podem ser lidos somente por dispositivos mecânicos. As instruções configuradas para o computador são: produzir uma chave de leitura-escrita usando ao menos um valor base; criar uma chave de escrita usando a chave de leitura e escrita produzida; combinar um primeiro identificador, unicamente associado com a primeira organização, e um segundo identificador, unicamente associado com o rótulo chave a ser produzido. Para a criptografia foi aplicada uma função *hash* de único sentido, a qual utiliza um gerador não determinístico de *bits* aleatórios, com o objetivo de produzir uma chave pura, associando-a com as chaves de leitura-escrita e de escrita para formar rótulo final (chave criptográfica final).

A invenção existente é aplicada especificamente para a área de criptografia. Assim como o processo de leitura da chave gerada, ela é realizada

por meio de dispositivos mecânicos (*hardware*), diferenciando-se da invenção proposta que trabalha com *software* tanto para a leitura quanto para a manipulação das chaves secretas. Nesse sentido, a tecnologia proposta pode ser aplicada em qualquer dispositivo de *hardware* computacional, tornando a invenção proposta independente e com maior gama de aplicabilidade. Em segundo lugar, o método para a geração das chaves secretas da patente **US7739501-B2** é distinto do proposto neste pedido, pois, o mesmo associa as chaves secretas aos nomes de domínios, que representam as organizações. Além disso, é utilizado um gerador não-determinístico de *bits* aleatórios, o que não ocorre no presente pedido no qual são aplicados conceitos de Seleção Natural e Genética. De modo resumido, o propósito da invenção, o método de geração de chaves secretas, que consiste em uma etapa da invenção, e os materiais empregados são distintos do presente pedido de patente.

A patente **US7372961-B2** refere-se a sistemas de criptografia de chave pública, mais particularmente, ao método geração de chaves dentro destes sistemas. A estrutura básica de um sistema de criptografia de chave pública é bem conhecida e se tornou ubíqua com a segurança em sistemas de comunicação de dados. Esses sistemas usam uma chave privada k e uma chave pública correspondente αk onde α é um gerador do grupo. Assim, um lado pode criptografar a mensagem m com a chave pública dos destinatários pretendidos e o destinatário pode solicitar sua chave privada para decifrar m.

Em termos gerais, a patente descrita provê uma técnica de geração de chaves em que qualquer desvio é eliminado durante a seleção da chave. Além disso, são descritos os principais elementos comuns aos cenários preferenciais, onde existe uma rede de comunicação e dois dispositivos eletrônicos (computadores, celulares, ou qualquer outro), os quais possuem segurança criptográfica baseadas em *hash*, tal como o *Secure Hash Algorithm* - SHA-1.

Na patente existente, **US007372961-B2,** foi desenvolvido um método para garantir a geração e o acesso a chaves secretas, e não o um

método para geração dessas chaves. No exemplo citado é utilizado o SHA-1, um conhecido método de criptografia.

De modo resumido, o objetivo e o método diferem do presente pedido de patente, pois o objetivo não consiste em gerar as chaves, mas sim, em garantir que novas chaves sejam geradas em casos de não conformidade com os parâmetros do sistema. O método proposto nesta invenção trata especificamente de um método para a geração de chaves secretas, de propósito geral, aplicando operadores aleatórios e de mutação, aplicando técnicas de algoritmos genéticos e seleção natural, para dar maior dinamismo a geração de chaves, assim como para permitir configurações específicas em função da aplicação a que a chave será destinada. Adicionalmente os processos realizados no método proposto são realizados totalmente por *software*, podendo ser aplicado em qualquer configuração de *hardware* e sistema operacional computacional. Desse modo o método proposto possui diversas características direcionas a ampliar o seu rol de aplicabilidades.

A patente **EP2120389-A1 (WO2008/113279)** apresenta a invenção de um método para geração de uma chave de sessão e dispositivos de comunicação. O método consiste na geração de uma chave pública e outra privada, de longo prazo, nas duas partes da comunicação. A parte *X* seleciona uma chave privada aleatoriamente, assim como a parte *Y* seleciona outra chave privada aleatoriamente. A parte *X* usa a chave secreta de longo prazo e sua chave secreta aleatória para calcular e enviar a mensagem para *Y*. Após isso, a parte *Y* usa sua chave secreta de longo prazo e sua chave secreta aleatória para calcular e enviar a mensagem *Y* para *X*. Desse modo, a parte *X* calcula a sua chave secreta de sessão *Kx* e a parte *Y* calcula sua chave secreta de sessão *Ky*.

A solução descrita possui um gerenciador de chaves central que cria e manipula as chaves utilizando algoritmos de mapeamento em conjunto com uma matriz de Fatores de Chaves Públicas e matrizes de Fatores de Chaves Públicas/Privadas. Além disso, na patente existente são apresentados diversos cenários de aplicação do método e os dispositivos de comunicação

empregados. Uma característica da patente **EP2120389-A1** é que as chaves de cada parte da comunicação são elaboradas de acordo com parâmetros do sistema de criptografia. Além disso, a chave de sessão gerada após a comunicação das partes é variável, evitando grande dependência do gerenciador de chaves central.

Os conceitos e procedimentos de geração da chave da patente existente são distintos do presente pedido de patente, pois utilizam matrizes de fatores e algoritmos de mapeamento. Além disso, são geradas diversas chaves dentre as quais uma é escolhida aleatoriamente para ser utilizada na criação da chave de sessão para a comunicação.

De modo resumido, a patente apresentada se distingue da invenção proposta em relação ao método de geração das chaves, aos dispositivos utilizados, e, principalmente em relação ao objetivo, que consiste em gerar uma chave de sessão para comunicação entre dois sistemas, e não a geração de chave secreta aplicável em qualquer cenário. Ambas as patentes podem ser utilizadas em conjunto, de forma de a patente **EP2120389-A1** pode aplicar em seus cenários de uso o método definido no presente pedido de invenção.

Outros diferenciais da tecnologia proposta consistem na aplicação não somente de fatores aleatórios para geração das chaves secretas, mas também de mutação. A invenção proposta pode ser aplicada para distintas finalidades, sendo que as características da chave a serem geradas podem ser configuradas em função das particularidades da aplicação. Outra particularidade da tecnologia proposta é que a mesma é implementada totalmente em *software* e aplicando operações de baixo custo de processamento.

Breve descrição da invenção

Refere-se o presente pedido de patente a um novo método computacional, por meio de *software*, cuja finalidade é a geração de chaves secretas que possam ser aplicadas de modo genérico para distintas

finalidades. Esse pedido de patente consiste em um **Método para Geração de Chaves Baseado em Algoritmos Genéticos.**

A chave gerada por meio do método proposto pode ser utilizada para qualquer fim que necessite uma identificação, denominada neste documento como **chave** ou **chave secreta**, que seja difícil de ser quebrada por invasores (*crackers*), principalmente aplicando-se métodos de força bruta.

Algumas possíveis aplicações do método incluem a sua utilização para a publicação de *streamings* de vídeo e/ou áudio por meio da Internet; para chaves de métodos criptográficos; como senhas de sistemas computacionais e redes; para a proteção de arquivos; entre outros.

O presente pedido de patente foi concebido baseado no conceito da Teoria da Evolução das Espécies aplicado a métodos computacionais.

O **Método para Geração de Chaves Baseado em Algoritmos Genéticos** foi definido conforme o sistema descrito na Figura 1, sendo este composto pelos seguintes elementos:

1. **Componente Gerador de Números Aleatórios - GNA** (2): responsável pela geração de números aleatórios, aplicando o operador de aleatoriedade inspirado na Teoria de Evolução das Espécies;

2. **Componente de Concatenação - CC** (3): possui a função de receber **N** números aleatórios (com número de dígitos variável), converter para o formato texto e por fim retornar uma **chave** consistindo na concatenação desses **N** números aleatórios;

3. **Componente de Mutação - CM** (4): O CM é derivado dos princípios de mutação de algoritmos genéticos, inspirados na Teoria de Evolução das Espécies. No caso do presente método, o CM recebe uma **chave1** como entrada e aplica uma mutação de 50% gerando uma **chave2**;

4. **Componente de Concatenação Final - CCF** (5): O CCF recebe uma chave como entrada, no caso deste método foi aplicada especificamente a **chave2**, e são acrescentadas algumas características adicionais para dificultar a descoberta da chave por técnicas maliciosas;

5. **Chave Final - CF** (6): Consiste na **chave** gerada a partir de todas as etapas do método e que poderá ser aplicada para as mais diversas aplicabilidades, conforme apresentado inicialmente.

A partir das definições gerais e da apresentação dos componentes que são aplicados no método, a seguir detalha-se a sequencia de execução do método, representado por três fases:

Fase 1: Geração da primeira Chave (chave 1)

Nesta fase é gerada a **chave1** por meio da aplicação de componentes aleatórios. Para isso são executados os seguintes procedimentos:

1. Gera-se **N** números aleatórios utilizando o Componente Gerador de Números Aleatórios - GNA (2). Cada um desse números deve ficar dentro dos limites entre **Y** e **K**. Cada um desses valores numéricos pode conter uma quantidade de caracteres variando entre o número de dígitos de **Y** e o número de dígitos de **K;**

2. O resultado da Fase 1 (**chave 1**) consiste na concatenação dos caracteres gerados pelos **N** números aleatórios, convertidos para formato texto. Esse procedimento é realizado pelo Componente de Concatenação (3).

Fase 2: Geração da segunda Chave (chave 2)

Nesta fase gera-se a **chave2 por meio do Componente de Mutação (4)**, a qual utilizar o operador de mutação sobre 50% da **chave1**. A seguir apresenta-se este procedimento:

1. Todos os caracteres da **chave1** são percorridos, de modo que:

   i. Se a posição do caracter na **chave1** for par, esse caracter é adicionado a **chave2**;

   ii.Se a posição do caracter na **chave1** for impar, será adicionado na **chave2** um caracter ASCCII aleatório.

Fase 3: Geração da Chave Final

A **chave final** é gerada pelo Componente de Concatenação Final (5), sendo composta pelos seguintes elementos:

i. Hora, minutos, segundos e milissegundos da geração da chave;

ii. chave2.

Parâmetros de Configuração:

Esse método pode ser aplicado para distintos propósitos e por conseguinte os valores de **N**, **Y** e **K** podem ser personalizados conforme critério de segurança da aplicação. Neste caso, especificamente, foram adotados os valores **N=300**, **Y=0**, **k=9999999999** e operador de mutação de **50%**.

Características do Método Proposto

A tecnologia proposta por meio deste pedido de patente diferencia-se dos métodos existentes por não ser direcionado a uma aplicação específica, e de modo contrário, podendo ser aplicada para distintas finalidades para segurança de informações e de procedimentos. Como exemplos de possíveis aplicações da tecnologia pode-se citar a utilização dessas chaves secretas para métodos criptográficas, a aplicação das chaves geradas como identificador para publicação de *streamings*, a sua utilização para a geração de senhas, a sua aplicação para a proteção de arquivos, entro outros.

Outro diferencial da tecnologia proposta consiste na definição e na implementação do método totalmente por *software*, desse modo não sendo necessário atrelar a utilização da solução a existência de componentes específicos de *hardware*, além de ser independente de plataforma e de sistema operacional.

Associado a essas características de dinamicidade e portabilidade apresentadas, o método proposto no presente documento aplica conceitos provenientes da Teoria de Evolução das Espécies, tais como operadores de aleatoriedade, mutação e cruzamento; permitindo assim a geração de chaves

secretas com altos níveis de segurança e sem a utilização de operações matemáticas que exijam alto poder de processamento.

Em função do tipo de aplicação e do grau de segurança necessário, o método foi concebido para permitir configurações que irão influenciar no tamanho da chave, grau de aleatoriedade e índices de mutação. Desse modo, a tecnologia se torna ainda mais flexível para ser aplicada a propósitos diversificados.

Quanto ao tempo de utilização das chaves geradas pelo método, essas podem ser utilizadas tanto para curto quanto para longo prazo, pois o tempo para quebra da chave por meio de técnicas de força bruta, para a configuração padrão do método, é de no mínimo ria $\mathbf{10^{338}}$ anos.

Breve descrição das figuras

A Figura 1 demonstra um diagrama do método para a geração de chaves secretas baseada em algoritmos genéticos (1); composto por um Componente Gerador de Números Aleatórios (2), um Componente de Concatenação (3), um Componente de Mutação (4), um Componente de Concatenação Final (5) e pela Chave Final (6).

A Figura 2 demonstra o Componente Gerador de Números Aleatórios.

Na Figura 3 é apresentado o Componente de Concatenação.

A Figura 4 demonstra o Componente de Mutação.

Na Figura 5 apresenta-se o Componente de Concatenação Final.

Descrição detalhada da invenção

Para alcançar os objetivos descritos na breve descrição da invenção definiu-se o **Método para Geração de Chaves Baseado em Algoritmos Genéticos,** o qual consiste na utilização de conceitos relacionados a algoritmos genéticos (Teoria da Evolução das Espécies) e recursos computacionais para a geração de chaves secretas que sejam difíceis de serem quebradas por meio das técnicas computacionais atuais, principalmente por meio de métodos de força bruta.

O presente pedido de patente foi concebido baseado no conceito da Teoria da Evolução das Espécies aplicado a métodos computacionais, os quais originaram diversos subgrupos como os Algoritmos Genéticos e a Programação Genética. A principal característica desses métodos é a aplicação dos conceitos de Seleção Natural e Genética para a busca por soluções de problemas complexos, utilizando para tanto conceitos como indivíduo, gene, lócus, alelo, genótipo, fenótipo, cromossomo e genoma. Essa busca pela solução é dada, de modo geral, pela evolução da população (conjunto de indivíduos) por meio da aplicação de operadores genéticos, como *crossover*, mutação e cruzamento, bem como de componente aleatório para a manutenção da diversidade da população.

O **Método para Geração de Chaves Baseado em Algoritmos Genéticos** foi delineado contemplando métodos e recursos computacionais e conceitos de Algoritmos Genéticos. Os componentes que fazem parte da invenção são apresentados na Figura 1, a partir da qual serão descritos os detalhes de seus elementos constituintes e dos métodos aplicados. Embora seja apresentada uma configuração específica, o método pode ser executado de modos diversos em face de personalizações que venham a ser aplicadas. Para isso podem-se personalizar alguns parâmetros, tais como quantidade de números aleatórios, valor mínimo e máximo permitidos para a geração de números aleatórios e o percentual de mutação da chave intermediária (denominada **chave1** neste documento).

O primeiro elemento constituinte do modelo é o Componente Gerador de Números Aleatórios - GNA (2), o qual possui a função de utilizar o operador de aleatoriedade e criar números aleatórios dentro do conjunto de números compreendidos entre um limite inferior e um limite superior. Esses limites, inferior e superior, podem ser definidos em função do objetivo de aplicação do método, sendo parâmetros configuráveis. Esses limites são representados na Figura 1 pelas variáveis de entrada **Y** e **K** respectivamente. Desse modo, cada vez que o GNA executa, pode gerar um número que além de variar o valor, também pode variar o número de dígitos. Cada número

gerado possuirá o número de dígitos variando entre a quantidade de dígitos de **Y** e a quantidade de dígitos de **K**. O GNA foi inspirado nos operadores de aleatoriedade dos Algoritmos Genéticos.

O Componente de Concatenação - CC (3) por sua vez é responsável pelo recebimento de **N** números aleatórios e pela geração de uma chave (denominada neste documento de chave1). O procedimento realizado pelo CC (3) consiste em solicitar um conjunto de **N** números aleatórios ao GNA (2). Posteriormente o CC (3) recebe esses **N** números aleatórios, os converte unitariamente para o formato texto e por fim concatena todos esses números em modo texto. O produto gerado pelo CC (3) foi denominado **chave1**. O valor de **N** também é parametrizado e pode ser definido em função das necessidades específicas de tamanho de chave e segurança que a aplicação necessite.

Após a geração da **chave1** utiliza-se outro elemento constituinte, denominado Componente de Mutação - CM (4). O CM (4) também foi inspirado nas operações genéticas aplicadas para a busca da evolução da população, especificamente pelos operadores de mutação. O CM (4) recebe uma chave como entrada, tendo sido aplicado neste método especificamente a **chave1** gerada pelo CC (3) e GNA (2), e gera uma chave de saída aplicando um conjunto de mutações sobre a chave de entrada. O percentual de mutação pode ser variável, tendo-se aplicado neste método específico um fator de aleatoriedade de 50%, o que significa de a metade dos caracteres presentes na chave de entrada sofrem modificações para gerar a chave de saída. Neste documento especificamente nomeou-se a chave gerada pelo CM (4) como **chave2**.

O Componente de Concatenação Final - CCF (5) recebe uma chave como entrada e agrega algumas características, também aplicando operadores evolutivos e de mutação. Especificamente neste trabalho o CCF (5) recebe como entrada a chave2 e gera uma chave final composta pela data, hora, minuto, segundo e milissegundo que a chave foi gerada. Posteriormente

o CCF (5) concatena a **chave2** a chave final e essa é o produto final do método.

Ainda na Figura 1 apresenta-se Chave Final - CF (6) que consiste no produto final gerado pelo método e que será aplicado para as mais distintas finalidades, entre as quais para a publicação de *streamings* de vídeo e/ou áudio por meio da Internet; para chaves de métodos criptográficos; como senhas de sistemas computacionais e redes; para a proteção de arquivos; como chave em sistemas de autenticação, entre outros.

A partir da descrição detalhada dos componentes do método expostos na Figura 1, a seguir apresenta-se o método computacional concebido para a implementação do modelo. O método pode ser representado por três fases:

Fase 1: Geração da primeira Chave (chave 1)

Nesta fase é gerada a **chave1** por meio da aplicação de componentes aleatórios. Para isso são executados os seguintes procedimentos:

1. Gera-se **N** números aleatórios utilizando o Componente Gerador de Números Aleatórios - GNA (2). Cada um desses números deve ficar dentro dos limites entre **Y** e **K**. Cada um desses valores numéricos pode conter uma quantidade de caracteres variando entre o número de dígitos de **Y** e o número de dígitos de **K;**

2. O resultado da Fase 1 (**chave 1**) consiste na concatenação dos caracteres gerados pelos **N** números aleatórios, convertidos para formato texto. Esse procedimento é realizado pelo Componente de Concatenação (3).

Fase 2: Geração da segunda Chave (chave 2)

Nesta fase gera-se a **chave2 por meio do Componente de Mutação (4)**, a qual utilizar o operador de mutação sobre 50% da **chave1**. A seguir apresenta-se este procedimento:

1. Todos os caracteres da **chave1** são percorridos, de modo que:

i. Se a posição do caracter na **chave1** for par, esse caracter é adicionado a **chave2**;

ii.Se a posição do caracter na **chave1** for impar, será adicionado na **chave2** um caracter ASCCII aleatório.

Fase 3: Geração da Chave Final

A **chave final** é gerada pelo Componente de Concatenação Final (5), sendo composta pelos seguintes elementos:

i. Hora, minutos, segundos e milissegundos da geração da chave;

ii. chave2.

Parâmetros de Configuração:

Esse método pode ser aplicado para distintos propósitos e, por conseguinte, os valores de **N**, **Y** e **K** podem ser personalizados conforme critério de segurança da aplicação. Neste caso, especificamente, foram adotados os valores **N=300**, **Y=0**, **k=9999999999** e operador de mutação de **50%**.

Análise de Segurança do Método para Geração de Chaves Baseada em Algoritmos Genéticos

Um dos objetivos de sistemas maliciosos e de invasores (*crackers*) é quebrar a segurança do sistema computacional. Um modo de obter êxito neste propósito consiste em utilizar algoritmos e técnicas computacionais para a descoberta de senhas, chaves criptográficas, identificações de *streamings*, entre outros. O método mais utilizado para buscar quebrar qualquer mecanismo de segurança é a utilização de algoritmos de força bruta, onde o propósito do invasor é tentar todas as combinações possíveis até quebrar uma senha ou chave de segurança.

Em função desse contexto, os diferentes métodos criptográficos, assim como métodos para geração de chaves secretas são analisados sob o prisma do tempo necessário para a segurança ser quebrada aplicando técnicas

de força bruta. Desse modo, na sequencia, será apresentada uma análise dos níveis de segurança do **método para Geração de Chaves Baseado em Algoritmos Genéticos** proposto neste documento.

A tentativa de quebra de segurança do **método para Geração de Chaves Baseado em Algoritmos Genéticos** poderia ser realizada, por invasores, por meio da identificação do componente mais elaborado da **chave final**, ou seja, a **chave2**. Para demonstrar a segurança do presente método, a seguir são apresentados os cálculos do tempo necessário para a identificação e quebra da **chave2**. O melhor e o pior caso do algoritmo são considerados em função da abordagem de invasão "força-bruta", na qual todas as alternativas de nomes são testadas pelo suposto invasor.

Também é importante ressaltar que a análise será realizada considerando os valores de configuração adotados especificamente nesta descrição do método, que são **N=300**, **Y=0**, **k=9999999999** e **operador de mutação de 50%**.

A **chave1** é gerada utilizando a concatenação de **300** números aleatórios e, por isso, ela contém tamanho variável. O pior caso do algoritmo e o mais simples para o invasor é o caso em que todos os **300** números aleatórios da **chave1** sejam gerados contendo apenas um único dígito. Desse modo, a **chave1** seria composta por **300** caracteres. No melhor caso para o algoritmo e o caso de maior complexidade para o invasor é a situação em que todos os **300** números aleatórios da **chave1** sejam gerados com o número máximo de algarismos. Nesse caso, a **chave1** seria composta por um total de **3000** caracteres. Por fim, a **chave2** é gerada substituindo cada caracter decimal de posição ímpar da **chave1** (**mutação de 50%**) por um caracter ASCII aleatório dentre os **256** possíveis.

Desse modo, considerando inicialmente o caso mais simples para o invasor, são necessárias $\mathbf{256}^{\mathbf{300}} \approx \mathbf{10}^{\mathbf{722}}$ tentativas para cobrir todas as possibilidades da **chave2**. Para simplificar os cálculos, ressalta-se que cada tentativa de quebra do algoritmo pode ser realizada por uma operação de ponto flutuante do processador. Considerando um supercomputador com

processamento de **1000 TFlops**[1] (10^{15} operações de ponto flutuante por segundo), seriam necessários $\mathbf{10^{722-15} = 10^{707}}$segundos para que esse supercomputador realizasse tentativas sobre todas as possibilidades de geração da **chave2** no caso mais simples. Levando em conta que um ano contém aproximadamente $\mathbf{3.158 \times 10^{7}}$ segundos e arredondando por simplicidade para $\mathbf{10^{8}}$segundos, seriam necessários $\mathbf{10^{699}}$ anos para a quebra da **chave2** utilizando essa abordagem.

Para o caso em que a **chave1**, e consequentemente também a **chave2**, seja gerada com **3000** caracteres, seriam necessárias $\mathbf{256^{3000} \approx 10^{7224}}$ tentativas para cobrir todas as combinações possíveis. Nesse caso, seguindo os cálculos de maneira análoga ao caso mais simples, seriam necessários $\mathbf{10^{7201}}$ anos para efetuar todas as tentativas de quebra da segurança da **chave2**.

Além das duas situações anteriormente mencionadas, também se considerou a situação hipotética de que o invasor conheça de antemão a **chave1** e também o mecanismo de geração da **chave2**, *i.e.*, o invasor sabe que precisa descobrir apenas os dígitos ímpares da **chave2**, gerados aleatoriamente com caracteres ASCII. Desse modo, cai pela metade a quantidade de caracteres a serem descobertos, tanto no caso mais simples quanto do caso mais complexo. Assim, no caso mais simples seriam necessárias $\mathbf{256^{150} \approx 10^{361}}$ tentativas para cobrir todas as possibilidades, o que, também de maneira análoga aos cálculos anteriores, gastaria $\mathbf{10^{338}}$ anos para ser realizada. Para o caso mais complexo seriam gastos $\mathbf{10^{3589}}$ anos para quebrar a **chave2**.

Para se ter uma ideia da ordem de grandeza desses números, ressalta-se que $\mathbf{10^{9}}$ anos é igual a um bilhão de anos, o que demonstra a segurança do sistema e a necessidade de estratégias muito mais complexas por parte do invasor.

---

[1] Um supercomputador com essa capacidade de processamento estaria entre os 10 computadores mais rápidos do mundo segundo o ranking disponibilizado em http://www.top500.org/list/2012/06/100 em Junho de 2012.

Além dos dados analisados em relação a **chave1** e a **chave2**, a **chave final** ainda inclui outras importantes características que dificultam a ação de possíveis invasores, como a inclusão da **data**, **hora**, **minuto**, **segundo** e **milissegundo** que a chave foi gerada.

Outro fator que dificulta a ação dos invasores é que cada chave gerada possuir um número variável de caracteres, sendo necessário por força bruta, testar todas as combinações para cada configuração possível. No caso em análise cada chave gerada pode ter um número de caracteres variando entre 300 e 3000, o que dificulta muito a ação dos invasores.

Desse modo verifica-se que o método proposto, por meio deste pedido de invenção, possui as seguintes características principais: não necessidade nenhum *hardware* especial, o algoritmo não aplica operações matemáticas complexas e tempo elevado de processamento, além de possuir alto índice de confiabilidade em relação a segurança.

REIVINDICAÇÕES

1. Método para geração de chaves baseado em algoritmos genéticos **caracterizado por** compreender basicamente três fases, sendo elas:

   Fase 1: Geração da primeira Chave (chave 1)

   Nesta fase é gerada a chave1 por meio da aplicação de componentes aleatórios;

   Fase 2: Geração da segunda Chave (chave 2)

   Nesta fase gera-se a chave2 por meio do Componente de Mutação (4), a qual utilizar o operador de mutação sobre 50% da chave1;

   Fase 3: Geração da Chave Final

   A chave final é gerada pelo Componente de Concatenação Final (5).

2. Método para geração de chaves baseado em algoritmos genéticos, de acordo com a reivindicação 1, **caracterizado por** na fase 1 serem executados os seguintes procedimentos:

   a. Gera-se **N** números aleatórios utilizando o Componente Gerador de Números Aleatórios - GNA (2), cada um desse números deve ficar dentro dos limites entre **Y** e **K**, cada um desses valores numéricos pode conter uma quantidade de caracteres variando entre o número de dígitos de **Y** e o número de dígitos de **K**;

   b. O resultado da Fase 1 (chave 1) consiste na concatenação dos caracteres gerados pelos **N** números aleatórios, convertidos para formato texto, esse procedimento é realizado pelo Componente de Concatenação (3).

3. Método para geração de chaves baseado em algoritmos genéticos, de acordo com a reivindicação 1, **caracterizado por** na fase 2 ser executado o seguinte procedimento:

a. Todos os caracteres da chave1 são percorridos, de modo que:
    i. Se a posição do caracter na chave1 for par, esse caracter é adicionado a chave2;
    ii. Se a posição do caracter na chave1 for impar, será adicionado na chave2 um caracter ASCCII aleatório.

4. Método para geração de chaves baseado em algoritmos genéticos, de acordo com a reivindicação 1, **caracterizado por** na fase 3, Componente de Concatenação Final (5) é composto pelos seguintes elementos:
    a. Hora, minutos, segundos e milissegundos da geração da chave;
    b. chave2.
5. Método para geração de chaves baseado em algoritmos genéticos, de acordo com a reivindicação 2, **caracterizado por N**, **Y** e **K** poderem ter seus valores personalizados conforme critério de segurança da aplicação.
6. Sistema para geração de chaves **caracterizado por** compreender os seguintes elementos:
    a. Componente Gerador de Números Aleatórios - GNA (2);
    b. Componente de Concatenação - CC (3);
    c. Componente de Mutação - CM (4);
    d. Componente de Concatenação Final - CCF (5);
    e. Chave Final - CF (6).
7. Sistema para geração de chaves, de acordo com a reivindicação 6, **caracterizado por** a etapa "a" ser responsável pela geração de números aleatórios, aplicando o operador de aleatoriedade inspirado na Teoria de Evolução das Espécies.
8. Sistema para geração de chaves, de acordo com a reivindicação 6, **caracterizado por** a etapa "b" possuir a função de receber **N** números aleatórios (com número de dígitos variável), converter para o formato

texto e por fim retornar uma chave consistindo na concatenação desses **N** números aleatórios.

9. Sistema para geração de chaves, de acordo com a reivindicação 6, **caracterizado por** a etapa "c" ser derivada dos princípios de mutação de algoritmos genéticos, receber uma chave1 como entrada e aplicar uma mutação de 50% gerando uma chave2.
10. Sistema para geração de chaves, de acordo com a reivindicação 6, **caracterizado por** a etapa "d" receber a chave2 como entrada e serem acrescentadas algumas características adicionais para dificultar a descoberta da chave por técnicas maliciosas.
11. Uso do método descrito nas reivindicações de 1 a 5 **caracterizado por** ser na geração de chaves que podem ser utilizadas para distintas finalidades, tais como para a publicação de *streamings* áudio e vídeo, para algoritmos de criptografia, para geração de senhas, para proteção de arquivos, entre outros.

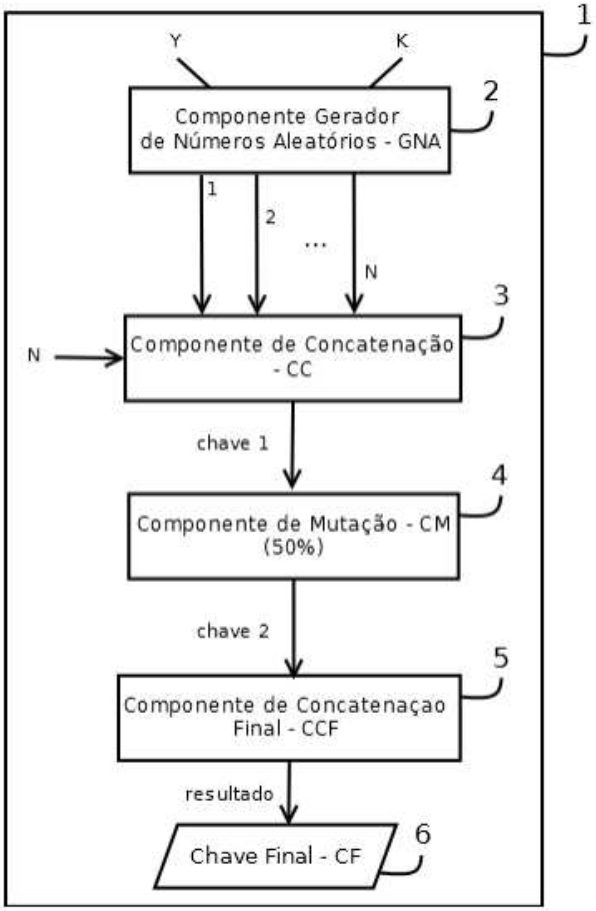

Figura 1

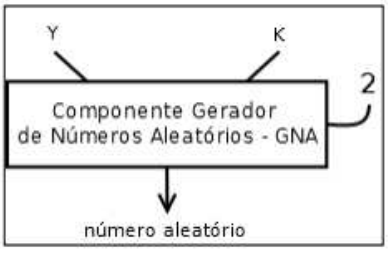

Figura 2

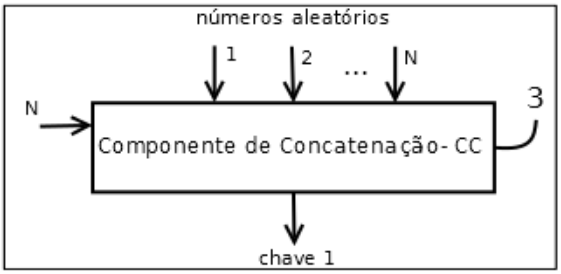

Figura 3

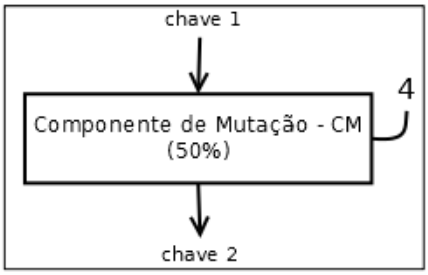

Figura 4

Figura 5

RESUMO

MÉTODO PARA GERAÇÃO DE CHAVES BASEADA EM ALGORITMOS GENÉTICOS

Refere-se o presente pedido de patente de invenção a um novo método computacional sistêmico para a geração de chaves secretas, inspirado na Teoria da Evolução das Espécies, especialmente na genética e seleção natural. Esse método permite que sejam definidos parâmetros importantes, como limite inferior e superior para geração de números aleatórios, assim como quantidade de números que irão contribuir para compor a chave e ainda índice de mutação que será aplicado no algoritmo.

Desse modo o método proposto pode ser aplicado para distintas finalidades, tais como para a aplicação como chaves de algoritmos de criptografia, para geração de senhas, para a proteção de arquivos, para publicação de *streamings* de áudio e vídeo, entre outros.

As principais vantagens do método proposto consistem em não necessitar nenhum *hardware* específico para ser executado, utiliza operações matemáticas simples e sem alto custo de execução, é configurável para trabalhar as variáveis e definir o grau de segurança desejado, e foi concebido com conceitos de algoritmos genéticos dificultando tentativas de invasão.

7. ARTIGO PROTOTYPE OF A COMPUTER SYSTEM FOR MANAGING DATA AND VIDEO COLONOSCOPY EXAMS

Original Article

Prototype of a computer system for managing data and video colonoscopy exams

Renato Bobsin Machado[1], Huei Diana Lee[2], Maria de Lourdes Setsuko Ayrizono[3], Raquel Franco Leal[3], Cláudio Saddy Rodrigues Coy[4], João José Fagundes[4], Feng Chung Wu[5]

[1]Attending Doctor's Degree program, Department of Surgery (D.M.A.D.) of the Service of Coloproctology at the Universidade Estadual de Campinas (UNICAMP) – Campinas (SP), Brazil; Professor and Researcher of the Laboratory of Bioinformatics (LABI) at the Universidade Estadual do Oeste do Paraná (UNIOESTE) – Foz do Iguaçu (PR), Brazil. [2]Doctor and Professor of Computer Science at UNIOESTE; Professor, Postgraduate Program of Dynamic and Energy Systems Engineering (PGESDE); General Coordinator of LABI at UNIOESTE – Foz do Iguaçu (PR), Brazil; Visiting Professor, Postgraduate Program of Surgery Sciences at the Faculdade de Ciências Médicas da UNICAMP – Campinas (SP), Brazil. [3]Doctor and Professor of the Department of Surgery (D.M.A.D.), Service of Coloproctology at UNICAMP – Campinas (SP), Brazil. [4]Doctor and Professor, Department of Surgery (D.M.A.D.), Service of Coloproctology at UNICAMP – Campinas (SP), Brazil. [5]Doctor and Professor and Researcher, Service of Coloproctology at the Faculdade de Ciências Médicas da UNICAMP – Campinas (SP), Brazil; Doctor and Professor at UNIOESTE and Coordinator of the Medical Area of LABI at UNIOESTE – Foz do Iguaçu (PR), Brazil.

Machado RB, Lee HD, Ayrizono MLS, Leal RF, Coy CSR, Fagundes JJ, Wu FC. Prototype of a computer system for managing data and video colonoscopy exams. **J Coloproctol**, 2012;32(1): 50-60.

ABSTRACT: **Objective**: Develop a prototype using computer resources to optimize the management process of clinical information and video colonoscopy exams. **Materials and Methods**: Through meetings with medical and computer experts, the following requirements were defined: management of information about medical professionals, patients and exams; video and image captured by video colonoscopes during the exam, and the availability of these videos and images on the Web for further analysis. The technologies used were Java, Flex, JBoss, Red5, JBoss SEAM, MySQL and Flamingo. **Results and Discussion**: The prototype contributed to the area of colonocospy by providing resources to maintain the patients' history, tests and images from video colonoscopies. The web-based application allows greater flexibility to physicians and specialists. The resources for remote analysis of data and tests can help doctors and patients in the examination and diagnosis. **Conclusion**: The implemented prototype has contributed to improve colonoscopy-related processes. Future activities include the prototype deployment in the Service of Coloproctology and the utilization of this model to allow real-time monitoring of these exams and knowledge extraction from such structured database using artificial intelligence.

Keywords: colonoscopy; telemedicine; exam management; remote patient monitoring; communication with hospital equipment.

RESUMO: **Objetivo**: Desenvolver um protótipo por meio de recursos computacionais para a otimização de processos de gerenciamento de informações clínicas e de exames de videocolonoscopia. **Materiais e Métodos**: Por meio de reuniões com especialistas médicos e computacionais, definiram-se os seguintes requisitos: gestão de informações sobre profissionais médicos, pacientes e exames complementares; aquisição dos vídeos e captura de imagens a partir do videocolonoscópio durante a realização desse exame, e a disponibilidade por meio da *Web* para análise posterior dessas imagens. As tecnologias aplicadas foram: Java, Flex, JBOSS, Red5, JBOSS SEAM, MySQL e Flamingo. **Resultados e Discussão**: O protótipo contribuiu para a área de colonocospia disponibilizando recursos para manutenção de histórico de pacientes, exames e imagens. O acesso à aplicação, por meio de *browser,* permite maior flexibilidade aos médicos e especialistas. Os recursos para análise remota de dados e exames podem auxiliar médicos e pacientes na realização de exames e diagnósticos. **Conclusão**: O protótipo implementado contribuiu para melhoria de processos relacionados a exames de videocolonoscopia. Trabalhos futuros incluem implantação do protótipo no serviço de coloproctologia, bem como a extensão do modelo para o acompanhamento dos exames em tempo real e extração de conhecimento dessa base de dados estruturada por meio de inteligência artificial.

Palavras-chave: colonoscopia; telemedicina; gerenciamento de exames; acompanhamento remoto de pacientes; comunicação com equipamentos hospitalares.

Study carried out at the Laboratory of Bioinformatics (LABI) at the Universidade Estadual do Oeste do Paraná (UNIOESTE), Foz do Iguaçu (PR) and the Service of Coloproctology (SC) of the Faculdade de Ciências Médicas (FCM) at the Universidade Estadual de Campinas (UNICAMP) – Campinas (SP), Brazil.
Funding source: Universidade Estadual do Oeste do Paraná (UNIOESTE) and Universidade Estadual de Campinas (UNICAMP).
Conflict of interest: nothing to declare.

Submitted on: 08/05/2011
Approved on: 09/06/2011

INTRODUCTION

The fast development of the technological area and, in particular, information technology resources, has allowed broad applicability in several areas of knowledge[1-5]. Some developments of the computer area that have contributed to this scenario include: increase in storage capacity, expansion of processing capacity, improvements in computer application safety, development of new data communication techniques, popularization of Internet and web-based systems[4,5].

Based on these developments, the utilization of computer techniques to help medical sciences has provided great contributions, involving the use of varied resources, including: computer graphics, image processing, database, distributed systems, data communication, artificial intelligence[6-14]. This scenario boosts the utilization of computer methods in different medical areas, from corporate solutions to hospitals and clinics to remote patient monitoring.

One important contribution linked with this multidisciplinary characteristics is the remote exchange of medical information, which enables distance diagnosis and treatment[11]. Examples of possible uses could be patient consultation and monitoring, information sharing, discussion of exams and medical inquiries, all made remotely[9,11,14]. These services need effective data communication mechanisms to ensure exchanged information privacy and reliability[15].

Due to the variety of computer applications in health areas, the computer systems have been classified as[13] *Hospital Information Systems* (HIS), *Radiology Information Systems* (RIS) and *Picture Archiving and Communication Systems* (PACS).

The integration PACS, RIS and HIS has been promoted with the creation of standards, such as current *Digital Imaging Communications in Medicine* (DICOM)[16] and *Health Level Seven* (HL7)[13,17]. These multidisciplinary applications, which involve the medical and computer areas, have encouraged the development of various products and studies, in both corporate and academic environments[11]. In this context, the Laboratory of Bioinformatics (LABI) of the Universidade Estadual do Oeste do Paraná (UNIOESTE), in a partnership with the Service of Coloproctology of the Faculdade de Ciências Médicas da Universidade Estadual de Campinas (UNICAMP), has developed several multidisciplinary studies[1,6,8-10,14,18-20].

The model proposed in this study is from the Telemedicine line of investigation conducted by both LABI and UNICAMP. The proposed solution involves the concepts of HIS[13], including data management related to the patients, health professionals, exams and reports.

The prototype includes other functionalities classified as PACS[13], in which a communication protocol is established between a computer system and the video colonoscopy equipment. Based on this interaction, this model provides management of patients' exams, including image and video capture during the examinations. Another important characteristic of this prototype is that it enables authenticated professionals to have a web-based access to patients' exams and data. Then, the development of this study was encouraged for ensuring continuity to previously developed models, this way contributing to exam supervision and offering technological resources that help perform distance diagnoses.

MATERIALS AND METHODS

The proposed experimental model involves concepts and functionalities of HIS[13] and PACS[13]. The development of this study followed methodological characteristics defined by Software Engineering[21], using the *Unified Modeling Language* (UML)[22] modeling.

One of the prerequisites for the development of this study was the study on the problem domain, through literature and meetings with experts, involving the protocol to perform video colonoscopy[23,24]. In addition, the study on items that constitute[23,25] the video colonoscope, such as: communication mechanisms available, differences between components according to the product manufacturer, model, video resolution, image quality, video input and output technology, was extremely important.

Regarding the problem domain, the literature related to protocols, standardizations and classifications of systems used in the medical area – e.g., HIS[13], RIS[13], PACS[13], DICOM[16] and HL7[17] – was also referred to.

After studying the involved domains, i.e. the medical and computer areas, observing real colonoscopy at the Gastrocentro at UNICAMP and having

meetings with experts from the medical and computer areas, the requirements for outlining this model were identified. The main characteristics defined were:

- The system accessibility should be made only by registered professionals, with permission to use the system;
- Maintainability of information about health professionals, patients and exams, using efficient safety and privacy criteria;
- Availability for web-based utilization of the solution;
- Permission to store and manage patient-related information through clinical history records and clinical exams performed;
- Permission to enter and maintain data about health professionals and researchers, who have access to the system to perform and/or analyze the exams;
- Capability to manage data and image captured during colonoscopy;
- Implementation of resources that enable the system communication with the video colonoscope, offering mechanisms for image capture and storage during colonoscopy;
- User-friendly interface to perform and monitor colonoscopy;
- Implementation of functionalities that enable the visibility and analysis of performed exams after they are concluded. For this requirement implementation, the remote utilization of the system should be considered via browser and internet connection.

After the definition of all requirements to be offered by the prototype and considering the particularities of the problem domain, the technological options were analyzed and, with these procedures, the solution model was defined, according to the sequence of architectural, logic/process and data models, presented as follows.

a) Architectural model

Figure 1 shows the architecture of the proposed model, considering the physical arrangement of its components, functionalities offered and technologies used in the solution. The computer model includes the utilization of Hospital Equipment (HE); in this case, equipment specifically designed for colonoscopy (video colonoscope).

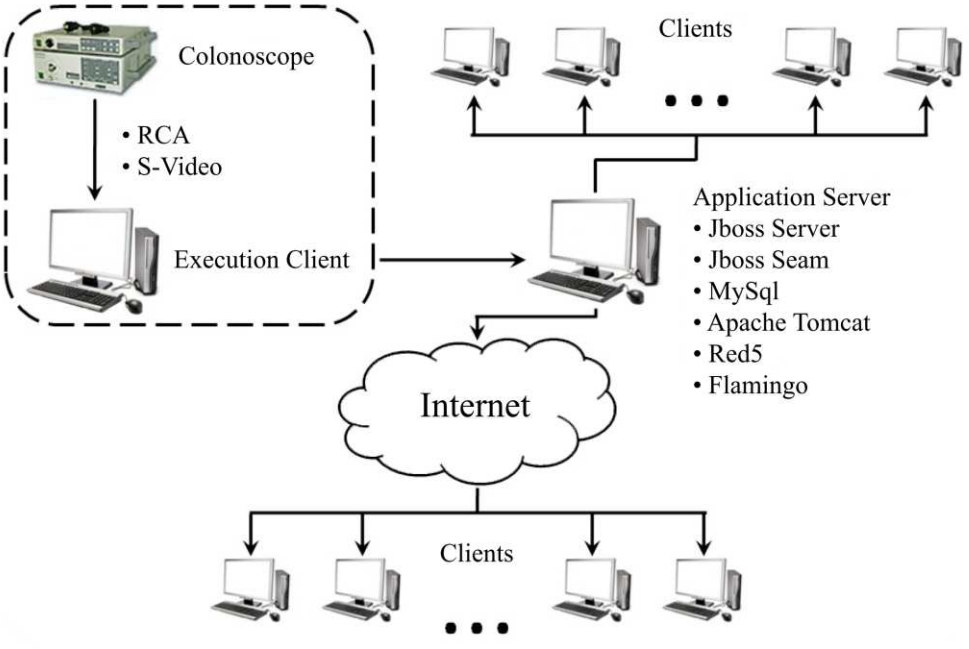

Figure 1. *Architectural model of the solution.*

Colonoscopy is an endoscopic exam that shows the internal part of the whole colon. It uses a flexible tube whose length is 70 to 160 cm. At the end of this tube, there is a camera, which sends images to a display[23]. These images can also be captured and stored in memory cards connected to the video colonoscopy equipment processor[23]. During the exam, images and videos are captured by distinct colonoscopy devices (different manufacturers and models) in *Intensity and Chroma* (Y/C), *Video Graphics Array* (VGA), Super Video formats, in *National Television System(s) Committee* (NTSC) color system. These exams can be monitored directly through the display and the selected images can be printed[23].

This way, video colonoscopes usually have the following components[24,25]: colonoscope (fiberscope), light source, aspiration and biopsy channels, enlargement lenses, air insufflation or irrigation channels, NTSC display with Y/C input and VGA with color and brightness adjustments, trolley or cart for equipment support, video printer compatible with NTSC color system, alphanumeric keys and printer.

As illustrated in Figure 1, the interaction between the video colonoscope and the computer system was defined in this model, named Execution Client. This computer is equipped with a video capture board and is physically located in the exam room. RCA or Super Video connected were selected to establish the communication, interconnecting the video colonoscope output to the capture board input.

The Execution Client has the access to software functionalities classified as HIS[13], such as registration of patients, health professionals and researchers and exams. Besides these functionalities, characteristics classified as PACS[13] are provided, which will be used during the exams, such as capture, monitoring and storage of images from the video colonoscope.

For the proper execution of the defined functionalities, the Execution Client should have the access to the services offered by the Application Server. These services include data management, network communication, functionalities for data entry, management and history analysis of patient and exam data. The technological resources employed to provide these characteristics were defined according to the Logic and Process Model section.

This way, the Application Server enables the services required for an adequate operation of the Execution Client and other Clients. It should be noted that the functionalities not directly related to the exam execution were available to Clients in both local network and internet, by using web technologies (Figure 1).

b) Logic and process model

The outlined computer architecture uses the *Model-view-controller* (MVC)[26] standard and Java programming language[27], JBOSS Application Server 4.2[28], Red5 1.0 streaming server[29], JBoss Seam Development Framework[30] and MySQL 5.1.42 Database Management System[31]. The visual presentation of videos and images and the communication with capture devices used Flex 4.0[32] programming language. The interaction and communication between the classes developed in Java and Flex were established through the access to remote objects, using functions available in Flamingo framework[33].

After the definition of all technological resources to be included in the computer project, the main processes implemented using the prototype were presented.

The main process is related to image communication during the video colonoscopy. For this process, VP-4400[25] Fuginon video colonoscope was used, connected to a Core 2 Duo 2.2 GHz computer, with PixelView PlayTV Xtreme video capture board, through the Super Video format video interface. For the streaming management, a connection with RED5 1.0[29] streaming server was used. The images collected during the exams were stored in the Application Server and the video capture was made by the video colonoscope, but the experiments were not performed during real exams.

For the image capture, H.264 codec was used, with 500 x 500 pixel resolution and 30 fps (frames per second). The images captured during the exams were stored in JPEG[34] format; the visual display of images and the communication with capture devices were made using Flex[32] language.

The registration and inquiry processes related to physicians, patients, exams and images were available to all professionals with system access, either in the institution's network or an external environment, using the internet. These characteristics were implemented in JBoss Seam[30] and the data were stored in a Mysql structured database[31,35].

c) Data model

To support data storage, a data model was elaborated, named Relation Entity Model, and implemented by a Mysql database management system[31,35], composed of the following entities and relations: Professional, for the storage of data related to physicians and professionals that will have access to the system, with encrypted password field, and using MD5[15] algorithm; Patient, to keep the history of patients that will be registered at the hospital or clinic; Equipment, to identify the exam equipment; and Exam, which constitutes in one entity that relates the other tables and stores the data regarding the exams performed, including patient, physician and equipment used, type of exam, medical care and institution where the exam was performed. This table also stores specific information about the exam, such as exam date and links to see the images captured during the exam.

RESULTS

The development of this study enabled the domain study in the medical and computer areas. The interaction with professionals from these areas allowed to list procedures that can contribute to better processes for exams that complement video colonoscopy.

Based on these information, the identification of resources, the evaluation of technological alternatives, the computer project definition and the prototype implementation were performed.

The computer model was defined and implemented integrating technologies based on free software, in such way to fulfill the requirements of layout (user-friendly interface), efficient user safety and privacy and robust data storage and management. Based on this context, the physical, logic and component architecture was implemented, according to the model illustrated in Figure 1.

Regarding the prototype implementation results, they can be categorized into: layout and interface, data management, application safety and availability of mechanisms for local and remote exam supervision and with resources for subsequent analysis.

The system interfaces were standardized, with a management screen and others for data insert, edit, display and other specific actions. These screens were created for the professional entities, patient, institution, equipment, reports and exams. For instance, Figure 2 illustrates the layout generated for the initial screen of the system, Figure 3 illustrates the interface for exam management, Figure 4 shows the screen for

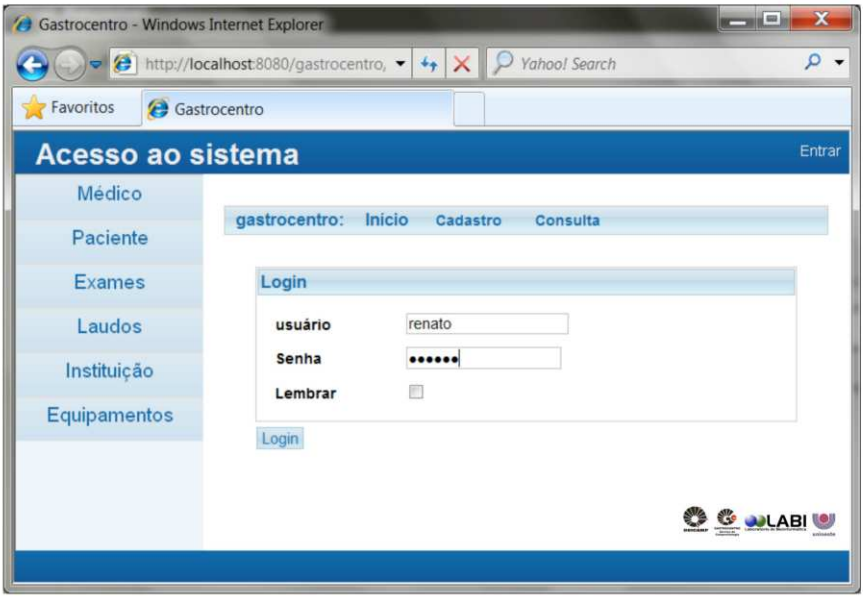

Figure 2. *System authentication screen.*

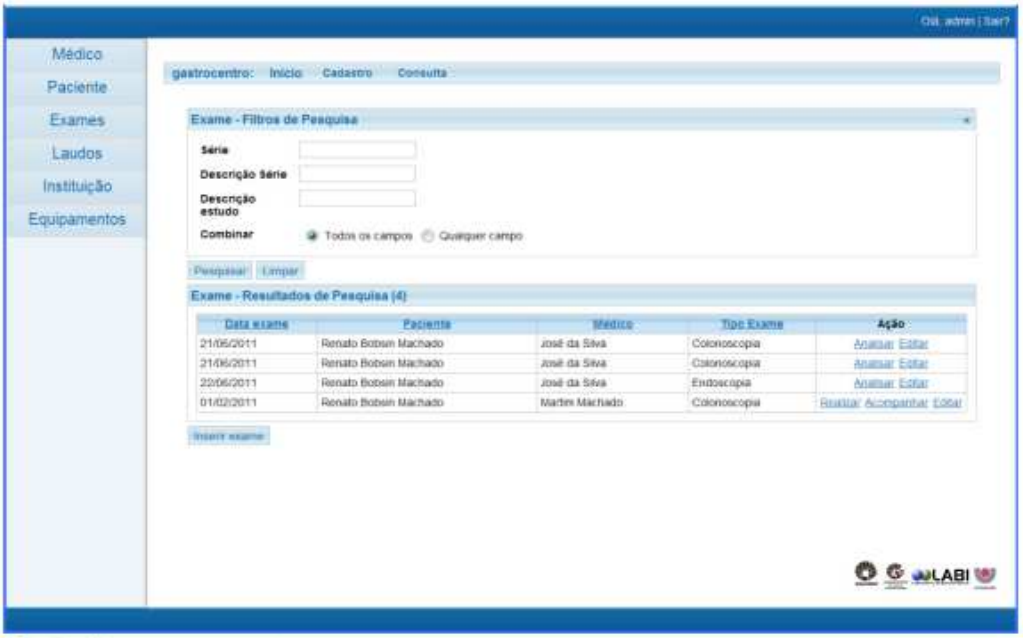

Figure 3. *Interface for exam management.*

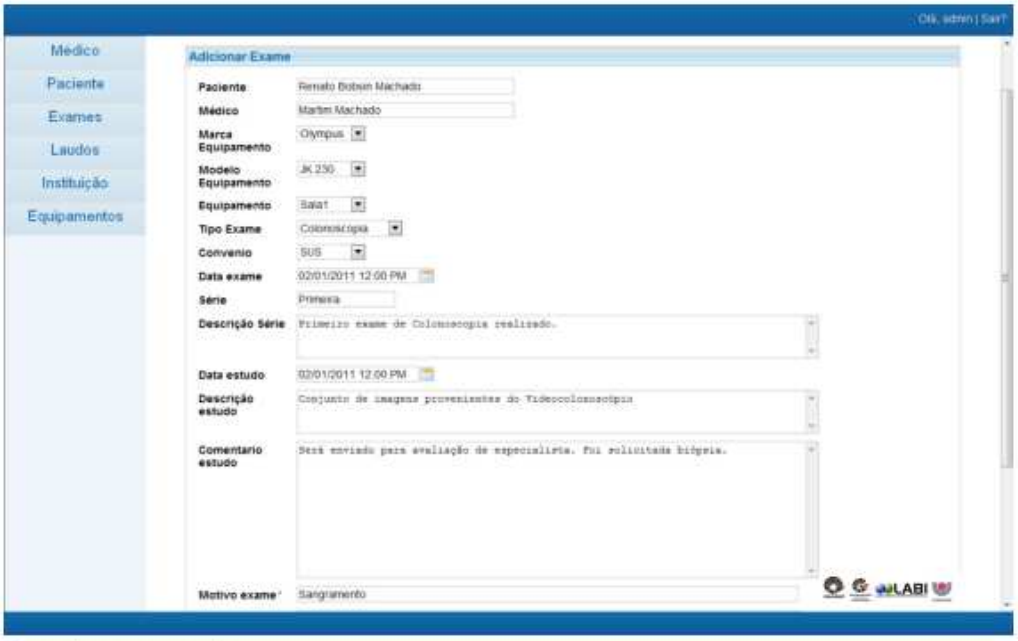

Figure 4. *Screen for new exam entry.*

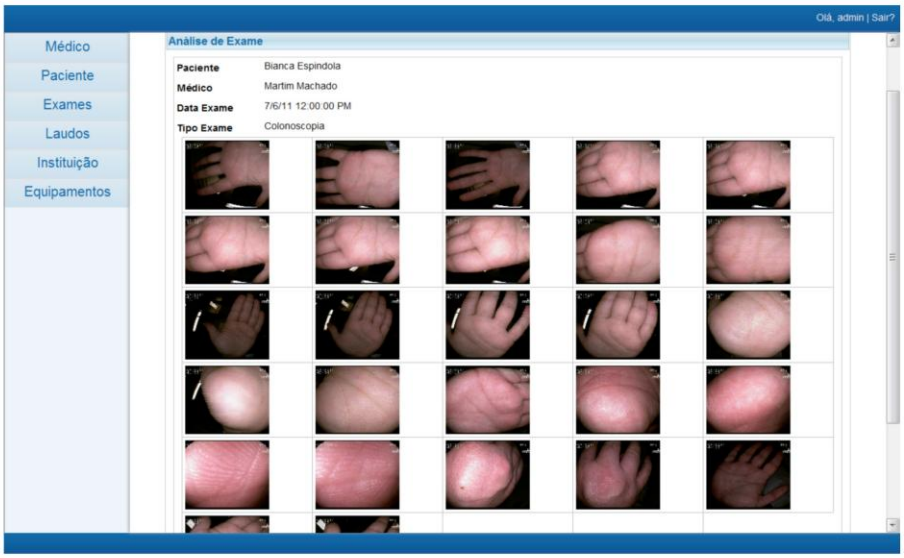

Figure 5. *Interface for colonoscopy exam and image display.*

entering a new exam and Figure 5 illustrates the layout to perform and supervise a video colonoscopy exam.

The figures mentioned above show the main characteristics available on the other screens of the prototype, involving the arrangement of graphic elements, menu bar, navigation mode, indexing and search resources, component to present the results, resources to view and supervise the videos and images from the video colonoscopy, among other characteristics.

Regarding data management, the Relation Entity model was created to ensure integrity and reliability to the storage of data from entities and relations. Besides the specific requirements of this prototype, the base was estimated to allow easy integration with other computer systems for the medical area and the application of knowledge extraction methods.

Besides data layout and model, the data and user safety requirement was implemented by using MD5[15] algorithm, generating a 128-bit hash.

For the prototype development, the integration of JBoss Seam[30] framework with Flex[32] language allowed greater flexibility for the interface and image handling, keeping the MVC[26] model robustness for database management, utilization of efficient encryption methods and prototype development in a web-based environment.

The characteristics implemented in the prototype were validated by experts from the medical and computer areas, with special regards to the functionalities that allow real-time exam supervision and the possibility of future analyses, as illustrated in Figure 5.

DISCUSSION

The prototype development for patient and colonoscopy data management uses the characteristics of HIS[13] and PACS[13].

The web-based access to the application allows greater flexibility to physicians and experts, as the system can be accessed from any hardware or operating system platform, via web browsers, with the internet connection as the only prerequisite[15]. This way, no applications have to be installed to access the prototype and its functionalities, and the architecture provides easier maintainability and transparent incorporation of new functionalities to end users; in this case, health professionals.

These definitions allowed to classify this prototype as an application linked with Telemedicine research. In this context, an important contribution of this study is that it enables physicians and experts to refer to patients' data and exams and discuss cases and interact in patients' diagnosis and treatment, also in

real time. This aspect can also help reduce the impact of geographical distances, considering that, in several situations, the experts cannot be present in all places where they practice, and the lack of experts in smaller cities, far from urban centers.

The resources used to provide system authentication was MD5[15] encryption method, which generates a 128-bit hash. This method is today's one of the most efficient algorithms, with flexibility to determine the key size according to the safety level required[15]. One of the advantages of using this method in the prototype is that both Jboss Seam[30] technology and Mysql[35] database have compatible functions with this method. Then, it was possible to ensure compatibility and the desirable level of encryption efficiency, reduce the development time and enable the encrypted password storage in the database. The system login interface is illustrated in Figure 2.

After the system authentication, the prototype functionalities are ready to be used. The interface was developed using JBoss Seam[30], a web-based platform, which integrates with the data management resources.

Mechanisms were developed in the prototype that integrate the interface with the database to enable data entry, edit, display and removal, keeping functional and referential data integrity. These characteristics were provided for data related to physicians, patients, exams, institutions and devices. The management of such data is performed using the menus on the left side of the interface (Figure 3), which open other screens with specific functions.

One of the prototype advantages is that it combines free software tools, reducing development costs, but keeping an intuitive, user-friendly and easy-to-navigate layout.

The interface provides a search field in the upper part of the screen and the entries stored in the system are displayed in the lower part. These entries are the result of a search parameter, the default is "display all" (Figure 3).

For each entry, links are provided on the right part of the screen for entry view or edit. When opening the edit option, data are viewed with all related fields, which can be altered by the system user. The lower part of the edit screen has the following buttons: Update (save alterations), Remove (remove the current entry) or Cancel (exit the edit mode, keeping the entry unaltered). The lower part of the search results has the Insert button. When clicking this button, an interface is provided to add new entries (Figure 4). These functional characteristics are typical of HIS[13].

The prototype has functionalities that were developed to allow the communication with the video colonoscopy, image capture and display during the exam and subsequent storage. After the conclusion of complementary exam procedure, data and images were available to health professionals via web resources. These functionalities are classified as PACS[13]. To better understand these functional requirements, the protocol proposed for exam management will be discussed.

Figure 3 shows the exam management interface. The insertion of an exam entry usually occurs at the moment the patient comes to the exam room. When clicking the Insert button, the user has the access to an interface to enter exam-related information (Figure 4).

The exam registration in the system requires the following: patient's name, physician in charge of the procedure, equipment to be used, exam date, the patient's medical care, reason for the exam, patient's reference, institution and specialty for which the exam will be performed. To support the integration of this prototype with the PACS model previously developed in this research line[19], optional fields were added of series description, study description and study remarks.

After saving the new exam, other functions are provided, which will allow to go to the exam screen (Figure 5) or return to the exam management screen (Figure 3). For entries of data on exams registered in the system, but that have not been performed yet, actions are provided for exam execution, real-time exam supervision and exam entry edit. For concluded exams, options are provided for analysis, to have access to all exam data and images, and edit, to alter concluded exam data.

When executing the "perform exam" action, the prototype opens a screen (Figure 5) to locally and remotely watch the exam video, allowing to capture images the physician considers important. After he images are captured, at the physician's discretion, the procedure can be concluded.

For the health professional to access exam data and images, he/she should use the "analyze" option in the

exam management interface (Figure 3), on the "Exam Inquiry" screen, as illustrated in Figure 5. The images from the palmar region of hand, illustrated in Figure 5, were used in the validation of exam execution and monitoring functionalities and the analysis characteristic. These images were captured using a video colonoscope from the Service of Coloproctology of UNICAMP.

After the prototype functionalities were outlined, it was confirmed that all requirements defined with the experts had been implemented and that they provide important contributions to video colonoscopy execution; some positive characteristics that could help physicians and experts are:

- Storage of patient and exam data history;
- The possibility of image capture and integration into the system during the colonoscopy execution. The video colonoscopy devices usually store captured images in magnetic media, which should be taken to a computer for visualization;
- The use-to-use, web-based graphic interface;
- The web-based exam and image display, allowing the exams to be remotely analyzed by experts, which contributes to diagnoses of improved effectiveness;
- The system can be used in distant cities without experts in the area, minimizing the patients' efforts of traveling to urban centers and, especially, reducing diagnosis times.

Besides the specific characteristics of the solution presented in this study, this model can be integrated with other studies previously developed in this research line[19].

Regarding the technology employed, it provides the advantage of using all components developed Java[27] and open coding services. These characteristics allow the system operation in any hardware or operating system platform that supports Java virtual machine, as well as reduced development cost, keeping the data management efficiency and the easy navigation in the application screens. The developed prototype was validated in *Windows* and *Linux* operating systems, using *Mozzila Firefox*, *Internet Explorer* and *Chrome* browsers.

CONCLUSION

This study presented a prototype of a computer solution that combines HIS and PACS characteristics.

The development of this prototype contributed to improved processes related to video colonoscopy exam execution, allowing to create a history of patients and exams in a structured database and the remote analysis of patient and exams.

One of the differentiations of this study is in the provision of resources for video colonoscopy exam supervision in real time. Future activities include the prototype deployment in the Service of Coloproctology at UNICAMP, the integration of the database from this prototype with other models defined in partnerships with LABI at UNIOESTE with the Service of Coloproctology at the Faculdade de Ciências Médicas da UNICAMP, and utilization of this model to allow real-time monitoring of these exams and knowledge extraction from such structured database using artificial intelligence.

REFERENCES

1. Costa LHD, Ferrero CA, Lee HD, Coy CSR, Fagundes JJ, Wu FC. Mapeamento de laudos médicos de endoscopia digestiva alta apoiados por ontologias. In: X Workshop de Informática Médica. Belo Horizonte: Sociedade Brasileira de Computação; 2010.
2. Fedel GS, Medeiros CMB. Busca multimodal para apoio à pesquisa em biodiversidade. In: IX Workshop de Teses e Dissertações em Banco de Dados. São Paulo: Universidade de São Paulo; 2010.
3. Liu H, Motoda H. Computational methods of feature selection. Boca Raton: Chapman & Hall/CRC; 2008.
4. Wright RT, Brown RA. Technology: design and applications. 2a ed. USA: Goodheart-Willcox Co; 2008.
5. Shortliffe EH, Cimino JJ. Biomedical informatics: computer applications in health care and biomedicine. 3a ed. New York: Springer Science+Business Media; 2006.
6. Nabo RGB, Machado RB, Lee HD, Zalewski W, Ferrero CA, Coy CSR, et al. Desenvolvimento de um protótipo de um sistema PACS para aquisição de exames médicos e transmissão de vídeos de colonocospia em tempo real pela internet. In: XVIII SIICUSP – Simpósio Internacional de iniciação Científica da USP. São Paulo: Universidade de São Paulo; 2010.
7. Spolaôr N, Lorena C, Lee HD. Use of multiobjective genetic algorithms in feature selection. In: Brazilian Symposium on Artificial Neural Network. São Bernardo do Campo: Sociedade Brasileira de Computação; 2010.
8. Wu FC, Lee HD, Ferrero CA, Coy CSR, Fagundes JJ, Machado RB, et al. Development of an ontology-based approach for mapping high digestive endoscopy medical

reports into structured databases. In: ALIO-INFORMS Joint International Meeting. Buenos Aires: Association of Latin-Iberoamerican Operational Research Societies; 2010.
9. Neitzel N. Desenvolvimento de uma solução para o armazenamento e a disponibilização de dados e exames médicos aplicando a padronização DICOM [Monografia de Graduação]. Foz do Iguaçu: Universidade Estadual do Oeste do Paraná, *campus* Foz do Iguaçu; 2009.
10. Silva RAL, Machado RB, Maciel JN, Lee HD, Wu FC, Fagundes JJ, et al. Avaliação de soluções multimídia para a utilização no desenvolvimento de aplicações em telemedicina. In: Anais do IV Congresso da Academia Trinacional de Ciências. Foz do Iguaçu: Universidade Estadual do Oeste do Paraná; 2009.
11. Urtiga KS, Louzada LA. Telemedicina: uma visão geral da arte. In: Proceedings do IX Congresso Brasileiro de Informática em Saúde. Ribeirão Preto: Sociedade Brasileira de Informática em Saúde; 2004.
12. Caritá EC. Sistema de gerenciamento de imagens para ambiente hospitalar com suporte à recuperação de imagens baseada em conteúdo [Tese de Doutorado]. Ribeirão Preto: Universidade de São Paulo; 2006.
13. Yu L, Jihong W. PACS and digital medicine: essential principles and modern practice. Boca Raton: Taylor and Fracis Group; 2011. ISBN: 13:978-1-4200-8366-8.
14. Maciel JN. Protótipo de conferência multimídia e transmissão de dados de experimentos médicos em tempo real pela *Web* [Monografia de Graduação]. Foz do Iguaçu: Universidade Estadual do Oeste do Paraná, *campus* Foz do Iguaçu; 2005.
15. Coulouris G, Dollimore J, Kindberg T. sistemas distribuídos: conceitos e projetos. 4a ed. Porto Alegre: Editora Bookman; 2007.
16. Pianykh OS. Digital Imaging and Communications in Medicine (DICOM): A practical introduction and survival guide. Boston: Editora Springer; 2008. ISBN 354074570X.
17. HL7. Join HL7 International. 2011. [cited 2011 Jun 29]. Available from: http://www.hl7.org/
18. Wu FC. Estudo dos efeitos de diferentes concentrações de oxigênio e da hiperoxigenação hiperbárica sobre anastomoses cólicas comprometidas ou não pela isquemia. Trabalho experimental em ratos [Tese de Doutorado]. Campinas: Faculdade de Ciências Médicas da Universidade Estadual de Campinas; 2003.
19. Lee HD, Machado RB, Ferrero CA, Coy CSR, Fagundes JJ, Wu FC. Modelo computacional para o gerenciamento de dados e exames de pacientes para o acompanhamento remoto por meio de conferência multimídia. Rev bras Coloproct 2010;30(4):399-408.
20. Lee HD, Costa LHD, Ferrero CA, Coy CSR, Fagundes JJ, Machado RB, et al. Protótipo de um sistema de gerenciamento de protocolos de câncer colorretal. Rev bras Coloproct 2011;31(1):1-9.
21. Pressman RS. Engenharia de software. 6a ed. São Paulo: McGraw-Hill; 2006.
22. Booch G, Rumbaugh J, Jacobson I. UML Guia do usuário. Rio de Janeiro: Campus; 2000.
23. Quilici FA, Grecco C. Colonoscopia. São Paulo: Lemos Editorial; 2000. ISBN 85-7450-048-8.
24. Rocha JJR. Coloproctologia: príncipios e prática. São Paulo: Atheneu; 2005.
25. Operation Manual. EVE Processor: VP-4400. Fukinon Corporation. v. 1.1. Japan.
26. Deacon J. Model-View-Controller (MVC) architecture. John Deacon Computer System Development, Consulting & Training 2005:1-6. [cited 2011 Jun 29]. Available from: http://www.jdl.co.uk/briefings/index.html#mvc
27. Deitel HM. Java: como programar. 6a ed. São Paulo: Editora Pearson Prentice Hall; 2005.
28. Jamae J, Johnson P. JBoss in action: configuring the JBoss application server. Greenwich: Manning Publications; 2009. ISBN: 1933988029.
29. RED5. The open source media server. [cited 2011 Jun 29]. Available from: http://www.red5.org/
30. Allen D. SEAM in action. Greenwich: Editora Manning Publications; 2008.
31. Korth AB, Silberschatz HF. Sistema de banco de dados. 2a ed. São Paulo: Editora Makron Books; 1995.
32. Tiwari S, Elrom E, Schulze C. Flex 4 avançado. São Paulo: Novatec; 2011.
33. Flamingo. Exadel Community. [cited 2011 Jun 29]. Available from: http://exadel.com/web/portal/opensource?redirected=/flamingo
34. JPEG. JPEG Homepage. [cited 2011 Jun 29]. Available from: http://www.jpeg.org/jpeg/index.html/
35. Mysql. Sistema gerenciador de banco de dados MySQL. [cited 2011 Jun 29]. Available from: http://www.mysql.com/

Correspondence to:
Renato Bobsin Machado
Laboratório de Bioinformática (LABI), Universidade Estadual do Oeste do Paraná (UNIOESTE), Parque Tecnológico Itaipu (PTI)
Avenida Tancredo Neves, 6731, Caixa Postal 39
CEP: 85856-970 – Foz do Iguaçu (PR), Brazil
E-mail: renatobobsin@gmail.com

8. RESULTADOS

8.1. CONSTRUÇÃO DO SISTEMA DE TELEMEDICINA EM TEMPO REAL (S2TR)

A interface gráfica do S2TR está ilustrada nas Figuras 25, 26 e 27 por meio das telas de gerenciamento, de cadastro e de visualização de exames de videocolonoscopia.

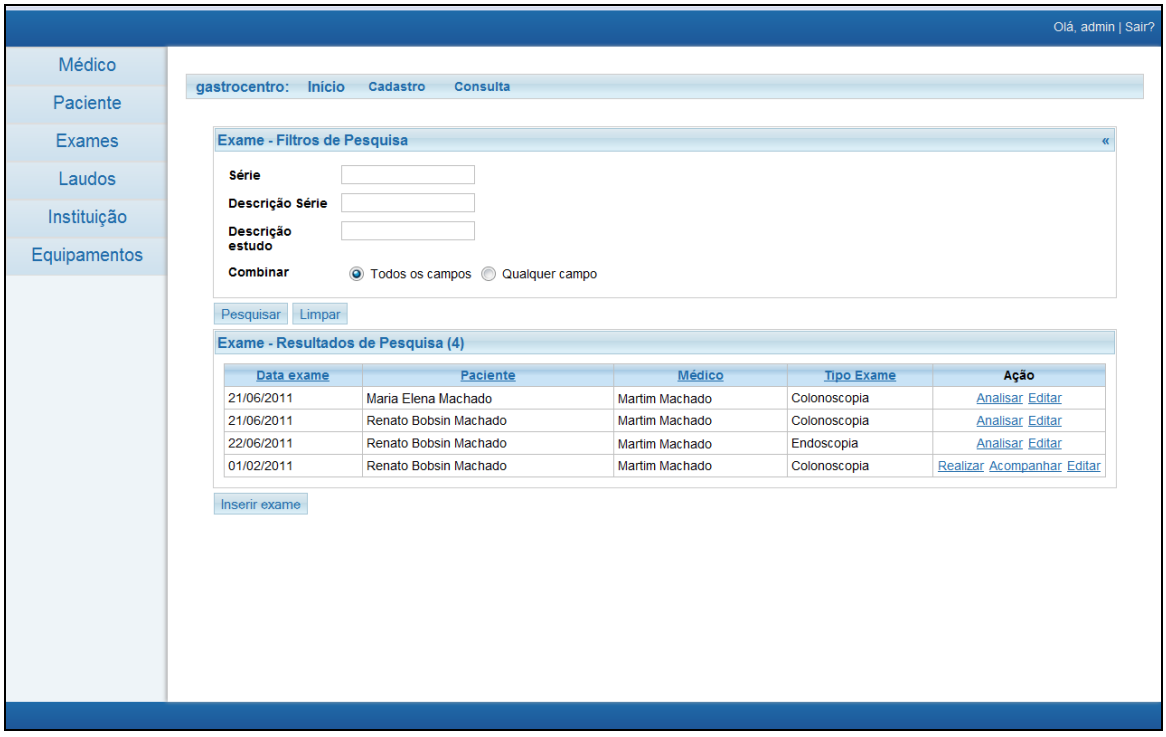

Figura 25: Tela para o Gerenciamento de Exames de Videocolonoscopia.

8.2. RESULTADOS DOS EXPERIMENTOS DE DESEMPENHO NO AMBIENTE INSTITUCIONAL

Nas Tabelas 1 e 2 são apresentados os resultados das médias das taxas de transmissão de Quadros por Segundo (QPS) e os respectivos Desvios-Padrão (DP) do EMISSOR e dos clientes ETHERNET e WIFI referentes aos experimentos realizados no período da manhã e da tarde no Ambiente Institucional, respectivamente. Em todas as tabelas, na última coluna estão representados as médias e os DPs conjuntos de todas as manhãs ou tardes para o EMISSOR e para os clientes ETHERNET e WIFI.

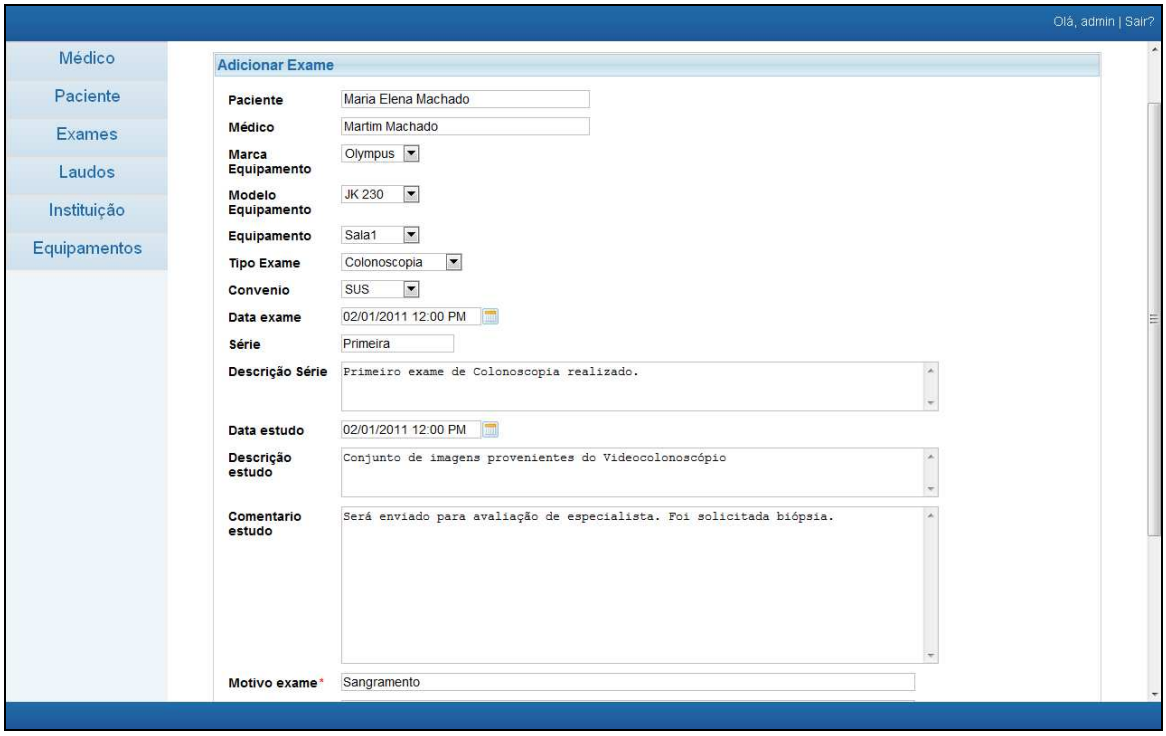

Figura 26: Tela para o Cadastro de Novos Exames de Videocolonoscopia.

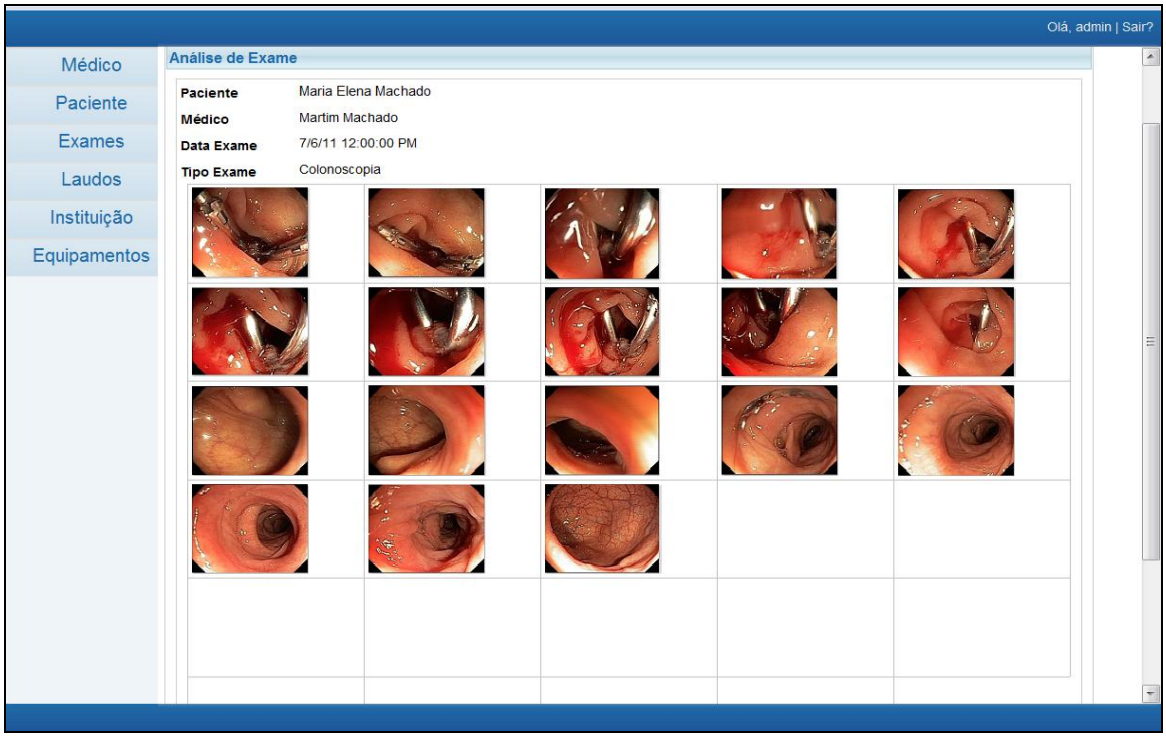

Figura 27: Tela para a Visualização de Exames de Videocolonoscopia.

Tabela 1: Médias e DP das Taxas de Transmissão de QPS do EMISSOR e dos Clientes ETHERNET e WIFI do Período de Experimentação Manhã no Ambiente Institucional.

QPS		Manhã 1	Manhã 2	Manhã 3	Manhã 4	Manhã 5	Conjunta
EMISSOR	**Média**	23,80	23,59	23,85	23,83	23,61	23,73
	DP	0,64	0,83	0,63	0,64	0,95	0,76
ETHERNET	**Média**	21,25	21,18	21,51	21,44	21,20	21,32
	DP	1,70	1,76	1,72	1,80	2,32	1,88
WIFI	**Média**	20,84	20,79	21,10	20,97	21,03	20,95
	DP	2,84	3,11	2,77	2,87	2,78	2,88
Média		**21,96**	**21,85**	**22,15**	**22,08**	**21,95**	
DP		**2,35**	**2,46**	**2,27**	**2,35**	**2,67**	

Tabela 2: Médias e DP das Taxas de Transmissão de QPS do EMISSOR e dos Clientes ETHERNET e WIFI do Período de Experimentação Tarde no Ambiente Institucional.

QPS		Tarde 1	Tarde 2	Tarde 3	Tarde 4	Tarde 5	Conjunta
EMISSOR	**Média**	23,97	23,95	23,67	23,61	23,96	23,83
	DP	0,46	0,49	0,76	0,83	0,48	0,64
ETHERNET	**Média**	21,42	21,48	21,36	21,22	21,65	21,43
	DP	1,82	1,70	1,74	1,72	1,71	1,74
WIFI	**Média**	21,27	21,09	21,16	20,93	21,28	21,15
	DP	2,83	2,82	2,51	2,80	2,64	2,72
Média		**22,22**	**22,18**	**22,06**	**21,92**	**22,30**	
DP		**2,32**	**2,30**	**2,14**	**2,30**	**2,18**	

Na Tabela 3 estão posicionados os valores das médias gerais e respectivos DPs de Transmissão de QPS do EMISSOR e dos clientes ETHERNET e WIFI dos períodos de experimentação manhã e tarde no Ambiente Institucional.

Na Figura 28 e na Figura 29 são ilustrados gráficos representativos das taxas de QPS transmitidas pelo EMISSOR e recebidas pelos diferentes clientes no Ambiente Institucional dos experimentos realizados no período da manhã e da tarde, respectivamente.

Por meio da Tabela 4, apresenta-se uma divisão em classes, distinguindo-se percentualmente as taxas de QPS menores que 10 e iguais ou superiores a 10.

Tabela 3: Médias Gerais e DP de Transmissão de QPS do EMISSOR e dos Clientes ETHERNET e WIFI dos Períodos de Experimentação Manhã e Tarde no Ambiente Institucional.

QPS		Manhãs	Tardes	Conjunta
EMISSOR	**Média**	23,73	23,83	23,78
	DP	0,76	0,64	0,71
ETHERNET	**Média**	21,32	21,43	21,37
	DP	1,88	1,74	1,81
WIFI	**Média**	20,95	21,15	21,05
	DP	2,88	2,72	2,80
Média		**22,00**	**22,14**	
DP		**2,38**	**2,25**	

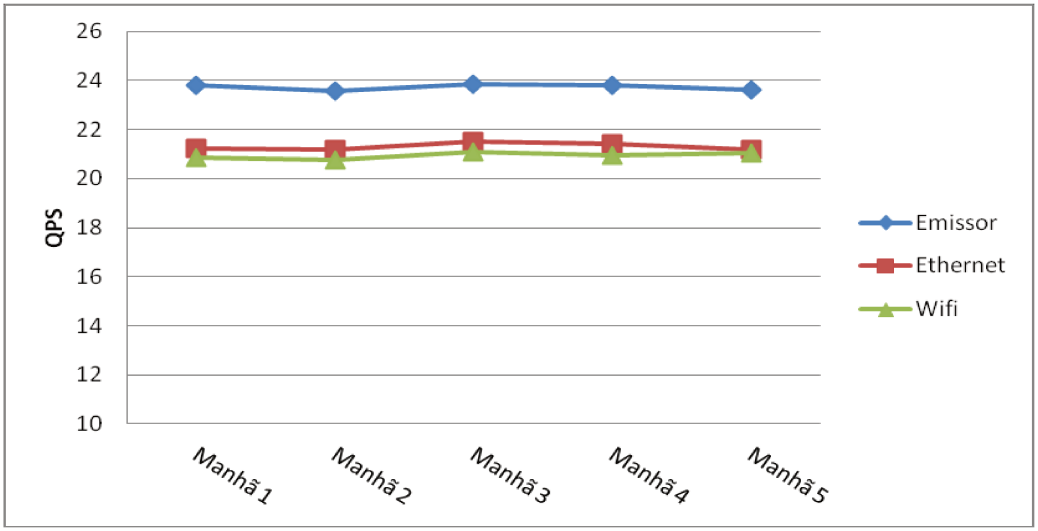

Figura 28: Taxa de QPS no Período da Manhã no Ambiente Institucional.

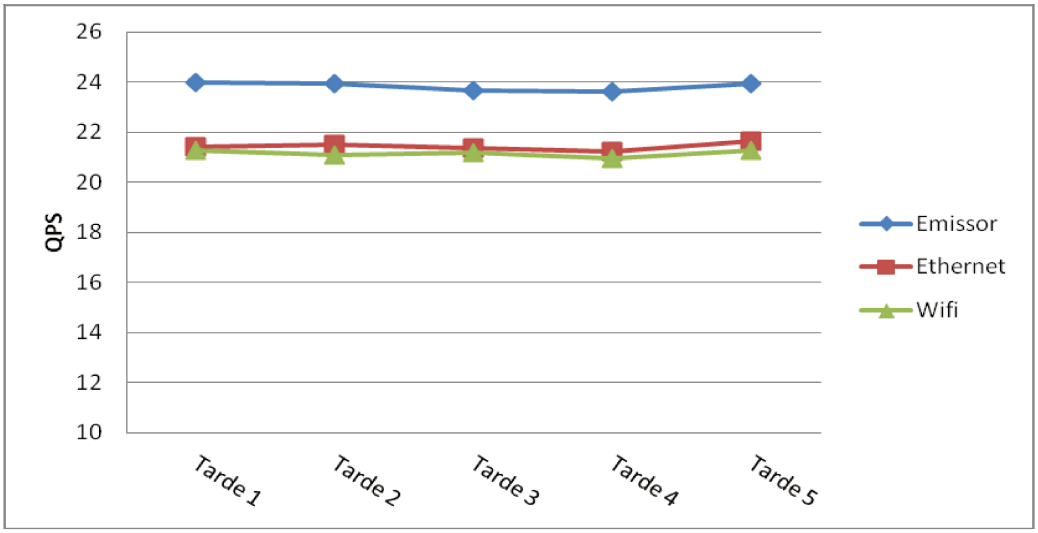

Figura 29: Taxa de QPS no Período da Tarde no Ambiente Institucional.

Tabela 4: Distribuição Percentual das Taxas de QPS em Classes no Ambiente Institucional.

QPS (%)	< 10	≥ 10
EMISSOR	0,01%	99,99%
ETHERNET	0,06%	99,94%
WIFI	1,82%	98,18%

8.3. Resultados dos Experimentos de Desempenho no Ambiente Institucional e Internet

Na Tabela 5 apresentam-se as taxas de QPS e respectivos DP em relação aos experimentos realizados no período da manhã no Ambiente Institucional e Internet, para o EMISSOR e os clientes ETHERNET, WIFI, A, B e ADSL, conforme configuração experimental descrita no Capítulo 4. Essas mesmas informações, referentes ao período da tarde, são apresentadas na Tabela 6.

Tabela 5: Médias e DP das Taxas de Transmissão de QPS do EMISSOR e dos Clientes ETHERNET, WIFI, A, B e ADSL do Período de Experimentação Manhã no Ambiente Institucional e Internet.

QPS		Manhã 1	Manhã 2	Manhã 3	Manhã 4	Manhã 5	Conjunta
EMISSOR	**Média**	23,97	23,92	23,83	23,90	23,94	**23,91**
	DP	0,52	0,58	0,67	0,62	0,66	**0,61**
ETHERNET	**Média**	21,48	21,31	21,59	21,31	21,51	**21,44**
	DP	1,65	1,69	1,87	1,74	1,95	**1,79**
WIFI	**Média**	21,43	21,29	21,35	21,35	21,27	**21,34**
	DP	1,75	2,10	2,55	1,72	2,39	**2,13**
A	**Média**	21,34	21,31	21,36	20,97	21,12	**21,22**
	DP	1,83	1,85	2,49	2,75	2,42	**2,30**
B	**Média**	12,68	12,88	11,71	12,08	12,08	**12,29**
	DP	6,01	6,07	5,75	5,97	6,01	**5,98**
ADSL	**Média**	13,44	14,29	14,77	13,48	14,09	**14,01**
	DP	6,29	6,20	6,10	6,31	6,35	**6,27**
Média		**19,06**	**19,17**	**19,10**	**18,85**	**19,00**	
DP		**5,75**	**5,57**	**5,76**	**5,87**	**5,84**	

Tabela 6: Médias e DP das Taxas de Transmissão de QPS do EMISSOR e dos Clientes ETHERNET, WIFI, A, B e ADSL do Período de Experimentação Tarde no Ambiente Institucional e Internet.

QPS		Tarde 1	Tarde 2	Tarde 3	Tarde 4	Tarde 5	Conjunta
EMISSOR	**Média**	23,95	23,85	23,83	23,94	23,94	**23,90**
	DP	0,59	0,71	0,79	0,70	0,55	**0,67**
ETHERNET	**Média**	21,29	21,29	21,34	21,19	21,49	**21,32**
	DP	1,99	1,74	2,00	2,00	1,73	**1,90**
WIFI	**Média**	21,09	21,22	21,06	21,38	21,32	**21,21**
	DP	2,25	2,07	2,28	2,15	1,74	**2,11**
A	**Média**	21,21	20,92	20,61	20,89	20,92	**20,91**
	DP	2,12	2,66	3,18	2,93	2,53	**2,72**
B	**Média**	13,13	12,31	12,46	12,17	13,13	**12,64**
	DP	6,19	5,96	6,04	6,13	6,09	**6,09**
ADSL	**Média**	13,74	14,94	14,69	14,81	14,71	**14,58**
	DP	6,26	6,28	6,34	6,31	6,28	**6,31**
Média		**19,07**	**19,09**	**19,00**	**19,06**	**19,25**	
DP		**5,66**	**5,60**	**5,68**	**5,74**	**5,50**	

Na Tabela 7 apresentam-se as taxas de médias gerais e os respectivos DPs de transmissão de QPS do EMISSOR e dos clientes ETHERNET, WIFI, A, B e ADSL dos períodos de experimentação manhã e tarde, conjuntamente, realizados no Ambiente Institucional e Internet.

Tabela 7: Médias Gerais e DP de Transmissão de QPS do EMISSOR e dos Clientes ETHERNET, WIFI, A, B e ADSL dos Períodos de Experimentação Manhã e Tarde no Ambiente Institucional e Internet.

QPS		**Manhãs**	**Tardes**	**Conjunta**
EMISSOR	**Média**	23,91	23,90	23,91
	DP	0,61	0,67	0,64
ETHERNET	**Média**	21,44	21,32	21,38
	DP	1,79	1,90	1,84
WIFI	**Média**	21,34	21,21	21,28
	DP	2,13	2,11	2,12
A	**Média**	21,22	20,91	21,07
	DP	2,30	2,72	2,52
B	**Média**	12,29	12,64	12,46
	DP	5,98	6,09	6,04
ADSL	**Média**	14,01	14,58	14,30
	DP	6,27	6,31	6,29
Média		**19,03**	**19,09**	
DP		**5,76**	**5,64**	

Na Figura 30 e na Figura 31 são apresentados os gráficos das taxas de QPS relativas aos experimentos realizados no período da manhã e da tarde, respectivamente, e transmitidas pelo EMISSOR e recebidas por todos os clientes no Ambiente Institucional e Internet.

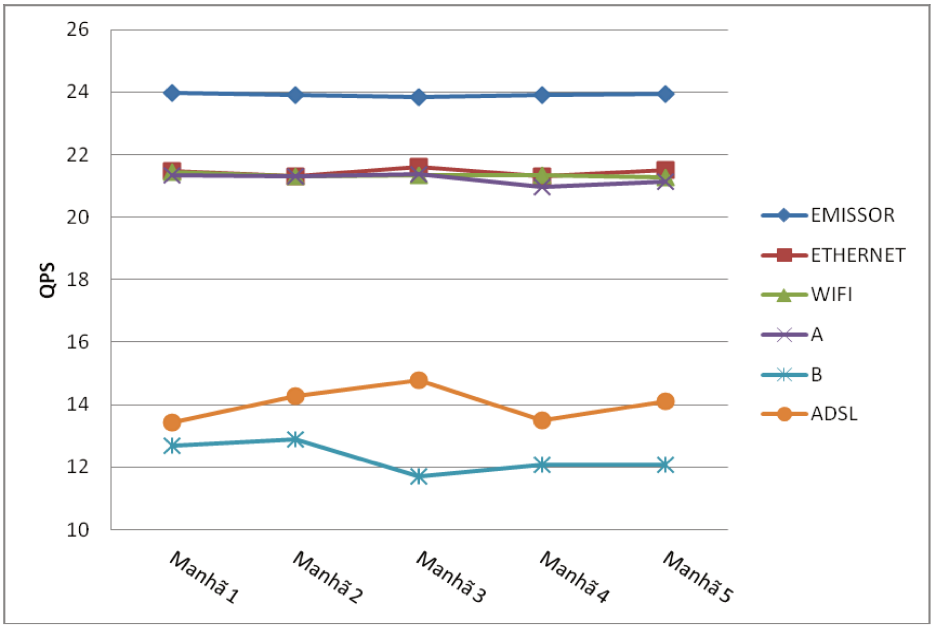

Figura 30: Taxa de QPS no Período da Manhã para o Ambiente Institucional e Internet.

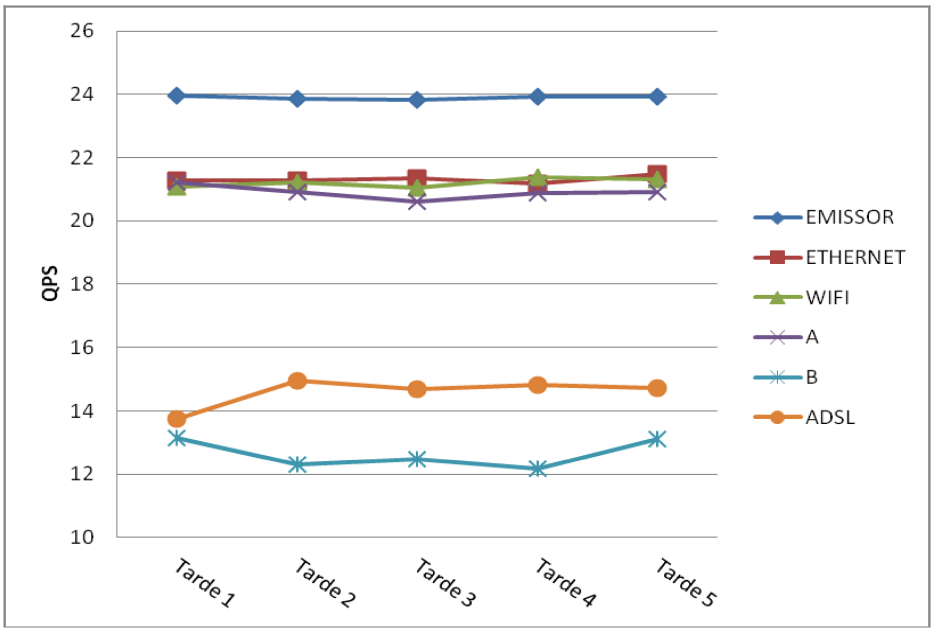

Figura 31: Taxa de QPS no Período da Tarde para o Ambiente Institucional e Internet.

Na Tabela 8 é apresentada a distribuição percentual de QPS abaixo de 10 QPS e igual ou superior a 10 QPS, relativos aos experimentos realizados no Ambiente Institucional e Internet.

Tabela 8: Distribuição Percentual da Taxa de QPS em Classes para o Ambiente Institucional e Internet.

QPS (%)	< 10	≥ 10
EMISSOR	0,01%	99,99%
ETHERNET	0,11%	99,88%
WIFI	0,39%	99,61%
A	1,30%	98,70%
B	47,67%	52,33%
ADSL	37,17%	62,83%

8.4. ANÁLISE ESTATÍSTICA

As análises estatísticas foram realizadas separadamente para o Ambiente Institucional e para o Ambiente Institucional e Internet, considerando três conjuntos representados pelo período da manhã, período da tarde e pelo total de experimentos. Para esse processo, foi utilizado o teste de Friedman com nível de significância de 5% e pós-teste de Dunn.

8.4.1. ANÁLISE ESTATÍSTICA DOS RESULTADOS DO AMBIENTE INSTITUCIONAL

Na Tabela 9 são apresentados os resultados da análise estatística comparando-se a quantidade de QPS transmitidos pelo EMISSOR, definido como grupo controle, com as taxas de QPS recebidas pelos clientes ETHERNET e WIFI dos períodos de experimentação manhã e tarde no Ambiente Institucional.

Tabela 9: Comparação das Taxas de QPS do Período de Experimentação Manhã e Tarde no Ambiente Institucional.

Comparações	p-valor Manhãs	p-valor Tardes	p-valor Conjunto
EMISSOR vs. ETHERNET	< 0,0001	< 0,0001	< 0,0001
EMISSOR vs. WIFI	< 0,0001	< 0,0001	< 0,0001
ETHERNET vs. WIFI	0,1183	> 0,9999	0,2111

8.4.2. Análise Estatística dos Resultados do Ambiente Institucional e Internet

Na Tabela 10 são apresentados os resultados estatísticos para o Ambiente Institucional e Internet comparando-se a quantidade de QPS transmitida pelo EMISSOR, definido como grupo controle, com as taxas de QPS recebidas pelos clientes ETHERNET, WIFI, A, B e ADSL dos períodos de experimentação manhã e tarde.

8.5. Resoluções de Imagens Provenientes de Exames de Vídeocolonoscopia

Nesta seção são apresentadas imagens relativas a exames videocolonoscópicos, contrastando-se as diferenças de percepção visual em virtude da utilização de distintas resoluções. Na Figura 32, uma imagem original, com resolução de 1024 x 768 *pixels*, de exame videocolonoscópico é demonstrada. Nessa imagem destaca-se, em cor amarela, uma área recortada com exibição de modo ampliado em 800% (Figura 33).

Nas Figuras 34, 35, 36 e 37 ilustram-se a imagem exibida na Figura 33, com as resoluções 720 x 540 *pixels*, 480 x 360 *pixels*, 360 x 270 *pixels* e 320 x 240 *pixels*, respectivamente.

Tabela 10: Comparação das Taxas de QPS do Período de Experimentação Manhã e Tarde no Ambiente Institucional e Internet.

Comparações	p-valor Manhãs	p-valor Tardes	p-valor Conjunto
EMISSOR vs. ETHERNET	< 0,0001	< 0,0001	< 0,0001
EMISSOR vs. WIFI	< 0,0001	< 0,0001	< 0,0001
EMISSOR vs. A	< 0,0001	< 0,0001	< 0,0001
EMISSOR vs. B	< 0,0001	< 0,0001	< 0,0001
EMISSOR vs. ADSL	< 0,0001	< 0,0001	< 0,0001
ETHERNET vs. WIFI	> 0,9999	0,2384	0,3205
ETHERNET vs. A	0,0395	< 0,0001	< 0,0001
ETHERNET vs. B	< 0,0001	< 0,0001	< 0,0001
ETHERNET vs. ADSL	< 0,0001	< 0,0001	< 0,0001
WIFI vs. A	0,4556	< 0,0001	< 0,0001
WIFI vs. B	< 0,0001	< 0,0001	< 0,0001
WIFI vs. ADSL	< 0,0001	< 0,0001	< 0,0001
A vs. B	< 0,0001	< 0,0001	< 0,0001
A vs. ADSL	< 0,0001	< 0,0001	< 0,0001
B vs. ADSL	< 0,0001	< 0,0001	< 0,0001

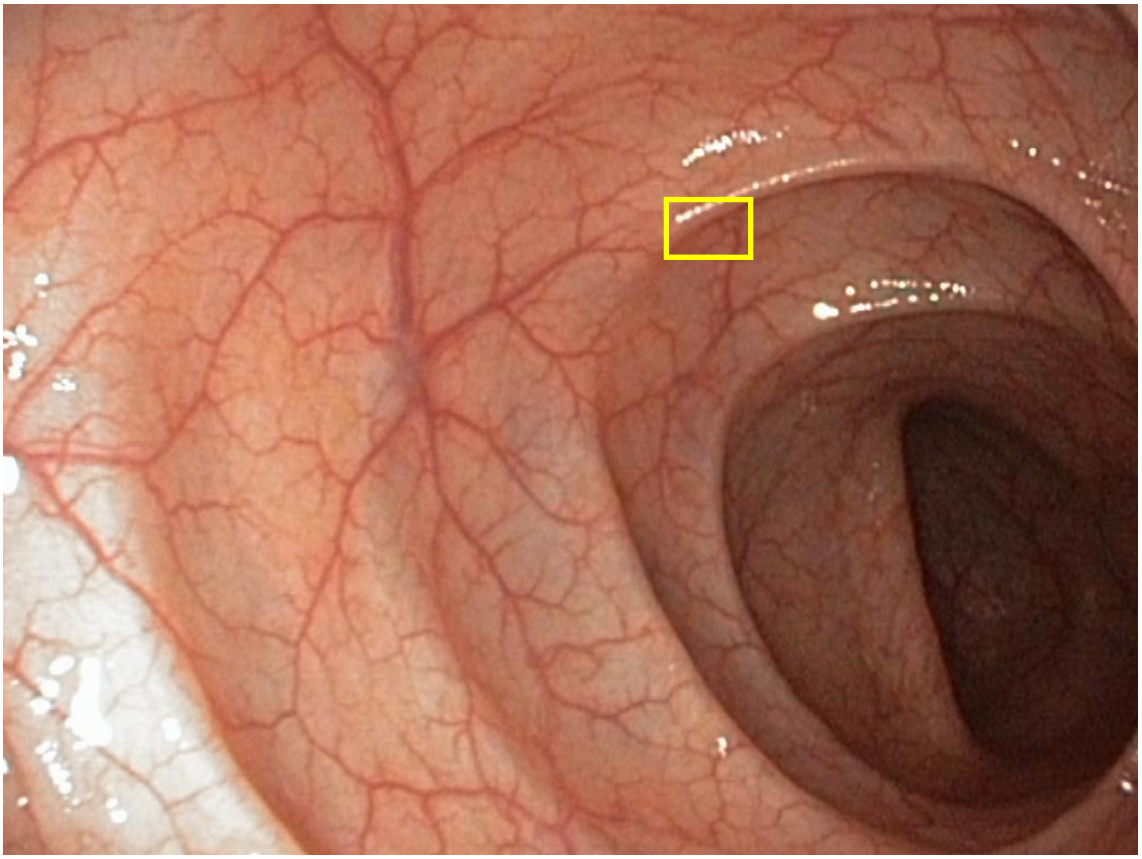

Figura 32: Imagem de Videocolonoscopia em Resolução 1024 x 768 *Pixels*.

Figura 33: Recorte da Imagem em Resolução 1024 x 768 *Pixels* com Zoom de 800%.

Figura 34: Recorte da Imagem em Resolução 720 x 540 *Pixels*.

Figura 35: Recorte da Imagem em Resolução 480 x 360 *Pixels*.

Figura 36: Recorte da Imagem em Resolução 360 x 270 *Pixels*.

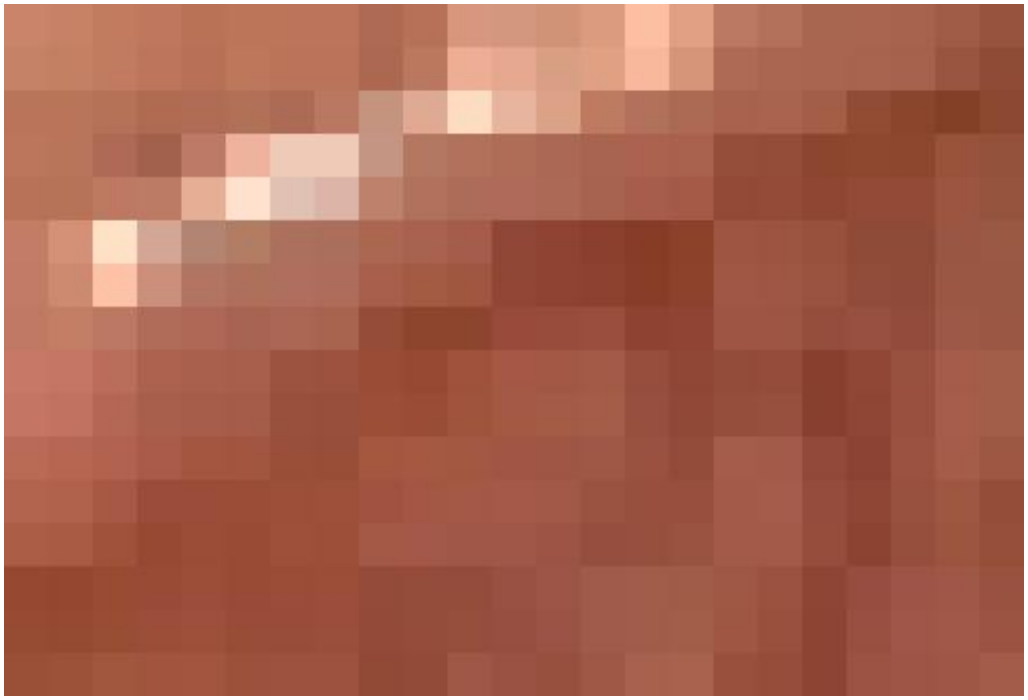

Figura 37: Recorte da Imagem em Resolução 320 x 240 *Pixels*.

9. DISCUSSÃO

9.1. CONSIDERAÇÕES GERAIS

Nas últimas décadas, o rápido desenvolvimento dos recursos de tecnologia da informação tem ocasionado aumento das aplicações em diversificadas áreas de conhecimento (123-128, 32, 129, 130). Nesse contexto, o avanço computacional na capacidade de armazenamento e de processamento, no aprimoramento dos métodos de segurança nas aplicações computacionais, no desenvolvimento de novas técnicas de comunicação de dados, na popularização da Internet e dos sistemas direcionados para a *Web*, tem permitido, de modo sinérgico, a realização de trabalhos multidisciplinares aplicados à área de saúde (131-135).

A popularização do acesso à Internet proporciona a criação de novos serviços em diferentes áreas de conhecimento (136, 137). Dentro desse escopo, a medicina também usufrui dessa ferramenta computacional, e decorrente ao fato, diversos trabalhos neste tema têm sido realizados (18, 32, 40, 42, 44, 45, 65, 67, 123, 124, 131-135, 138-154).

A aplicação de processos tecnológicos à medicina vem de longa data histórica, desde o trabalho clássico do Einthoven (49), o qual demonstrou a possibilidade de transmissão de dados de exames de eletrocardiogramas através de linhas telefônicas, passando pela época de transmissão por rádio e pela televisão, até alcançar os dias atuais, utilizando-se da transmissão por meio da Internet (50, 51, 155).

O desenvolvimento desses novos recursos computacionais tem contribuído para a automatização dos processos em hospitais e em clínicas, principalmente no que se refere ao registro de informações de pacientes em bases de dados (45, 58, 57, 156). No entanto, importantes procedimentos na área da saúde ainda não são regidos por mecanismos automáticos e podem ser otimizados com o emprego de soluções computacionais (32, 89, 157-159). Estes fatos estão diretamente relacionados à falta de recursos tecnológicos disponibilizados e, como exemplo, cita-se a captura, o acompanhamento e a análise de exames e de processos que utilizam vídeos e imagens, tais quais exames de endoscopia digestiva alta e baixa, laparoscopia, entre outros (3, 32).

Apesar de existirem diversos trabalhos na área de telemedicina com o intuito de desenvolver tecnologias que visam auxiliar a atividade médica (3, 5-7, 53-56, 58-61, 155, 156), até o momento, não é de nosso conhecimento a proposição de um método

computacional com a finalidade de viabilizar o acompanhamento e a discussão, em tempo real, sobre procedimentos médicos juntamente com a comunicação com equipamentos diagnósticos endoscópicos. Outro aspecto fundamental quando se trata do tema transmissão de dados médicos é a manutenção, em consideração máxima, de aspectos como integridade, confidencialidade e autenticidade dessas informações. Dentro dessa linha, modelos vêm sendo propostos e desenvolvidos para alcançar o quesito segurança, mas todos são passíveis de críticas (14, 15, 83, 84, 91-93).

Desse modo, na idealização do S2TR, o tema segurança do tráfego dos dados referentes ao exame endoscópico foi desenvolvido com a finalidade de bloquear acessos indevidos aos fluxos de vídeo e de áudio disponibilizados para o acompanhamento remoto dos procedimentos médicos, assim como todas as informações pertencentes aos pacientes e aos profissionais da área de domínio. Esses módulos de segurança foram implementados, de modo original, por meio de recursos criptográficos e da geração de chaves secretas inspirada em conceitos da Teoria da Evolução das Espécies (106, 107).

Vale a pena ressaltar que processos tecnológicos inovadores, frequentemente, estão diretamente relacionados com altos custos operacionais, desde o desenvolvimento, a disponibilização e a manutenção por meio de Empresas Privadas (18, 19, 79, 80, 160-163).

Em Estados brasileiros, como o Paraná, a inclusão digital e o uso de *software* livre em algumas repartições públicas já alcançaram, em seis anos, resultados positivos com economia de mais de 300 milhões de reais dos cofres públicos (164). Ainda sobre o tema, o investimento para ampliar o uso de aplicativos desenvolvidos em plataformas livres deverá sofrer um aumento de cinco vezes do valor estipulado no ano de 2008 representado por quatro milhões de euros para 22 milhões (165, 166).

Assim sendo, atento ao fato, neste trabalho utilizou-se para o desenvolvimento do S2TR, ferramentas computacionais na modalidade *open source*. Com esse processo, acredita-se que critérios como redução de custo operacional, customização, qualidade de segurança e liberdade de ação de implementação foram alcançados (78-81).

A partir da identificação dessas possibilidades de melhorias e das contribuições que podem ser aplicadas para a área da saúde, construiu-se, neste trabalho, um método em telemedicina para o acompanhamento remoto e em tempo real de procedimentos

videocolonoscópicos. Essa abordagem foi definida com a finalidade de promover a discussão, antes, durante e após a realização do exame endoscópico por meio de distintas mídias representadas por vídeo, áudio, texto e imagens. Além desse processo, os profissionais da área médica são capazes de participar ativamente do exame executando a captura e o compartilhamento das imagens relativas ao mesmo (151, 154, 167-169).

De modo a implementar o método em telemedicina proposto, desenvolveu-se neste trabalho o S2TR, um sistema computacional aplicado para exames videocolonoscópicos. Para auxiliar no melhor entendimento, a discussão acerca do desenvolvimento e da experimentação desse sistema está organizada nas seguintes seções:

- Análise de desempenho no Ambiente Institucional;
- Análise de desempenho no Ambiente Institucional e Internet.

9.2. ANÁLISE DE DESEMPENHO NO AMBIENTE INSTITUCIONAL

O Ambiente Institucional foi representado pela rede local com tecnologia Gigabit Ethernet (31) com presença de dois clientes, sendo um conectado através de cabo a essa rede local (ETHERNET), enquanto o outro por meio de redes sem fio com padrão 802.11b (WIFI) (120). Ainda nos experimentos, o vídeo utilizado apresentava resolução 1024 x 768 *pixels*, taxa de *bitrate* de 13000 Kbps e sem a utilização de algoritmos de compactação, ou seja, com qualidade máxima. A taxa de *bitrate* possui uma relação direta com a qualidade do vídeo e varia de acordo com o número de *pixels* da imagem obtidos por meio da resolução e da quantidade de imagens transmitidas por segundo (170, 171).

Essa configuração se deve ao fato de coincidir com a resolução máxima aplicada no monitor de vídeo e a respectiva taxa de *bitrate* proporcionada pelo videocolonoscópio marca *Fuginon* modelo 4400 (122), aparelho este usado na Gastrocentro da UNICAMP.

Essa similaridade do cenário computacional foi essencial, pois reproduz as redes de informática e de equipamentos presentes na maioria de Instituições de Ensino e de Pesquisa do Brasil, como por exemplo, na Universidade Estadual de Campinas (UNICAMP), Universidade Federal do Paraná (UFPR), Universidade de São Paulo (USP), Universidade Federal do Rio Grande do Sul (UFRGS), Universidade Federal de Santa Catarina (UFSC), Universidade Federal de Minas Gerais (UFMG), Centro de Engenharias e Ciências Exatas

da Universidade Estadual do Oeste do Paraná (CECE/UNIOESTE), Universidade Estadual de Maringá (UEM), Universidade Federal do Pará (UFPA), Universidade Federal do Amazonas (UFAM), Universidade de Brasília (UnB), entre outras.

Com isso e em ambiente controlado, os experimentos de análise da eficiência e da precisão do S2TR, foram realizados e monitorados por meio da taxa de transmissão de Quadros por Segundo (QPS).

A quantidade QPS é definida como a unidade de medida de um dispositivo audiovisual e é caracterizada pelo número de imagens registrado, processado e exibido por unidade de tempo (172).

Essa unidade é fundamental pelo fato de que a cognição visual humana apresenta dependência direta em relação ao número de quadros recebidos e projetados em interface de imagem como a tela de um computador, e essa taxa interfere na qualidade da imagem apresentada (173, 174).

Os vídeos com taxas inferiores a 10 QPS causam sensação de descontinuidade, pois as falhas de configuração da imagem são perceptíveis à visão humana (173-177). Sob esse aspecto, Apteker et al. (175) demonstraram que os usuários possuem uma percepção diferente, dependendo do conteúdo, quanto à taxa de transmissão de QPS. Resultados similares foram encontrados por Steinmetz (176), por meio de série de experimentos a respeito da percepção humana.

Wang, Claypool e Zuo (178) realizaram um estudo sobre o tráfego de fluxo de vídeo a partir de servidores para usuários em diversos locais geográficos. Esses vídeos eram de alta qualidade, tipicamente contendo 10 QPS e constataram que o desempenho foi influenciado, em grande parte, pela largura de banda da conexão do usuário com a Internet. Vale ressaltar que esses resultados foram confirmados por outro trabalho de Wang e Claypool (179).

Na Seção 8.5 do Capítulo 8 foi apresentada uma mesma imagem, em distintas resoluções, demonstrando o impacto desse atributo sobre a qualidade da imagem. À medida que as resoluções foram reduzidas, as imperfeições das imagens se tornaram mais perceptíveis e, por conseguinte, podem dificultar na realização de análises e de diagnósticos.

McCarthy, Sasse e Miras (180) realizaram análise prospectiva para comparar os efeitos de quantização *versus* taxas de transmissão de QPS para fluxos de vídeo, aplicando testes de percepção em 37 indivíduos, antes e após treinamento. Os autores concluíram que, ao contrário do relatado em outros estudos, os usuários mostraram maior preferência por alta resolução à alta taxa de exibição de QPS. Os resultados desse estudo representam importantes implicações para os provedores de serviço e *designers* de aplicações de fluxo de vídeos.

Diante desse cenário, o método proposto neste trabalho teve como propósito empregar a máxima qualidade disponibilizada pelo equipamento de videocolonoscopia e a manutenção das resoluções aplicáveis às características dos ambientes de redes definidos, mesmo que para isso, acarrete em redução de taxas de QPS.

Por meio dos trabalhos citados, é notório o entendimento de que o processo de cognição humana apresenta-se de modo multivariável. Esse processo constitui um dos problemas clássicos em visão computacional devido à ampla gama de aplicações possíveis, bem como os respectivos desafios associados. Embora muitas abordagens se comportem bem para alguns casos específicos, existe ainda, de modo tímido, pesquisa sobre a praticidade e a robustez dessas abordagens em cenários reais, nos quais vídeos são adquiridos, frequentemente, com diferentes taxas de transmissão de QPS a partir de diversas fontes de imagens.

Nesse sentido, Harjanto et al. (174) investigaram e avaliaram o desempenho de quatro abordagens do estado da arte para reconhecimento de movimentos humanos. Nos experimentos realizados, apesar dos três diferentes valores de taxas de transmissão de QPS considerados e analisados, não se encontrou diferença no desempenho. Assim, melhores abordagens de reconhecimento, incluindo novas características visuais e algoritmos de aprendizado robustos à variação de taxas de transmissão de QPS são necessários para o desenvolvimento, na prática, desse processo.

Desse modo, com a preocupação nos quesitos eficiência e precisão nas taxas de transmissão de QPS e para assegurar consistente percepção visual dos dados, neste trabalho, foi estipulada a taxa de transmissão, a partir do EMISSOR, em 25 QPS, ou seja,

150% acima da referida pela maioria dos trabalhos na literatura acerca do tema (172, 173, 176, 178-181).

Sob esse escopo, no Ambiente Institucional, verificou-se que o computador responsável pelo envio do vídeo, denominado de EMISSOR, obteve uma taxa de transmissão de 23,73 QPS no período da manhã e de 23,83 QPS no período da tarde. Já o cliente ETHERNET recebeu os fluxos de vídeo em taxas de 21,32 QPS e 21,43 QPS nos turnos manhã e tarde, respectivamente.

Os valores dessas taxas mostraram que ocorreram perdas de quadros durante a captura e o envio de imagens. Essa perda de dados pode ser devido a uma série de razões como mecanismos de processamento da Unidade Central de Processamento (CPU) do EMISSOR e do servidor, sincronização na captura de áudio e vídeo, e pelo comutador da rede de comunicação de dados (181-186). Além dessas razões, outros motivos também interferem na taxa de transmissão como problemas de ordem elétrica, danos de componente mecânico e do disco rígido, superaquecimento do processador, incompatibilidade de *hardware*, corrupção de aplicativos, presença de vírus, falta de higienização do computador, entre outras (187-189).

Assim sendo, o delineamento dos passos experimentais foi realizado com a precaução para que essas situações fossem previamente controladas, e com isso, todos os equipamentos e acessórios eram testados, sempre, antes de cada experimento. Ainda, para evitar as oscilações e quedas de energia elétrica, os componentes computacionais de *hardware* se apresentavam conectados em *nobreak*. Cabe ressaltar que em nenhum momento, durante todos os experimentos, ocorreu a falta de energia.

Outro aspecto fundamental foi a definição do período em que os testes seriam realizados, ou seja, no período da manhã, às 10h00 e às 11h00, e da tarde, às 15h00 e às 16h00.

Esses períodos representam momentos de intenso fluxo de uso da Internet, quando um elevado número de pessoas está utilizando algum tipo de serviço dessa rede, repercutindo na velocidade e na qualidade de transmissão dos dados (190). Desse modo, foi possível realizar os experimentos em um cenário de máxima utilização da Internet que de acordo com IBOPE Media (191), há no Brasil 53,9 milhões de usuários dessa rede mundial

e a transmissão de todo esse fluxo de dados pode ser realizado por diversos meios, como satélite, rádio, fibra ótica, entre outros.

O cliente WIFI, conectado de modo sem fio a um *Access Point* com codificação 802.11b, obteve taxas de recebimento de QPS de 20,95 e de 21,15 em experimentos realizados no período da manhã e no período da tarde, respectivamente. Esses valores também indicam uma redução da taxa de QPS recebida em relação à taxa de QPS enviada.

Conforme estudos de pesquisas anteriores (172, 173, 176, 178-181), vídeos com taxas inferiores ao limiar de 10 QPS podem causar a percepção de descontinuidade ao ser humano. Assim sendo, neste trabalho, foi considerado este valor de QPS como o valor de referência para a realização das análises.

Na Tabela 4 do Capítulo 8, verifica-se que durante todos os experimentos realizados, o EMISSOR enviou, em apenas 0,01% do tempo, quadros com taxa abaixo de 10 QPS, enquanto que o cliente ETHERNET recebeu taxas menores que 10 QPS em 0,06% do tempo e o cliente WIFI obteve taxas abaixo de 10 QPS em 1,82% do tempo.

Esses resultados demonstram que, considerando o cenário completo, apenas em uma pequena parcela do tempo, ocorreram taxas de transmissão menores que 10 QPS e embora todas as precauções tomadas neste trabalho em se prevenir os problemas descritos anteriormente quanto à perda de quadros durante a transmissão, ainda assim, essas perdas são passíveis de acontecer.

Em relação ao EMISSOR, as diferenças são justificadas por seu próprio processamento. No caso do cliente ETHERNET, este sofre atrasos promovidos pelo processamento do servidor, do *switch* da rede, pela latência da rede e por seu próprio processamento (1, 36). Já o cliente WIFI recebe o impacto dos mesmos elementos citados em relação ao cliente ETHERNET e, adicionalmente, decorrente ao sinal ser transmitido por ondas de rádio, este cliente sofre as influências como distância entre o *Access Point* e o cliente WIFI, presença de barreiras físicas no percurso da onda de rádio, interferências de sinais, entre outros (36, 192).

Por meio da avaliação estatística verificou-se que houve diferença estatisticamente significativa considerando as taxas de QPS entre o EMISSOR e o cliente ETHERNET (p-valor < 0,0001) e entre o EMISSOR e o cliente WIFI (p-valor < 0,0001). Não foi

constatada diferença estatisticamente significativa de desempenho entre os clientes ETHERNET e WIFI para os experimentos realizados no Ambiente Institucional (p-valor=0,2111). No momento em que foram analisados de modo separado, também não encontrou diferença estatisticamente significativa para o período da manhã (p-valor=0,1183) e para o período da tarde (p-valor=0,9999).

Desse modo, verifica-se que a divergência entre o processamento para a transmissão e o recebimento de vídeos por esses dois clientes, de acordo com as configurações adotadas nos experimentos, não foi suficiente para provocar uma diferença de performance estatisticamente significativa entre os clientes ETHERNET e WIFI. Essa similaridade dos resultados experimentais no período da manhã e da tarde, no Ambiente Institucional, era esperado, pois na rede local as conexões são estabelecidas ponto a ponto no *switch* (36) e o cliente WIFI usava *link* de 54 Mbps, ao passo que a largura de banda utilizada para o recebimento do vídeo era de 13 Mbps.

9.3. ANÁLISE DE DESEMPENHO NO AMBIENTE INSTITUCIONAL E INTERNET

No Ambiente Institucional e Internet utilizou-se um vídeo com resolução de 480 x 360 *pixels* para as avaliações experimentais a qual é maior quando comparada com outras aplicações que disponibilizam vídeos pela Internet, como o *Youtube*, que emprega originalmente como padrão a resolução de 320 x 240 *pixels* (192-194).

O parâmetro de resolução definido neste trabalho também teve como motivação o fato da Gastrocentro da UNICAMP utilizar um sistema local para aquisição de imagens do videocolonoscópio com configuração de resolução de 320 x 240 *pixels*, cuja qualidade, conforme avaliação dos especialistas é suficiente para a realização dos diagnósticos. Desse modo, procurou-se utilizar resolução acima do que é aplicada localmente.

Para a avaliação de desempenho do Ambiente Institucional e Internet, a exemplo do Ambiente Institucional, foi também aplicada qualidade máxima das imagens, isto é, sem utilização de algoritmos de compactação. Por outro lado, a taxa de *bitrate* do vídeo foi de 6000 Kbps para vídeos com resolução de 480 x 360 *pixels*, diferentemente do Ambiente Institucional, que gerou uma taxa de 13000 Kbps. Este fato se deve à utilização de resolução maior, 1024 x 768 *pixels*, no Ambiente Institucional.

Algumas ferramentas computacionais disponibilizadas para a transmissão de vídeo pela Internet, como o site do Terra[12], que faz transmissões esportivas pela Internet em tempo real, usam mecanismos de compactação. Durante a confecção deste trabalho, em um experimento piloto não publicado, foi efetuado *download* de uma transmissão de vídeo com resolução *full* HD de 1920 x 1080 *pixels* a partir desse site. Com esse procedimento, verificou-se que o vídeo possuía uma taxa de *bitrate* de 1000 Kbps, ou seja, seis vezes menor do que a taxa utilizada por este método no Ambiente Institucional e Internet.

Vale ressaltar que os clientes da rede local pertencentes ao Ambiente Institucional e Internet, foram os mesmos utilizados no Ambiente Institucional, sendo um deles o cliente ETHERNET conectado fisicamente à rede por meio da tecnologia Gigabit Ethernet e padrão 802.3z (31), enquanto o outro cliente, denominado de WIFI, conectado à rede local através de conexão de rede sem fio e padrão 802.11b (120).

Em relação aos clientes conectados por meio da Internet, estes foram denominados de cliente A, cuja conexão foi feita por via *link* RNP de 1 Gbps, cliente B com conexão via *link* RNP de 100 Mbps e cliente ADSL por meio do link ADSL de 15 Mbps.

A escolha destes clientes para o processo de avaliação do método proposto foi com o propósito de contemplar diferentes conexões de Internet (1 Gbps, 100 Mbps e ADSL 15 Mbps), comumente usadas por instituições de ensino e pesquisa, bem como usuários e instituições privadas de menor porte.

Assim como no Ambiente Institucional, os experimentos no Ambiente Institucional e Internet foram realizados durante cinco dias úteis de uma semana nos horários 10h00, 11h00, 15h00 e 16h00. Estes horários foram definidos pelo fato de coincidirem com o período em que a carga de tráfego da Internet está mais elevada, promovendo uma análise de desempenho em cenário mais crítico de transmissão de dados (190).

Por meio da análise das Tabelas 5, 6 e 7 do Capítulo 8, foi possível verificar que o computador EMISSOR, responsável pelo envio do vídeo, obteve taxas médias de 23,91 QPS e 23,90 QPS nos períodos da manhã e da tarde, respectivamente. Do mesmo modo que ocorreu no Ambiente Institucional, esse resultado caracteriza a ocorrência de perda no

[12]< www.terra.com.br>.

processo de captura das imagens, de processamento e de envio dos quadros para o Servidor por parte do EMISSOR, pois a taxa média de captura definida foi de 25 QPS (181-189).

Em relação ao cliente ETHERNET, este obteve uma taxa de recepção de 21,44 QPS e 21,32 QPS, considerando-se respectivamente os experimentos realizados no período da manhã e da tarde. Já o cliente WIFI obteve as taxas de recebimento de 21,34 QPS no período da manhã e de 21,21 QPS no período da tarde. O desempenho desses clientes, assim como os distintos processamentos que influenciaram esses resultados em relação à taxa de QPS enviado pelo EMISSOR, são os mesmos apresentados em relação ao Ambiente Institucional, uma vez que estes clientes e o modo de conexão são os mesmos apresentados naquele ambiente.

Quanto aos clientes conectados à Internet, o cliente A recebeu o vídeo a uma taxa de 21,22 QPS nos experimentos realizados no período da manhã e 20,91 QPS no período da tarde. Entre os clientes pertencentes a esse cenário, este foi o que obteve o melhor desempenho. Os fatores que contribuíram para esse rendimento foram a conexão por meio de *link* de 1 Gbps provido pela RNP e o número de quatro dispositivos intermediários, *hop counts*, entre a origem (EMISSOR) e o destino (cliente A).

O número de *hop counts* influencia no tempo de latência, ou seja, em cada dispositivo intermediário pelo qual um pacote de dados *Transmission Control Protocol* (9) trafega, há um custo de processamento referente às características de *hardware* e *software* destes dispositivos como conversão de protocolos, execução de algoritmos de roteamento, gerenciamento de filas de entrada e de saída, utilização de políticas de controle de congestionamento, entre outros. Desse modo, o número de dispositivos intermediários influencia diretamente na latência do protocolo TCP e, consequentemente, repercute no desempenho na transmissão de *quadros* de vídeo (182, 183, 195-197).

No cliente B, as taxas de QPS alcançadas nos experimentos realizados no período da manhã e no turno da tarde, foram respectivamente de 12,29 QPS e de 12,64 QPS, caracterizando o pior desempenho dentre os clientes avaliados.

A conexão com a Internet da instituição na qual o cliente B está localizado, possui

um *link* de 1 Gbps provido pela RNP[13]. No entanto, internamente, a largura de banda com o Departamento em que foi posicionado o cliente B é de 100 Mbps, sendo este compartilhado por aproximadamente 2000 pessoas entre elas acadêmicos, professores e funcionários. Desse modo, o *link* real é 10 vezes menor quando comparado com o *link* do cliente A. Dos 14 *hop counts* que influenciaram no desempenho do cliente B, sete são externos à rede da instituição e possuem as mesmas características de *hardware* e de *software* dos dispositivos intermediários utilizados em relação ao cliente A. No entanto, foi importante observar que o aumento do número de dispositivos, neste cenário, sobe de quatro para sete, impactando desse modo, também, no desempenho do cliente B. Outro fator que provocou pior desempenho do cliente B foi a existência adicional de sete dispositivos intermediários internos à rede da instituição.

Desse modo, num cenário como o do cliente B, seria necessário alterar configurações da rede interna para melhorar o desempenho do método computacional delineado neste trabalho. Uma dessas alterações seria o posicionamento do cliente B em redes virtuais que estejam próximas a conexão com a Internet, evitando-se processamentos internos desnecessários para essa aplicação e permitindo que o sistema tenha acesso ao *link* de 1 Gbps que a instituição dispõe.

Em relação ao cliente ADSL, foram obtidas taxas de recebimento de fluxo de vídeo de 14,01 QPS nos experimentos realizados no período da manhã e 14,58 QPS à tarde. O canal de conexão utilizado por este cliente é o de menor custo e amplamente disponível para qualquer usuário, sendo utilizado principalmente em ambientes residenciais e empresariais e representa aproximadamente 69% das conexões à Internet utilizadas atualmente no Brasil (198). Neste cliente a conexão contratada foi de 15 Mbps e o número de *hop counts*, entre a origem e o destino, era de 10.

Esses resultados permitiram verificar que é possível utilizar o método com conexões ADSL, as quais são comuns e amplamente disseminadas, além de possuírem os custos mais acessíveis.

[13] <http://www.rnp.br/>.

Essa alternativa pode ser aplicada por clínicas e instituições que não possuam outras demandas que consumam grande largura de banda Internet. Os planos atuais de 15 Mbps possuem um custo aproximado de R$ 100,00 mensais. As empresas de Telecomunicações[14] estão disponibilizando, nos dias atuais, conexões com maior largura de banda, como planos de 100 Mbps a um custo mensal médio de R$ 500,00. Esses dados são importantes para a utilização de clientes por meio de canais ADSL.

Também é necessário destacar que as conexões ADSL, diferentemente de outras alternativas abordadas, utilizam apenas 10% de sua largura de banda para *upload*. Desse modo seria necessário um *link* de 100 Mbps para utilizar o método em uma instituição com a finalidade de executar procedimentos médicos, e não somente como cliente.

Em relação ao desempenho, mesmo em conexões ADSL com maior largura de banda, não existe garantia de qualidade de serviço, e o sistema estará sujeito ao efeito da latência provocada pelos dispositivos intermediários. Nessas circunstâncias, caso deseje garantia de desempenho, uma das melhores alternativas é a contratação de conexões dedicadas junto às companhias de Telecomunicações a um custo mensal aproximado de R$1.000,00 por MBps.

Do mesmo modo que no Ambiente Institucional, o valor de 10 QPS foi considerado como referência para realização das análises das taxas de transmissão de fluxo de vídeo enviadas pelo EMISSOR e recebidas pelos clientes.

Na Tabela 8 do Capítulo 8, constata-se que o EMISSOR enviou taxas abaixo de 10 QPS em 0,01% do tempo, enquanto os clientes apresentaram taxas de recebimento de quadros inferiores a 10 QPS nos seguintes percentuais de tempo: cliente ETHERNET 0,11%, cliente WIFI 0,39%, cliente A 1,30%, cliente B 47,67% e cliente ADSL 37,17%.

Esses dados reforçam os resultados de desempenho do EMISSOR e de cada cliente, assim como os fatores que influenciaram esse rendimento. Considerando-se a influência da taxa de QPS sobre a sensação de continuidade do vídeo pela percepção humana (172, 173, 176, 178-181), o efeito de claudicação seria fortemente sentido no cliente B e no cliente ADSL. Mesmo nessas condições, o acompanhamento dos exames é possível, mas com

[14] <http://www.gvt.com.br> e <http://www.oi.com.br>.

prejuízo no vídeo transmitido, assim como a participação remota e a interatividade. Vale ressaltar que esse revés de transmissão não é decorrente ao método proposto neste trabalho, e sim a fatores externos de infraestrutura computacional.

Nesta configuração de ambiente, encontraram-se os seguintes valores de desvios padrão: EMISSOR (0,64), cliente ETHERNET (1,84), cliente WIFI (2,12), cliente A (2,52), cliente B (6,04) e cliente ADSL (6,29). Esses números evidenciam um comportamento instável com relação à taxa de recebimento de QPS no cliente B e no cliente ADSL, que normalmente ocorre na Internet em função de *links* congestionados, de altas taxas de enfileiramento dos pacotes e de problemas de processamento nos dispositivos intermediários (182, 183, 195-197). As particularidades e as melhorias a serem realizadas nestes ambientes, e em outros similares, foram apresentadas, anteriormente, na discussão acerca do desempenho de cada cliente.

A análise estatística dos resultados de desempenho provenientes do Ambiente Institucional e Internet nos períodos de manhã e tarde, conjuntamente, não demonstrou diferença estatisticamente significativa entre os clientes ETHERNET e WIFI (p-valor=0,3205). Para todas as outras comparações conjuntas, foi constatada diferença estatisticamente significativa com p-valor < 0,0001.

Analisando de modo separado os períodos da manhã e da tarde, não foi constatada diferença estatisticamente significativa, pela manhã, com relação ao desempenho dos clientes ETHERNET e WIFI (p-valor > 0,9999) e WIFI e Cliente A (p-valor=0,4556). No entanto, realizando-se a mesma avaliação para os experimentos feitos no período da tarde, a diferença de desempenho foi estatisticamente significativa para todas as comparações (p-valor < 0,0001), exceto para ETHERNET e WIFI (p-valor=0,2384).

Esses resultados são esperados já que os clientes ETHERNET e WIFI encontram-se na rede local e, portanto, não estão sujeitos à influência de fatores externos, como a existência de *hop counts*. O Cliente A, por sua vez, apesar de se encontrar na Internet, possui um baixo número de *hop counts* e um *link* de largura de banda alto e por isso o seu desempenho foi o melhor entre os clientes Internet, aproximando-se dos valores dos clientes na rede local.

9.4. CONSIDERAÇÕES FINAIS

As contribuições deste trabalho incluem:

Ambiente Institucional:

- Validação da aplicação do S2TR com a resolução máxima disponível pelo videocolonoscópio Fuginon 4400 e sem compactação;
- Aplicação remota do S2TR para o acompanhamento dos vídeos relativos aos exames de videocolonoscopia, bem como a interação com os demais participantes, locais e remotos;
- Captura e compartilhamento de imagens com resoluções e qualidade superiores às utilizadas, atualmente, no sistema localizado na sala de Videocolonoscopia da Gastrocentro da UNICAMP.

Ambiente Institucional e Internet:

- Aplicação do S2TR utilizando-se de resolução de 480 x 360 *pixels,* sem compactação. Esta resolução é maior do que a ampla maioria dos vídeos disponibilizados na Internet e também maior que a utilizada na sala de videocolonoscopia da Gastrocentro da UNICAMP para a captura de imagens (360 x 240 *pixels*);
- Utilização do S2TR em conexões ADSL, caracterizadas por apresentarem baixo custo e amplo uso pela população, de modo remoto e em tempo real, durante a realização dos exames videoendoscópicos.

10. CONCLUSÕES

Os resultados deste trabalho permitiram alcançar as seguintes conclusões:

1. O método proposto, implementado no sistema computacional S2TR, cumpre os requisitos estabelecidos para transmissão de dados, segurança de informações e interação em tempo real entre os usuários;
2. O método proposto é aplicável para a realização de procedimentos videocolonoscópicos, em redes locais e na Internet.

11. REFERÊNCIAS BIBLIOGRÁFICAS

1. Tanenbaum AS, Wetherall DJ. Networks Computers. United States of America: Prentice Hall. 2011. 960p.

2. Colin P. RTP audio/video transport for the internet. United States of America: Addison-Wesley. 2003. 414p.

3. World Health Organization. Telemedicine: Opportunities and Developments in Member States. Geneva: WHO. Global Observatory for eHealth, 2009. 94p.

4. Cao DM, Shuji S, Yasuaki A, Nobuhiro T, Kuriko K, Koji O, et al. Emerging Technologies for Telemedicine. Korean J Radiol 2012; 13(4):S21-S30.

5. Wootton R, Jebamani LS, Dow SA. E-health and the Universitas 21 organization: 2. Telemedicine and underserved populations. Journal of Telemedicine and Telecare. 2005; 5(11):221-224.

6. Gazula K. Novel One Integrated System For Real-Time Virtual Face-To-Face Encounters. Patente US 2011/0106557 A1. 2009.

7. Silva Filho EV, Passos MG, Santos BA, Oliveira SS, Melo EAG, Motta GHMB, Tavares TA, Filho GLS. Uma Ferramenta para Gerenciamento e Transmissão de Fluxos de Vídeo em Alta Definição para Telemedicina. Anais do XXX Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos. 2012; 948-955.

8. Leiner BM, Cerf VG, Clark DD, Kahn RE, Kleinrock L, Lynch DC, et al. The Past and Future History of the Internet. Commun. ACM. 1997; 40(2):102-108.

9. Yanowitz J. Under the hood of the Internet: an overview of the TCP/IP protocol suite. Crossroads - Special issue on the Internet, 1994; 8-10.

10. Chen Z, Yu X, Feng D. Telemedicine system over the internet. In Pan-Sydney Workshop on Visualisation (VIP '00). 2000; 2(1):113-118.

11. Iren S, Amer PD, Conrad PT. The transport layer: tutorial and survey. ACM Comput. Surv. 1999; 31(4):360-405.

12. Rindfleisch TC. Privacy, information technology, and health care. Commun., ACM. 1997; 40(8):93-100.

13. Maciel JN, Machado RB, Wu, FC, Lee HD, Fagundes JJ, Goes JRN. Protótipo de Conferência Multimídia e Transmissão de Dados de Experimentos Médicos em Tempo Real pela Web. Anais do VI Workshop de Informática Médica WIM 2006, 2006; 52-61.

14. Cole E. Network Security Bible. Wiley Publishing. 2009. 936p.

15. Stallings W. Cryptography and network security - principles and practice. 3ª ed. Prentice Hall. 2003. 681p.

16. Siponen MT. Information Security Management Standards: Problems and Solutions, 7th Pacific Asia Conference on Information Systems. 2003; (46)5:267-270.

17. Mallapragada G, Grewal R, Lilien G. User-Generated Open Source Products: Founder's Social Capital and Time to Product Release. Marketing Science. 2012; 31:474-492.

18. Almeida AGC, Bortolon S, Berger M, Junior HS. Integração de PACS Software Livre em Aplicações Médicas: Gerenciamento de Pesquisas Clínicas Multicêntricas e de Prontuários Digitalizados. Anais do Workshop de Informática Médica (WIM). SBC. 2008; 235-238.

19. Karels MJ. Commercializing Open Source Software. Queue - The Business of Open Source 2003; 1(5):40-50.

20. Collen MF. A History of Medical Informatics in the United States: 1950 to 1990. American Medical Informatics Association. 1995. 489p.

21. Randell B, Wilkes MV, Ceruzzi PE. Digital computers, history of. In: Encyclopedia of Computer Science. 4ed. John Wiley and Sons Ltd. 2003. 545-570.

22. Greer AL. Medical technology: Assessment, adoption, and utilization, Journal of Medical Systems, Kluwer Academic Publishers-Plenum Publishers. 1981. 129-145.

23. Goldstine HH, Goldstine A. The Electronic Numerical Integrator and Computer (ENIAC). Mathematical Tables and Other Aids to Computation). Reprinted in IEEE Annals of the History of Computing 18, No. 1 (Spring 1996). 1946; 2(15):97-110.

24. Knuth DE. The IBM 650: An Appreciation from the Field. IEEE Annals of the History of Computing. 1986; 8(1):50-55.

25. Schmeck HMJ. Computers Bound for Medical Role. The New York Times. 1960.

26. Plumb RK. Computer Makes Heart 'Diagnosis'. The New York Times. 1962.

27. Greenes RA, Barnett GO, Klein SW, Robbins A, Prior RE. Recording, retrieval and review of medical data by physician-computer interaction. N Engl J Med. 1970; 282(6):307-315.

28. Collen MF. Cost and technology: the case for preventive medicine. Clin Eng. 1978;6(6):65-8.

29. Roberts HE, Yates W. Altair 8800 minicomputer. Popular Electronics (Ziff Davis). 1975; 7 (1):33-38.

30. Metcalfe RM, Boggs DR. Ethernet: distributed packet switching for local computer networks (1976). Commun ACM 19. 1983; 26(1):90-95.

31. Institute of Electrical and Electronics Engineers. IEEE Standard for Information technology - Specific requirements - Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications. IEEE 802.3 Standard Specification. 2008 [Acesso em 3 abril 2013]. Disponível em: URL: http://standards.ieee.org/about/get/802/802.3.html.

32. Shortliffe EH, Cimino JJ. Biomedical informatics: computer applications in health care and biomedicine. 3ª ed. New York: Springer Science Business Media. 2006. 1017p.

33. Greenes RA. OBUS: a microcomputer system for measurement, calculation, reporting, and retrieval of obstetric ultrasound examinations. Radiology. 1982;144(4):879-83.

34. Templeton AW, Dwyer SJ 3rd, Johnson JA, Anderson WH, Hensley KS, Rosenthal SJ, Lee KR, Preston DF, Batnitzky S, Price HI. An on-line digital image management system. Radiology. 1984;152(2):321-5.

35. Arenson RL, Seshadri SB, Kundel HL, DeSimone D, Van der Voorde F, Gefter WB, Epstein DM, Miller WT, Aronchick JM, Simson MB, et al. Clinical evaluation of a

medical image management system for chest images. AJR Am J Roentgenol. 1988; 150(1):55-9.

36. Kurose JF, Ross KW. Computer Networking: A Top-Down Approach. 5ª ed. Addison-Wesley Publishing Company. USA. 2009. 634p.

37. Berners-Lee T, Cailliau R. WorldWideWeb: Proposal for a HyperText Project. 1990. [Acesso em 25 Jan 2013]. Disponível em: URL: http://www.w3.org/Proposal.html.

38. Leiner BM, Cerf VG, Clark DD, Kahn RE, Kleinrock L, Lynch DC, et al. The past and future history of the Internet. Magazine Commun ACM 40, 1997; 40(2):102-108.

39. Shortliffe EH. The Evolution of Health-Care Records in the Era of the Internet. Medinfo 98, 1998; 8(14):1-8.

40. Abate AF, Nappi M, Tortora G, Tucci M. Assisted browsing in a diagnostic image database. Proceedings of the workshop on Advanced visual interfaces (AVI '96). 1996; 223-232.

41. Duarte DCS, Aires T, Leite JC, Lemos G. A user's interface project for the Infralife system videoconference module. Proceedings of the Latin American conference on Human-computer interaction (CLIHC '03). ACM. 2003; 227-230.

42. Argenziano M, Katz M, Bonatti J, Srivastava S, Murphy D, Poirier R, et al. Results of the Prospective Multicenter Trial of Robotically Assisted Totally Endoscopic Coronary Artery Bypass Grafting. Ann Thorac Surg 81. 2006; 81(5):1666-1674.

43. Mougiakakou SG; Valavanis IK, Mouravliansky NA, Nikita KS, Nikita, KS. DIAGNOSIS: A Telematics-Enabled System for Medical Image Archiving. Management, and Diagnosis Assistance. Instrumentation and Measurement, IEEE Transactions on. 2009; 58(7):2113-2120.

44. Ford ST, Viola I, Bruckner S, Torp H, Kiss G. HeartPad: real-time visual guidance for cardiac ultrasound. Proceedings of the Workshop at SIGGRAPH Asia (WASA '12). ACM. 2012; 169-176.

45. Rygh E, Arild E, Johnsen E, Rumpsfeld M. Choosing to live with home dialysis-patients' experiences and potential for telemedicine support: a qualitative study. BMC Nephrology. 2012; 13(13):1-8.

46. Soirefmann M, Blom MB, Leopoldo L, Cestari T. Telemedicina: uma revisão da literature. Revista HCPA. 2008; 28(2):116-119.

47. World Health Organization. Bridging the "know–do" gap: meeting on knowledge translation in global health. Geneva: WHO. 2006. [Acesso em 24 Ago 2012]. Disponível em: URL: http://www.who.int/kms/WHO_EIP_KMS_2006_2. pdf.

48. Craig J, Patterson V. Introduction to the practice of telemedicine. Journal of Telemedicine and Telecare. 2005; 1(11):3-9.

49. Einthoven W. Le télécardiogramme [The telecardiogram]. Archives Internationales de Physiologie, 1906; 4(1):132-164.

50. Costa FJ. O médico homeopata da família. Rio de Janeiro: Almeida Cardoso. 1924. 1050p.

51. Gershon-Cohen J, Cooley AG. Telegnosis. Radiology. 1950; (55):582-587.

52. Zundel KM. Telemedicine: history, applications, and impact on librarianship. Bull Med Libr Assoc. 1996; 1(84):71-9.

53. Benschoter RA, Eaton MT, Smith P. Use of videotape to provide individual instruction in techniques of psychotherapy. Academic Medicine. 1965; 40(12):1159-1161.

54. Anupam V, Bajaj C. Shastra: Multimedia Collaborative Design Environment. IEEE Multimedia. 1994; 1(2):39-49.

55. Gomez EJ, Del Pozo F, Quiles JA, Arredondo MT, Rahms H, Sanz M, et al. Telemedicine System for Remote Cooperative Medical Imaging Diagnosis. Computer Methods and Programs in Biomedicine. 1996; 49(1):37-48.

56. Sung MY, Kim MS, Sung MW, Kim EJ, Yoo JH. CoMed: a real-time collaborative medicine system. Proceedings of the 13th IEEE Symposium on. 2000; 57(2):117-26.

57. Scharcanski J, Machado MS. Sistema configurável para gerenciar imagens médicas digitais e seus dados associados nas etapas de aquisição, armazenamento, distribuição, recuperação e visualização. Patente PI0406144-6. INPI. 2004.

58. Peifer JW, Hopper A, Burrow M, Sudduth B, Panchal S. A packet-based telemedicine system for communicating information between central monitoring stations and remote patient monitoring stations. Patente TW400503(B) 20000801, 2000.

59. Bassani T, Neto AB, Figueredo MVM, Rogal SRJ. Telemedicine System for Remote Monitoring of Patients. Patente BRPI0603602(A). 2006.

60. Sun A, Jin H, Zheng R, He R, Zhang Q, Guo W, et al. UCIPE: Ubiquitous Context-Based Image Processing Engine for Medical Image Grid. UIC 2007. LNCS 4611. 2007; 4611(2007):888-897.

61. Christ RER, Figueredo MVM, Bassani T, Dias JS, Nievola JC. Sistema de Monitoração Remota de Pacientes em Tempo-Real Através da Intranet do Hospital. Anais do CBIS. 2009; 42-47.

62. Cinaglia P, Tradigo G, Veltri P. A system for acquiring and management of ECG signals by using mobile devices: a support for first intervention in heart attacks. Proceedings of the ACM Conference on Bioinformatics, Computational Biology and Biomedicine (BCB '12). ACM. 2012; 677-682.

63. D'Alessandro M, Computers in radiology. SIGBIO Newsl. 1988; 10(4):2-7.

64. Zimeras S, Gortzis LG. Interactive tele-radiological segmentation systems for treatment and diagnosis. Proceedings of the Internation Journal Telemedicine Applied. 2012; 2012(4):713-739.

65. Sankaranarayanan G, King IH, Ko SY, Lum MJH, Friedman DCW, Rosen J, et al. Portable surgery master station for mobile robotic telesurgery. USA: Proceedings of the 1st international conference on Robot communication and coordination (RoboComm '07). IEEE Press. 2007; 28(1):1-8.

66. Guthart GS, Salisbury JJ. The IntuitiveTM telesurgery system: overview and application. Robotics and Automation. In: Proceedings of the ICRA '00, IEEE International Conference on. 2000; 1(1):618-621.

67. Figueredo MVM, Dias JS. Mobile Telemedicine System for Home Care and Patient Monitoring. Proceedings of the 26th Annual International Conference of the IEEE EMBS, 2004; 7(2):101-107.

68. Weller P, Rakhmetova L, Ma Q, Mandersloot G. Evaluation of a wearable computer system for telemonitoring in a critical environment. Personal Ubiquitous Comput. 2010; 2010(14):73-81.

69. Panayides A, Pattichis MS, Pattichis CS, Loizou CP, Pantziaris M, Pitsillides A. Towards Diagnostically Robust Medical Ultrasound Video Streaming using H.264. Book Biomedical Engineering, 2009; 219-237.

70. Iren S, Amer PD, Conrad PT. The transport layer: tutorial and survey. ACM Comput. Surv. 1999; 31(4):360-405.

71. Akrout NM, Gordon H, Palisson PM, Prost R, Goutte R. StreamWorks: the live and on-demand audio/video server and its applications in medical information systems, Proceedings of the SPIE 2711, Medical Imaging 1996: PACS Design and Evaluation: Engineering and Clinical Issues. 1996; 2711:543-552.

72. Babel M, Pasteau F, Strauss C, Pelcat M, Bédat L, Blestel M, et. al. Preserving data integrity of encoded medical images: the LAR compression framework. Advances in Reasoning-Based Image Processing Intelligent Systems, 2012; 29(1):91-125.

73. Wang B, Kurose J, Shenoy P, Towsley D. Multimedia streaming via TCP: An analytic performance study. ACM Trans. Multimedia Comput. Commun. Appl. 2008; 4(2):16.1-16.22.

74. Bovik A. Handbook of Image and Video Processing. 2ª ed. Elsevier Academic Press. 2005. 1384p.

75. Karam LJ, Lossless Coding. In: Handbook of Image and Video Processing. 2ª ed. Al Bovik A (org). Elsevier Academic Press, 2005; 461-474. Sabin M. Free and open source software development of IT systems. Proceedings of the 2011 Conference on Information Technology Education (SIGITE '11). ACM. 2011; 27-32.

76. Barnett B. Basic Concepts and Techniques of Video Coding and the H.261 Standard. In: Handbook of Image and Video Processing. 2ª ed. Al Bovik A (org). Elsevier Academic Press, 2005; 555-574.

77. Chen JYC, Thropp JE. Review of Low Frame Rate Effects on Human Performance. Journal IEEE Transactions on Systems, Man, and Cybernetics, Part A: Systems and Humans. 2007; 37(6):1063-1076.

78. Piresa FA, Gutierrezab MA, Furuie SS, Rebeloac MS, Moreno RA Santos M, Almeida AGC, Bortolon S, Berger M, Junior HS. Implementação de um sistema integrado de gestão hospitalar usando software livre em arquitetura de três camadas. Anais do IX CBIS, 2004.

79. Duerinckx AJ, Hagan GT, Wanchoo V. Evaluation and early medical experience with an ultrasound mini-PACS system at the VA Medical Center. SPIE Proceedings of Medical Imaging, 1994; 13-18.

80. Sabin M. Free and open source software development of IT systems. Proceedings of the 2011 Conference on Information Technology Education (SIGITE '11). ACM. 2011; 27-32.

81. Kohli N, Verma NK. Videoconferencing System using Open Source Technologies. Proceedings of the International Journal of Computer Applications. 2012; (3):1-3.

82. Kahn D. The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet. 2 ed. Nova York: Macmillan, 1995. 1200p.

83. Horst F. Cryptography and Computer Privacy. Scientific American. 1973; 228(5):15-23.

84. Diffie W; Hellman ME. New directions in cryptography, Information Theory. IEEE Transactions on. 1976; 22(1):644-654.

85. Rivest RL, Shamir A, Adleman L. A method for obtaining digital signatures and public-key cryptosystems. Commun. ACM 21. 1978; (21):120-126.

86. Mueller-Schloer C, Neal WR. The implementation of a cryptography-based secure office system. Proceedings of the National Computer Conference (AFIPS '82). ACM. 1982; 487-492.

87. Thomas YC, Woo RB, Shaowen S, Lam SS. SNP: An Interface for Secure Network Programming. USENIX Summer. 1994; (1):45-58.

88. Freier AO, Karlton P, Kocher PC. The SSL Protocol Version 3.0, Netscape Communications IETF RFC, 1996.

89. Gary FE, Zhi-Qiang L. Computers and networks in medical and healthcare systems, Computers in Biology and Medicine, 1995; 25(3):355-365.

90. Daemen J, Rijmen V. The Design of Rijndael AES - The Advanced Encryption Standard. Springer-Verlag New York. New Jersey. USA. 2002. 238p.

91. Short K. Method and Apparatus for Remote Digital Key Generation. Patente US WO/2003/081829. 2003.

92. Jung B, Kim D. Conference session key distribution method in an ID-based cryptographic system. Patente US 20050084114. 2005.

93. Li C, Huawei Technologies Co Ltd. A Method, System and Communication Device for Generating Session Cryptographic. Patente EP2120389. 2009.

94. Hiromi M, Eiichiro M, Masao T. Key generator device, encoding/decoding device, and key generation method. Patente US7406175B2. 2008.

95. Vanstone SA, Vadekar A, Lambert RJ, Gallant, Robert P, Brown DR. Menezes A. Patent Method Of Public Key Generation. Patente US7372961B2. 2008.

96. Kimmel GD, Domangue EL. Cryptographic key construct. Patente US 7739501. 2010.

97. Tilley T, Cole R, Becker P, Eklund P. A survey of formal concept analysis support for software engineering activities. In: Formal Concept Analysis. Ganter B, Stumme G, Wille R (org). Springer-Verlag: Berlin. 2005; 250-271.

98. Basili VR, Selby RW. Paradigms for experimentation and empirical studies in software engineering, Reliability Engineering & System Safety. 1991; 1(32):171-191.

99. Boehm BW. A spiral model of software development and enhancement. Computer. 1988; 21(5):61-72.

100. Paetsch F, Eberlein A, Maurer F. Requirements engineering and agile software development. In: Enabling Technologies: Infrastructure for Collaborative Enterprises, 2003 (WET ICE 2003). Proceedings of the Twelfth IEEE International Workshops on. 2003; 308-313.

101. Bakker AR. HIS, RIS, and PACS. Comput Med Imaging Graph. 1991; 15(3):157-60.

102. Lim DH, Choi SW, Park SC. Interface HIS/RIS and PACS using HL7 and Non-HL7 in two hospitals. CARS, International Congress Series. 2003. 1384p.

103. Willians CB, Muto R. Examination of the whole colon with the fibre-optic colonoscope. Brit Med J. 1972; 3(5821):278-281.

104. Eusebio EB. A practical aid in colonoscopy. Dis Colon Rectum. 1989; 32(11):996-997.

105. Pianykh OS. Digital Imaging and Communications in Medicine (DICOM): A practical introduction and survival guide. Boston (USA): Springer. 2008. 383p.

106. Back T, Hammel U, Schwefel HP. Evolutionary computation: comments on the history and current state. Evolutionary Computation. In: IEEE Transactions on. 1997; 1(1) 3-17.

107. Bergmann KP, Scheidler R, Jacob C. Cryptanalysis using genetic algorithms. Proceedings of the 10th annual conference on Genetic and evolutionary computation (GECCO '08). Maarten Keijzer (org). ACM. 2008; 1099-1100.

108. Xu C, Chen Y, Chiew K. An Approach to Image Spam Filtering Based on Base64 Encoding and N-Gram Feature Extraction. In: Tools with Artificial Intelligence (ICTAI), Proceedings of the 22nd IEEE International Conference on. 2010; 1(1):171-177.

109. Miano J. Compressed Image File Formats: Jpeg, Png, Gif, Xbm, Bmp. Addison-Wesley Professional. 1999. 264p.

110. Leff Avraham, Rayfield JT. Web-application development using the model/view/controller design pattern. In: Enterprise Distributed Object Computing Conference (EDOC'01). Proceedings of the Fifth IEEE International. IEEE. 2001; 118-127.

111. Deitel HM. Java: Como Programar. 6. Ed. São Paulo (SP), Brasil: Editora Pearson Prentice Hall, 2005. 1152p.

112. Jamae J, Johnson P. JBoss in Action: Configuring the JBoss Application Server. Manning Publications. 2009. 646p.

113. Wang D, Xu K. Red5 Flash server analysis and video call service implementation. In: Web Society (SWS). IEEE 2nd Symposium on. IEEE. 2010; 397-400.

114. Korth AB, Silberschatz HF. Sistema de Banco de Dados. 6ª ed. São Paulo (SP): Elsevier, 2012. 904p.

115. Tiwari S, Elrom E, Schulze C. Flex 4 Avançado. São Paulo (SP): Novatec. 2011. 576p.

116. Exadel Open Source Community. Exadel Flamingo Developer Guide. 2010. [Acesso em 3 jun 2011]. Disponível em: URL: http://download.exadel.org/flamingo/docs/pdf/Guide_reference.pdf.

117. Marrs T, Davis S. JBoss at Work: A Practical Guide. O'Reilly Media. 2005. 308p.

118. The Apache Software Foundation. Tomcat documentation - The Apache Jakarta Project. APACHE. 2000. [Acesso em 8 jun 2011]. Disponível em: URL: http://jakarta.apache.org/tomcat/tomcat-3.3-doc.

119. Institute of Electrical and Electronics Engineers, IEEE Standard for Information technology - Telecommunications and information exchange between systems Local and metropolitan area networks - Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. IEEE 802.11 Standard Specification, 2012 [Acesso em 3 abril 2013]. Disponível em: URL: http://standards.ieee.org/about/get/802/802.11.html.

120. Yeung R, Weinman L. Macromedia Flash MX 2004: hands-on training. Peachpit Press. 2004. 953p.

121. Valin, JM. Speex: a free codec for free speech. In: Australian National Linux Conference. New Zealand. 2006.

122. Fujinon Corporation. Operation Manual EVE Processor: VP-4400. 2006. [Acesso em 8 mai 2011]. Disponível em: URL: http://1800endoscope.com/pdf/4400System.pdf.

123. Lee HD, Costa LHD, Ferrero CA, Coy CSR, Fagundes JJ, Machado RB, et al. Protótipo de um sistema de gerenciamento de protocolos de câncer colorretal. Revista Brasileira de Coloproctologia. 2011; 31:1-7.

124. Wu FC, Lee HD, Niz MAK, A, Coy CSR, Góes JRN, Fagundes JJ. Estudo Comparativo da Resistência de Ruptura de Cólon Descendente por Meio de Ensaio Uniaxial Força de Ruptura à Tração e Energia Total de Ruptura: Trabalho Experimental em Ratos. Revista Acta Cirurgica Brasileira: São Paulo (SP). 2006; 21(2):97-100.

125. Fedel, GS, Medeiros CMB. Busca multimodal para apoio à pesquisa em biodiversidade [Dissertação]. Campinas (SP): Universidade Estadual de Campinas. In: IX Workshop de Teses e Dissertações em Banco de Dados. 2010.

126. Lima TFM, Carneiro TGS, Faria SD. Desenvolvimento de uma Plataforma Gráfica para a Descrição de Modelos de Sistemas Ambientais. Anais do X Simpósio Brasileiro de Geoinformática. 2008; 121-126.

127. Liu H, Motoda H. Computational Methods of Feature Selection. Chapman & Hall/CRC. 2008. 440p.

128. Wright RT, Brown RA. Technology: Design and Applications. 2ª ed. USA: Goodheart-Willcox Co. 2004. 125p.

129. Baniasadi E, Aydin M, Dincer I, Naterer GF. Computational Aerodynamic Study of Automotive Cooling Fan in Blocked Conditions. In: Engineering Applications of Computational Fluid Mechanics. 2013; 7(1):66-73.

130. Iskander MF (org). Computer Applications in Engineering Education. Wiley Periodicals Inc Online Library. 2013; 21(2).

131. Eysenbach G. Medicine 2.0: Social Networking, Collaboration, Participation, Apomediation, and Openness. J Med Internet Res. 2008; 10(3):1-22.

132. Murray E, Lo B, Pollack L, Donelan K, Catania J, Lee K, et al. The Impact of Health Information on the Internet on Health Care and the Physician-Patient Relationship: National U.S. Survey among 1.050 U.S. Physicians. J Med Internet Res. 2003; 5(3):1727-1734.

133. Eysenbach G. Consumer health informatics, British Medical Journal. 2000; 7251(320): 1713–1716.

134. Sanjay P. A., Sindhu M., Jesus Z., A Survey of the State of Cloud Computing in Healthcare, Networks and Communications Technologies, 2012; 1(2):12-19.

135. Reiner BI. Improving Healthcare Delivery Through Patient Informatics and Quality Centric Data. J Digit Imaging. Springer Publisher. 2011; 2011(24):177–178.

136. Organisation for Economic Co-Operation and Development. The Future of the Internet Economy. OCDE. 2008. [Acesso em 20 fev 2013]. Disponível em: URL: http://www.oecd.org/sti/ieconomy/40789235.pdf.

137. Perset K. The Economic and Social Role of Internet Intermediaries, In: Organisation For Economic Co-Operation and Development (OCDE). 2010. [Acesso em 20 fev 2013]. Disponível em: URL: http://www.oecd.org/internet/ieconomy/44949023.pdf.

138. Dick RS, Steen EB. The computer-based patient record: An essential technology for health care. Washington, DC: National Academy Press, 1991. 190p.

139. Maani R, Camorlinga S, Eskicioglu R. A Remote Real-time PACS-based Platform for Medical Imaging Telemedicine. Proceedings of SPIE 7264. 2009; 7264(1):1-12.

140. Morton, ME. Use and Acceptance of an Electronic Health Record: Factors Affecting Physician Attitudes. [Tese - Doutorado]. Philadelphia (CA): Drexel University; 2008.

141. Nisanbayev Y, Na H, Lim D, Ko F. Designing an electronic medical records system using design patterns. Proceedings of the 2nd International Conference on Interaction Sciences: Information Technology, Culture and Human (ICIS '09). ACM. 2009; 8(6):1410-1415.

142. Park SY, Chen Y. Adaptation as design: learning from an EMR deployment study. Proceedings of the 2012 ACM annual conference on Human Factors in Computing Systems (CHI '12). 2012; 1(1):2097-2106.

143. Masih A. Towards requirements engineering for a tumour removing robot: work-practice observation of surgical teams performing brain tumour surgery. Proceedings of the ACM 2011 conference on Computer supported cooperative work (CSCW '11), 2011; 677-680.

144. Lee JD, Srivastava M, Bonatti J. History and Current Status of Robotic Totally Endoscopic Coronary Artery Bypass. Circulation Journal - The Japanese Circulation Society, 2012; 9(76):2058-2065.

145. Dwivedi J, Mahgoub I, Robotic Surgery - A Review on Recent advances in Surgical Robotic Systems. Florida Conference on Recent Advances in Robotics. Boca Raton. 2012; 1(1):1-7.

146. Hounsfield G. N., Computerized transverse axial scanning (tomography): Part 1. Description of system. Brazilian Journal Radiology. 1973; 1973(46):1016-1022.

147. Piatek L, Hippe ZS. Synthesis of selected features of melanocytic skin lesion images. Proceedings of the 27th Conference on Image and Vision Computing New Zealand (IVCNZ '12). ACM. 2012; (65)1:238-243.

148. Hung K, Zhang YT. Implementation of a WAP-based telemedicine system for patient monitoring Information Technology in Biomedicine. IEEE Transactions on, 2003; 7(1): 101-107.

149. Maani R, Camorlinga S, Arnason N. Transforming medical imaging applications into collaborative PACS-based telemedical systems. Proceedings of SPIE 7967. Medical Imaging 2011. 2011;7967(1):1-10.

150. Espindola B, Tibes CMS, Lee HD, Machado RB, Maletzke AG, Wu FC. Analysis of biomechanical parameters extracted from anorectal manometry of fecally-continent and incontinent patients. Revista Latino-Americana de Enfermagem. 2012; 20(1):1117-1124.

151. Machado RB, Lee HD, Ayrizono MLS, Leal RF, Coy CSR, Fagundes JJ, et al. Prototype of a computer system for managing data and video colonoscopy exams. Journal of coloproctology. 2012; 32(1):50-59.

152. Wu FC, Lee HD, Niz MAK, Ayrizomo MLS, Coy CSR, Góes JRN, et al. Comparative study of descendent colon rupture resistance considering traction force of rupture and total energy of rupture in rats. Revista Acta Cirurgica Brasileira. 2006; 21(2):97-100.

153. Wu FC. Estudo dos efeitos de diferentes concentrações de oxigênio e da hiperoxigenação hiperbárica sobre anastomoses cólicas comprometidas ou não pela isquemia. Trabalho experimental em ratos [Tese - Doutorado]. Campinas (SP): Universidade Estadual de Campinas - Faculdade de Ciências Médicas. 2003.

154. Lee HD, Jung W, Silva AC, Costa LHD, Espindola B, Coy CSR, et al. Protótipo de um Sistema para Gerenciamento de Cirurgia Coloproctológica com Monitoramento de Qualidade. Revista Brasileira de Coloproctologia (Suplemento 1). 2011; 31(4):351-361.

155. Dwyer TF. Telepsychiatry: psychiatric consultation by interactive television. American Journal of Psychiatry. 1973; 130(8):865-869.

156. Lin D, Labeau F. An Algorithm That Predicts CSI to Allocate Bandwidth for HealthcareMonitoring in Hospital'sWaiting Rooms. International Journal of Telemedicine and Applications. 2012; 2(1):1-13.

157. Wess BP. Distributed Computer Networks In Support Of Complex Group Practices. Proceedings of the Computer Application in Medical Care. 1978; 469-477.

158. Ellington WW. A medical care application using the integrated services digital network. Proceedings of the Third Annual IEEE Symposium, 1990; 24-31.

159. Vagelis H. Challenges and communities of medical informatics research. ACM SIGMOD Records. 2013; 41(4):51-54.

160. Chopra S, Dexter S. Free software, economic 'realities', and information justice. SIGCAS Comput. 2009; 39(3):12-26.

161. Hawkins RE. The economics of open source software for a competitive firm. Netnomics. 2004; 6(2):103-117.

162. Munga N, Fogwill T, Williams Q. The adoption of open source software in business models: a Red Hat and IBM case study. Proceedings of the 2009 Annual Research Conference of the South African Institute of Computer Scientists and Information Technologists (SAICSIT '09). ACM. 2009; 112-121.

163. Cerqueira LS. A Economia do Software Livre à luz da Teoria do Aprisionamento Tecnológico. Revista de Administração e Contabilidade. 2011; 3(1):4-18.

164. Silveira S. Governo do Paraná economiza R$ 300 milhões com uso do software livre. 2009. [Acesso em 15 nov 2012]. Disponível em: URL: http://softwarelivre.org/portal/governos/governo-do-parana-economiza-r-300-milhoes-com-uso-do-software-livre.

165. Ghosh RA. Study on the: Economic impact of open source software on innovation and the competitiveness of the Information and Communication Technologies (ICT) sector in the EU. Final report. UNU-MERIT. Netherlands. 2006. [Acesso em 10 jan 2013]. Disponível em: URL: http://ec.europa.eu/enterprise/sectors/ict/files/2006-11-20-flossimpact_en.pdf.

166. Centro Nacional de Referencia de Aplicación de las TIC. Report on the International Status of Open Source Software. CENATIC: National Open Source Software Observatory. 2010. [Acesso em 19 ago 2012]. Disponível em: URL: http://www.inst-informatica.pt/servicos/informacao-e-documentacao/biblioteca-digital/arquitectura-e-desenvolvimento-de-aplicacoes/open-source/2010/report-on-the-international-status-open-source-software-2010/at_download/file.

167. Machado RB, Lee HD, Ayrizono MLS, Leal RF, Coy CSR, Fagundes JJ, et al. Sistema Computacional de Telemedicina para o Acompanhamento e a Interação Remota Durante a Realização de Exames de Videocolonoscopia Baseado em Soluções Não Proprietárias. In: 61 Congresso Brasileiro de Coloproctologia: Belo Horizonte (MG). Journal of Coloproctology. 2012; 32(1): 1-1.

168. Machado RB, Wu FC, Lee HD, Coy CSR, Fagundes JJ, Maciel JN, et al. Método para Geração de Chaves Baseado em Algoritmos Genéticos. Patente BR1020120331284. Instituto Nacional da Propriedade Industrial. 2012.

169. Machado RB, Wu FC, Lee HD, Coy CSR, Fagundes JJ, Maciel JN, et al. Método em Telemedicina para o Acompanhamento Remoto e em Tempo Real de Procedimentos Médicos. Patente BR1020120331250. Instituto Nacional da Propriedade Industrial. 2012.

170. Gupta PC. Data Communications and Computer Networks. PHI Learning. 2006. 828p.

171. Guimarães DA. Digital Transmission: A Simulation-Aided Introduction with VisSim/Comm. Spinger Verlag. 2010. 886p.

172. Joskowicz J, Ardao JCL. Combining the effects of frame rate, bit rate, display size and video content in a parametric video quality model. Proceedings of the 6th Latin America Networking Conference (LANC '11). ACM. 2011; 4-11.

173. Ou YF, Liu T, Zhao Z, Ma Z, Wang Y. Modeling the impact of frame rate on perceptual quality of vídeo. In: Image Processing (ICIP 2008). Proceedings of the 15th IEEE International Conference on. 2008; 12(15):689-692.

174. Harjanto F, Wang Z, Lu S, Feng DD. Evaluating the impact of frame rate on video based human action recognition. Proceedings of the 27th Conference on Image and Vision Computing New Zealand (IVCNZ '12). ACM. 2012; 376-381.

175. Apteker RT, Fisher JA, Kisimov VS, Neishlos H. Video acceptability and frame rate. MultiMedia IEEE. 1995; 2(3): 32-40.

176. Steinmetz R. Human perception of jitter and media synchronization. In: Selected Areas in Communications. Proceedings of the IEEE Journal on. 1996; 14(1):61-72.

177. Stocker A, Simoncelli E. Noise characteristics and prior expectations in human visual speed perception. Nature Neuroscience. 2006; 9(4):578-595.

178. Wang Y, Claypool M, Zuo Z. An empirical study of realvideo performance across the internet. Proceedings of the 1st ACM SIGCOMM Workshop on Internet Measurement (IMW '01). ACM. 2001; 295-309.

179. Wang Y, Claypool M. RealTracer-Tools for Measuring the Performance of RealVideo on the Internet. In: Multi-media Tools and Applications. Springer Science. 2005; 27(1):411-430.

180. McCarthy JD, Sasse MA, Miras D. Sharp or smooth?: comparing the effects of quantization vs. frame rate for streamed video. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '04). ACM. 2004. 535-542.

181. Nguyen TP, Zakhor A. Distributed Video Streaming Over Internet. Proceedings of the ACM/SPIE Conf. on Multimedia Computing and Networking. 2002; 186-195.

182. Goel A, Krasic C, Walpole J. Low-latency adaptive streaming over tcp. ACM Trans Multimedia Comput Commun Appl. 2008; 4(3):20:1-20:20.

183. Brosh E, Baset SA, Misra V, Rubenstein D, Schulzrinne H. The delay-friendliness of TCP for real-time traffic. IEEE/ACM Trans Netw. 2010; 18(5): 1478-1491.

184. Bhamidipati VD, Kilari S. Effect of Delay/ Delay Variable on QoE in Video Streaming [Dissertation]. Sweden: School of Computing Blekinge Institute of Technology. 2010.

185. Calyam CGL. Characterizing voice and video traffic behavior over the Internet. In: International Symposium on Computer and Information Sciences (ISCIS). 2005.

186. Mikhail M, Palumbo G, Mohammad J, El-Helaly M, Amer A. An Online System for Synchronized Processing of Video and Audio Signals (CCECE 2006). 2006; 2065-2068.

187. Cuomo F, Cianfrani A, Polverini M, Mangione D. Network pruning for energy saving in the Internet. Computer Networks. 2012; 56(10):2355-2367.

188. Kunz T. The influence of different workload descriptions on a heuristic load balancing scheme. Software Engineering, IEEE Transactions on. 1991; 17(7): 725-730.

189. Perkins D, Hughes H, Owen CB. Factors affecting the performance of ad hoc networks. In: Communications 2002 (ICC 2002). Proceedings of the IEEE International Conference on. 2002; 4(1):2048-2052.

190. Borland J. Net video explosion triggers traffic jam worries. 2006 [Acesso em 10 mai 2013]. Disponível em: URL: http://news.com.com/2100-1025_3-6042300.html.

191. Instituto Brasileiro de Opinião Pública e Estatística. Pesquisa sobre uso da internet no Brasil. IBOPE. 2013 [Acesso em 10 mai 2013]. Disponível em: URL:http:// www.ibope.com.br/pt-br/noticias/Paginas/Numero-de-usuarios-ativos-na-internet-cresce-4.aspx.

192. Taher TM, Al-Banna AZ, Ucci DR, LoCicero JL. Characterization of an Unintentional Wi-Fi Interference Device - the Residential Microwave Oven. Military Communications Conference (MILCOM 2006). IEEE. 2006; 1856-1862.

193. Uro T. The quest for a new video codec in Flash 8. 2005. [Acesso em 03 mai 2013]. Disponível em: URL: http://www.kaourantin.net/2005/08/quest-for-new-video-codec-in-flash-8.html.

194. Gill P, Arlitt M, Li Z, Mahanti A, Youtube traffic characterization: a view from the edge. Proceedings of the 7th ACM SIGCOMM conference on Internet measurement (IMC '07). ACM, 2007; 15-28.

195. Raghavendra R, Belding EM. Characterizing high-bandwidth real-time video traffic in residential broadband networks. In: Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks (WiOpt 2010). Proceedings of the 8th International Symposium on. 2010; 597-602.

196. Merwe JVD, Sen S, Kalmanek C. Streaming Video Traffic: Characterization and Network Impact. Proceedings of the International Web Content Caching and Distribution Workshop. 2002.

197. Kihl M, Odling P, Lagerstedt C, Aurelius A. Traffic analysis and characterization of Internet user behavior. In: Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT). Proceedings of the 2010 International Congress on. 2010; 224-231.

198. Associação Brasileira das Empresas de Tecnologia da Informação e Comunicação. Índice Brasscom de Convergência Digital. São Paulo: Brasscom. 6ª ed. 2012. [Acesso em 10 jan 2013]. Disponível em: URL: http://www.brasscom.org.br.

12. ANEXOS

12.1. ANEXO I: DECLARAÇÃO DE DISPONIBILIZAÇÃO DE EXAME DE COLONOSCOPIA PARA FINALIDADE DE PESQUISA ACADÊMICA

DECLARAÇAO

DISPONIBILIZAÇÃO DE EXAME DE COLONOSCOPIA PARA FINALIDADE DE PESQUISA ACADÊMICA

MARIA ELENA BOBSIN MACHADO, brasileira, solteira, servidora pública federal, com endereço profissional na Avenida Pedro Basso, 920, bairro Alto São Francisco, nesta cidade, titular de cédula de identidade RG nº. 7042062931 SSP/RS, inscrita no CPF/MF sob nº. 673.868.730-34, residente e domiciliada na Rua Puma, nº. 70, Conjunto A, Foz do Iguaçu-PR, **D E C L A R O** para todos os fins, que disponibilizo gratuitamente o vídeo relativo a procedimento médico de Videocolonoscopia que realizou, na data de 21/10/2008, em Clínica Privada, na cidade de Foz do Iguaçu, para que o Pós-Graduando da Faculdade de Ciências Médicas da Universidade Estadual de Campinas (FCM/UNICAMP), Renato Bobsin Machado, assim como para o seu Orientador, Wu Feng Chung e a FCM/UNICAMP, utilizem esse vídeo para a finalidade de avaliação experimental de desempenho de sua Tese de Doutoramento, a qual consiste no delineamento de um método computacional para o acompanhamento remoto, em tempo real, de exames complementares de videocolonoscopia.

Vale ressaltar que:

1. Estou ciente e esclarecida da RESOLUÇÃO Nº 196 DE 10 DE OUTUBRO DE 1996/CONSELHO NACIONAL DE SAÚDE-CNS;
2. Estou ciente e esclarecida em relação ao método do trabalho de Tese de doutoramento acima citada;
3. Estou ciente e esclarecida quanto aos itens pertencentes ao TERMO DE CONSENTIMENTO LIVRE E ESCLARECIDO, além dos riscos e benefícios.

Desse modo, após ciência e esclarecida frente aos itens supracitados, eu, MARIA ELENA BOBSIN MACHADO, estou de acordo com a disponibilização do meu exame de endoscopia digestiva baixa (colonoscopia).

2º TABELIONATO FOZ DO IGUAÇU

Maria Elena Bobsin Machado

SELO FUNARPEN

2º TABELIONATO DE NOTAS
Av. Jorge Schimmelpfeng, 38 - Fone/Fax: (45) 3038-2845 - Cep 85851-110
Foz do Iguaçu - Paraná - E-mail: cartoriopinheirofoz@ucl.com.br
Tabelião - Gustavo Sebastião Pinheiro

Reconheço como autêntica a firma de: MARIA ELENA BOBSIN MACHADO.....
Em test° da verdade.
Foz do Iguaçu-PR, 01 de abril de 2013
00046780(001-000690360)

2º TABELIONATO DE NOTAS
01 ABR. 2013
CARTÓRIO PINHEIRO
FOZ DO IGUAÇU - PARANÁ

Lucy M. Bruczenitski