UNIVERSIDADE ESTADUAL DE CAMPINAS

FACULDADE DE ENGENHARIA ELÉTRICA E DE COMPUTAÇÃO

DEPARTAMENTO DE COMUNICAÇÕES

Tese de Doutorado

Um Sistema Biométrico de Identificação Pessoal via Internet com ênfase em Assinaturas Estáticas

Miguel Gustavo Lizárraga Espinosa

Orientador: Prof. Dr. Lee Luan Ling

Banca Examinadora:

Profa. Dra. Sherry Chou Chen (INPE - S. J. dos Campos)

Prof. Dr. Manoel Raimundo de Sena Junior (UFPE/Recife)

Prof. Dr. Yuzo Iano (FEEC/UNICAMP)

Prof. Dr. João B. T. Yabu-uti (FEEC/UNICAMP)

Prof. Dr. Renato Baldini Filho (FEEC/UNICAMP)

Tese apresentada à Faculdade de Engenharia Elétrica e de Computação como parte dos requisitos exigidos para a obtenção do título de Doutor em Engenharia Elétrica

Campinas – SP – Brasil

Agosto de 2000

FICHA CATALOGRÁFICA ELABORADA PELA
BIBLIOTECA DA ÁREA DE ENGENHARIA - BAE - UNICAMP

L768s

Lizárraga Espinosa, Miguel Gustavo
Um sistema biométrico de identificação pessoal via internet com ênfase em assinaturas estáticas / Miguel Gustavo Lizárraga Espinosa.--Campinas, SP: [s.n.], 2000.

Orientador: Lee Luan Ling.
Tese (doutorado) - Universidade Estadual de Campinas, Faculdade de Engenharia Elétrica e de Computação.

1. Reconhecimento de padrões. 2. Biometria. 3. Internet (Redes de computação). I. Lee, Luan Ling. II. Universidade Estadual de Campinas. Faculdade de Engenharia Elétrica e de Computação. III. Título.

RESUMO

Neste trabalho foi implementada uma plataforma que permite o cadastramento, consulta e autenticação automática de identidade via rede internet. A identificação pessoal pode ser feita através de diferentes métodos biométricos. Cada um desses métodos biométricos podem ser adicionados à plataforma através de módulos de identificação. Um módulo de identificação consiste em programas CGI que realizam tanto a tarefa de autenticação pessoal quanto a comunicação entre os dados enviados por um usuário através de um *browser* e um servidor *Web*.

No presente trabalho foi também implementado o módulo de identificação pessoal por imagens de assinaturas. Esse módulo é constituído por um método de verificação automático de assinaturas que se caracteriza por ser um sistema multi-especialista de dois estágios, onde o primeiro estágio trata das falsificações aleatórias e simples, e o segundo estágio de falsificações habilidosas.

Esse método de verificação se serve tanto de características globais quanto locais para fazer a descrição da assinatura. As características utilizadas no primeiro estágio do sistema se baseiam na distribuição espacial dos pixels que compõe a assinatura. No segundo estágio, as características escolhidas se servem de técnicas de morfologia matemática para descreverem as inclinações e contornos dos traços que compõe a assinatura.

Como parâmetros de desempenho do método de verificação automático, obtivemos os valores de 0,47 % de taxa de erro de falsa rejeição e 2,35 % de taxa de erro de falsa aceitação frente a falsificações aleatórias. No caso de falsificações habilidosas, as taxas de erros foram de 12,75 % e 19,22 % para falsa rejeição e falsa aceitação, respectivamente.

ABSTRACT

In this work, it was implemented a platform for identity's enrollment, consulting and automatic authentication through Internet. The personal identification could be made using different biometric methods. Each one of those methods could be add into the platform like as an identity module. An identity module is a group of CGI programs that authenticates an identity and deals with the communication between a user using a browser and a web server.

Also, it was implemented a personal identity module using signature's images. This module is based on an automatic verification method that is characterized by being a multi-expert system that works in two stages. In the first stage, the system deals with simple and random forgeries and, in the second one, with skilled forgeries.

The verification method uses global and local features for describing a signature. The features used in the first stage are based on the pixels' spatial distribution that compose the signature. In the second stage, the chosen features use mathematic morphology techniques for describing the strokes' inclinations and contours of a signature.

As a measure of performance, it was obtained 0.47 % of false rejection error rate and 2.35 % of false acceptance error rate working with random forgeries. Working with skilled forgeries, error rates were 12.75 % and 19.22 % for false rejection and false acceptance, respectively.

Para meus irmãos,
David e *Alfredo*,
pelo seu carinho, compreensão
para comigo e,
pela persistência e
força de vontade com que
enfrentam o dia a dia.

O que for a profundeza do teu ser, assim será teu desejo.
O que for o teu desejo, assim será tua vontade.
O que for a tua vontade, assim serão teus atos.
O que forem teus atos, assim será teu destino.

Brihadaranyaka Upanishad IV, 4.5

AGRADECIMENTOS

- A Deus, pela inspiração.
- A meus pais, Gustavo e Carmen, pelo seu amor e dedicação.
- Ao Prof. Lee Luan Ling, pela oportunidade da realização deste trabalho.
- Ao colega Hugo Cavalcanti, pelo incentivo e companheirismo.
- Aos colegas de LRPRC, Nata, Evandro, JoseRai, AndreFer, Tarciano, Fcalves, Heller, Lucila, Zimmer, pela valiosa contribuição nos mais diversos momentos da elaboração deste trabalho.
- A Magali Rondón, pelo carinho que vem me oferecendo, sem o qual não teria tido a paz de espírito para conclusão deste trabalho
- Aos amigos, Carlos, Rocio e Pedro, por todos os bons momentos.
- Aos meus colegas, amigos e conterrâneos que me ajudaram ao longo da minha vida acadêmica.

ÍNDICE

CAPÍTULO 5

CAPÍTULO 6

CAPÍTULO 7

LISTA DE TABELAS

LISTA DE FIGURAS

CAPÍTULO 1

INTRODUÇÃO

Este capítulo apresenta a motivação para o estudo e implementação de sistemas de identificação pessoal baseados em características biométricas. Introduz o conceito de verificação automática de assinaturas manuscritas dentro de um contexto de autenticação de identidade via rede internet. Relaciona as áreas de concentração do conhecimento associadas. Apresenta os objetivos da dissertação e, finalmente, introduz a estrutura dos capítulos.

1.1 Identificação Pessoal

Com o aumento da complexidade e sofisticação da sociedade, as pessoas passam cada vez mais por situações em que são obrigadas a ter que provar sua identidade. Esse fato é tão comum, que estamos acostumados a fazê-lo de forma corriqueira em nosso cotidiano. Assim sendo, é perfeitamente aceitável utilizar cartões, rubricas ou documentos para autenticar nossa identidade. Podemos citar como exemplos, os cartões magnéticos para retirar dinheiro em bancos, assinaturas para autenticar cheques bancários ou ainda a apresentação de documentos com nossa foto como passaportes e carteiras de identidade.

O propósito de tais procedimentos é oferecer uma evidência adicional para autenticar o pedido de identidade, ou seja, auxiliar na confirmação de que nós realmente somos quem dizemos ser. Fica visto pelos exemplos que anteriormente apresentamos, que isso pode ser feito de várias formas diferentes.

Existem basicamente quatro maneiras de autenticar uma pessoa. A primeira maneira é a de possuir fisicamente um dispositivo que em si seja a autenticação, como por exemplo, um cartão válido ou um crachá que permite o acesso a algum lugar. A segunda maneira é a de ter acesso a chaves baseadas no seu conhecimento, como por exemplo senhas e contra-senhas. A terceira opção é a validação de identidade através de um padrão ou atividade específica do indivíduo, como por exemplo sua assinatura ou fala. A quarta maneira, é a análise das possíveis características físicas que a pessoa possui, dentre as quais podemos mencionar as impressões digitais, geometria da mão, íris, etc.. Cada uma dessas abordagens de validação de identidade estão sujeitas a um maior ou menor sucesso, dependendo do tipo de aplicação e situação em que desejamos empregá-las.

Na maioria das vezes, a maneira de autenticar a identidade de um indivíduo recai sobre as duas primeiras categorias. Ou seja, é muito comum que hoje em dia precisemos memorizar mais de dez números de identificação incluindo senha do cartão do banco ou *login* do computador, número de RG, de passaporte, de CPF e vários outros. Ou ainda, termos que carregar conosco vários documentos de identificação, como por exemplo, carteira de identidade, carimbos, selos, cartões e chaves. Porém, nenhum desses métodos são 100% confiáveis, visto que podem ser esquecidos, roubados, emprestados, perdidos, copiados ou falsificados.

Por essas razões, tem aumentado o interesse em desenvolver métodos de verificação de identidade pessoal que levem em consideração estratégias que se fundamentem na terceira e quarta categorias. Essas técnicas se baseiam em medidas biométricas, onde "medida biométrica" é definida pela *Association for Biometrics* [1] como: "A medida de atributos/características físicas ou de comportamento de uma pessoa com o objetivo de distinguí-la entre as demais".

As medidas biométricas podem ser divididas em dois grupos. O primeiro, a biometria fisiológica, que engloba características tais como o padrão da íris, as impressões digitais, a forma do contorno da mão e face. E o segundo, a biometria de comportamento, que se preocupa com a extração de características mais sutis, como o tipo de escrita do indivíduo, a maneira como assina seu nome, a forma como se pronuncia determinadas palavras, etc..

Embora antigamente muitos dispositivos tivessem sido apresentados como capazes de captar características biométricas com boa precisão, eles raramente satisfaziam as expectativas. Mais recentemente, a evolução da pesquisa na área da biometria em conjunto com o desenvolvimento da tecnologia, tanto na aquisição de informação como no aumento do poder de

processamento dos computadores, ofereceram um novo impulso para a crescente utilização da biometria como método de autenticação.

A escolha de um método de autenticação de identidade através de características biométricas, seja pela abordagem fisiológica ou de comportamento, pode gerar amplos debates. Nesse contexto, a abordagem fisiológica está bastante aberta a discussões, por outro lado, a abordagem de comportamento possui um consenso geral, embora outras alternativas possam ser consideradas, a utilização de assinaturas manuscritas tem vantagens significativas [2]:

a) A assinatura é o método mais natural e mais amplamente utilizado para confirmar nossa identidade.

b) Medidas das características de assinaturas não são invasivas (quando comparadas com outras técnicas, como por exemplo, as medidas feitas sobre a íris) e não tem conotações negativas ou de higiene indesejável (se comparadas com medidas feitas sobre impressões digitais).

c) A utilização de técnicas de verificação automática de assinaturas agilizam processos e minimizam erros em operações que solicitem a autenticação de indivíduos através de assinaturas.

Os sistemas biométricos possuem três componentes principais. Um é o mecanismo de automação que capta o sinal digital ou analógico da característica de um indivíduo. A segunda componente executa a extração e processamento da característica assim como sua classificação. A terceira componente é a interface com os sistemas de aplicação.

Dentro desse contexto, neste trabalho propomos e implementamos uma aplicação que se baseia no modelo computacional cliente/servidor. Essa aplicação implementa a plataforma de um sistema que utiliza características biométricas para realizar a tarefa de identificação pessoal através da rede internet. Essa plataforma permite que diferentes métodos biométricos possam ser utilizados para identificação pessoal através do acoplamento de diversos módulos, sejam eles referentes a autenticação de identidade mediante imagens de íris, impressões digitais, assinaturas, etc..

1.2 Verificação de Assinaturas

Na década passada, o problema de verificação automática de assinaturas foi solucionado através de sistemas de verificação de assinaturas dinâmicas (SVAD). Esses sistemas se caracterizam pelo uso de informações dinâmicas do processo de escrita, tais como velocidade e aceleração. A taxa de acerto desses sistemas é bastante elevada, em torno de 99%, mesmo quando as falsificações são feitas por especialistas [3]. O bom desempenho desses sistemas é obtido por que os falsificadores normalmente procuram imitar somente a forma da assinatura original e não conseguem reproduzir os traços da assinatura nos mesmos intervalos de tempo efetuado pelo indivíduo genuíno. Desta forma, esses sistemas se valem da falta de consistência dos dados temporais nas assinaturas falsificadas, para obter uma melhor discriminação entre a classe de assinaturas verdadeiras e a classe de assinaturas falsas.

O principal limitante desse tipo de sistema é que a assinatura sempre deve ser escrita sobre um equipamento que permite a aquisição das informações dinâmicas. De fato, escrever sobre esse tipo de equipamento muitas vezes não deixa que o escritor assine de maneira natural, implicando em mudanças do estilo de sua assinatura [4].

Por outro lado, os sistemas de verificação de assinaturas estáticas (SVAE), se caracterizam por utilizar apenas a imagem da assinatura para extrair as informações que alimentam o sistema. As taxas de acerto dos SVAE são geralmente inferiores às taxas de acerto dos SVAD. Isso se deve ao fato de que as imagens de assinaturas podem ser facilmente copiadas e a informação dinâmica que poderia ser extraída dessas imagens torna-se altamente degradada na amostra estática [5]. Dessa forma, um bom falsificador poderia criar uma copia suficientemente fiel da assinatura original, levando o sistema a classificar erroneamente a assinatura falsificada como sendo verdadeira.

A principal vantagem dos SVAE é preservar ao máximo a naturalidade do processo de escrita, pois no ato de assinar não existe nenhum tipo de dispositivo que venha interferir diretamente na escrita da assinatura.

Neste trabalho são propostas técnicas para verificação de assinaturas estáticas, com alta taxa de acerto para falsificações feitas sem o conhecimento da assinatura original. Além disso, é verificado que as técnicas propostas no caso anterior apresentam um bom desempenho na detecção de falsificações que são feitas conhecendo-se previamente a assinatura original.

1.3 Áreas de Concentração

Este trabalho aborda basicamente três áreas de conhecimento. A primeira área é a de processamento de imagens digitais, visto a necessidade de implementar técnicas para melhoramento das imagens sejam elas de assinaturas, impressões digitais, íris, etc.. A segunda, reconhecimento de padrões, a qual lida com a extração e classificação de informações. E por último, a área de redes de computadores, onde a aplicação da plataforma do sistema de identificação pessoal foi implementada.

1.3.1 Processamento de Imagens Digitais

Numa abordagem simplificada, o termo imagem se refere a função de intensidade bidimensional, denotada por $I(x, y)$, onde o valor ou amplitude de I nas coordenadas espaciais (x, y) fornece a intensidade (brilho) da imagem naquele ponto. Como a luz é uma forma de energia, teoricamente, $I(x, y)$ pode variar de 0 até infinito, isto é:

$$0 < I(x, y) < \infty \tag{1.1}$$

Para que essa função possa ser processada convenientemente no computador, é necessário transformá-la para a forma digital, isto é, fazer uma aproximação discreta da função continua $I(x, y)$. Mais especificamente, uma imagem digital é uma imagem que foi aproximada de duas formas:

- **Digitalização espacial**: Também referida como amostragem, envolve a representação da noção contínua de distribuição da função de imagem como um conjunto finito de amostras específicas em pontos discretos dentro de um sistema bidimensional de referência.

- **Digitalização em amplitude**: Cada ponto no conjunto precisa codificar a intensidade de brilho local da imagem. Isto é feito através da associação de cada intensidade a um número fixo dentro de uma escala discreta e finita de níveis.

Uma vez digitalizada, a imagem pode ser vista como uma matriz de *pixels*, onde cada *pixel* representa um elemento da matriz e que por sua vez possui um valor discreto que representa a intensidade de brilho da função original $I(x, y)$.

O interesse em métodos de processamento de imagens digitais advém de dois principais domínios de aplicação: melhoramento de informação pictorial para interpretação humana e processamento de dados de cenas para percepção de máquinas. No primeiro caso, procedimentos para o melhoramento e restauração de imagens são utilizados no processamento de imagens degradadas. No segundo caso, o interesse está focalizado em procedimentos para extrair informações de imagens de forma conveniente que permitam ser processadas pelo computador.

1.3.2 Reconhecimento de Padrões

O termo reconhecimento de padrões aplica-se aos métodos para classificação de elementos num conjunto de dados, com base em suas características. Entende-se por elemento, o objeto que é observado e cujas propriedades medidas constituem suas características ou padrões de medida.

Historicamente, tem-se utilizado três tipos de técnicas para resolver os problemas gerais de reconhecimento de padrões:

- **Reconhecimento Estatístico**: As características são da forma de n-tuplas ou vetores, sendo utilizadas regras de decisão, teoria de probabilidades, funções discriminantes e outros procedimentos estatísticos. Esse é o tipo de reconhecimento mais tradicional.

- **Reconhecimento Estrutural/Sintático**: As características são da forma de sentenças de uma linguagem reconhecida por uma gramática de estrutura de frases. Reconhecimento sintático é também conhecido como reconhecimento estrutural de padrões, onde as características estruturais dos elementos, em termos de suas partes constituintes, propriedades e relacionamentos, são representadas sintaticamente.

- **Reconhecimento via Redes Neurais**: Alguns autores consideram o reconhecimento via redes neurais como um tipo particular de reconhecimento estatístico, uma vez que as características também são da forma de n-tuplas ou vetores e existe uma equivalência entre

certos modelos de redes neurais com técnicas estatísticas fundamentais. Por possuírem propriedades peculiares, tais como a capacidade de generalização, abstração, aprendizagem a partir de exemplos, o reconhecimento por redes neurais acaba sendo tratado como uma área distinta.

É possível estabelecer uma fronteira entre as áreas de processamento de imagens e de reconhecimento de padrões. Pode-se dizer que a primeira lida principalmente com operações sobre imagens cujo objetivo é melhorar sua qualidade de alguma forma, ou enfatizar características de importância particular, já a segunda, trata da identificação, verificação ou interpretação de imagens através da extração e classificação de informações (em nível de abstração mais alto) a respeito do que a imagem denota.

1.3.2 Redes de Computadores

O objetivo principal de uma rede de computadores é compartilhar recursos e fornecer um meio para estabelecer a comunicação entre os computadores que fazem parte da rede. Um recurso da rede pode ser tanto um dispositivo como um programa que esteja disponível para utilização dos usuários.

O computador no qual os recursos da rede estão vinculados é chamado de servidor. Os outros computadores que acessam esses recursos através da rede são chamados de clientes.

No modelo computacional cliente/servidor, uma aplicação é dividida em duas partes:

- Um cliente *front-end*, que tanto apresenta como capta informações do usuário.

- Um servidor *back-end*, que armazena, recupera e manipula dados, e que geralmente trata da maior parte das tarefas computacionais do cliente.

No contexto em que está inserida essa área de conhecimento dentro do nosso trabalho, propomos uma aplicação que se serve do modelo computacional cliente/servidor para implementar um sistema onde usuários localizados nos mais diferentes locais possam acessar o serviço de autenticação de identidade via internet. Nesse caso o cliente, é um navegador de

internet (*browser*) e o servidor é um gerenciador de páginas html (servidor *Web*) com acesso a programas de *gateway*. Esses programas de *gateway*, por sua vez, são os que realizam a tarefa automática de autenticação de identidade dos indivíduos.

1.4 Objetivos do Trabalho

O primeiro objetivo deste trabalho é apresentar técnicas e métodos que utilizam medidas biométricas para realizar a tarefa automática de autenticação pessoal. Em nosso caso, essas técnicas e métodos de medidas biométricas serão feitas a partir de imagens de assinaturas estáticas. A tarefa de autenticação pessoal, é feita através da verificação automática de assinaturas. Isto é, temos por objetivo, dizer que uma pessoa é realmente quem diz ser, se o sistema aceitar como verdadeira uma assinatura que a pessoa fornecer como sendo genuína, caso contrário, a autenticação desse indivíduo será falha.

O segundo objetivo é o de disponibilizar uma plataforma que permite que diferentes métodos biométricos possam ser utilizados para identificação pessoal através do acoplamento de diversos módulos. Esses módulos se referem a autenticação de identidade de indivíduos mediante algumas medidas biométricas que vem sendo desenvolvidas no Laboratório de Reconhecimento de Padrões e Redes de Comunicações (LRPRC) da Faculdade de Engenharia Elétrica e de Computação da UNICAMP, como por exemplo, imagens de impressões digitais, assinaturas estáticas e rostos.

A principal característica dessa plataforma é a de utilizar o modelo computacional cliente/servidor. Assim sendo, os módulos de identificação que fazem parte da plataforma possuem essa mesma característica. Dessa forma é possível o cadastramento, consulta e autenticação de identidade sejam feitas se utilizando uma rede de computadores. Em nosso caso específico, as tarefas anteriormente mencionadas podem ser realizadas de forma local dentro de uma intranet e de uma forma mais ampla através da internet.

No decorrer deste trabalho apresentaremos os vários componentes que formam o protótipo da plataforma para identificação pessoal via internet, assim como o estudo e implementação de técnicas para verificação automática de assinaturas estáticas.

1.5 Estrutura da dissertação

Com o intuito de fornecer uma apresentação estruturada do assunto, favorecendo uma cadência lógica das idéias, esta tese é constituída de oito capítulos:

1. Introdução
2. Biometria
3. Reconhecimento de Padrões
4. Estado da Arte de Verificação de Assinaturas
5. Verificação de Assinaturas
6. Redes de Computadores
7. Um Sistema de Identificação Pessoal
8. Conclusões

No capítulo 2 é feita uma apresentação geral sobre o que é biometria e os principais métodos biométricos de identificação. No capítulo 3 fazemos uma introdução a reconhecimento de padrões e particularizamos essa área do conhecimento para a verificação de assinaturas, o que na prática significa apresentar um modelo de reconhecimento de padrões para apenas duas classes. No capítulo 4 discursamos sobre o processo de escrita das assinaturas, discutindo sobre suas características e tipos de falsificações. Ainda nesse capítulo fazemos uma revisão da literatura sobre o tema de verificação de assinaturas. O método de verificação de assinaturas proposto é descrito no capítulo 5, no qual detalhamos as diferentes características que são extraídas das imagens das assinaturas, assim como as etapas de pré-processamento e classificação que fazem parte do método proposto. No capítulo 6, apresentamos uma visão geral sobre rede de computadores fazendo uma descrição de seus principais componentes, protocolos e mecanismos que permitem a implementação de uma aplicação para redes de computadores. O capítulo 7 descreve como foi implementada a plataforma do sistema biométrico de identificação pessoal via internet e mostra a interface homem/máquina que foi construída para acesso a esse sistema. Finalmente, um sumário geral da tese descrevendo o método de elaboração deste trabalho, os objetivos iniciais que foram alcançados, as contribuições e as perspectivas para novos trabalhos estão contidos no capítulo 8.

CAPÍTULO 2

BIOMETRIA

Neste capítulo apresentamos os conceitos básicos que regem a biometria e sistemas biométricos de identificação pessoal. Apresentamos também alguns métodos biométricos tais como impressões digitais, padrões dos olhos, geometria da mão, verificação de voz, dinâmica da digitação, padrões de face e assinaturas detalhando as características em que se baseiam esses métodos para realizar a tarefa de autenticação.

2.1 O que é biometria ?

A biometria é o ramo da ciência que estuda a mensuração dos seres vivos [6]. Tecnologias biométricas são definidas como "métodos automáticos de verificação ou identificação de identidade de uma pessoa viva baseados em características fisiológicas ou de comportamento" [7]. Vamos examinar algumas das palavras chaves encontradas nessa definição:

Métodos Automáticos: Dentro do contexto de um sistema automatizado, os componentes que servem de fundamento para implementação de um sistema biométrico são três: O primeiro componente é o mecanismo de captura de um sinal digital ou analógico de características de uma pessoa; o segundo componente é aquele que trata do processamento e classificação dos sinais; finalmente o terceiro componente é a interface homem/máquina que permite ao usuário fazer a entrada de dados no sistema para que se realize a tarefa de verificação/identificação automática. O termo "automática", demanda que uma vez feita a captura da imagem, os processos que envolvem

o processamento, classificação e finalmente o resultado da identificação, sejam feitos sem intervenção humana.

Verificação versus Identificação: Um sistema automático baseado em características biométricas pode ser classificado com relação à maneira como seus dados de entrada são classificados junto à base de dados. Nesse caso, duas categorias podem ser definidas: sistemas um para um e sistemas um para muitos.

Um sistema um para um compara a informação biométrica apresentada por um indivíduo com a informação biométrica armazenada em uma base de dados correspondente àquele indivíduo. Nesse caso, o sistema decide se existe um casamento (*matching*) entre a informação de entrada e a armazenada na base de dados. Esse tipo de sistema é chamado também de sistema de verificação.

Em contrapartida, um sistema um para muitos compara a informação biométrica apresentada por um indivíduo com toda a informação biométrica armazenada na base de dados, isto é, informações de todos os indivíduos (ou determinado conjunto deles), e declara se existe um casamento com algum deles ou não. Esse tipo de sistema é também chamado de sistema de identificação.

Pessoa viva: Inicialmente, a interpretação desse termo parece bastante óbvia, porém é importante no contexto da definição de tecnologias biométricas. Pode ocorrer, por exemplo, que diante de um sistema de verificação de locutor, um indivíduo tente se passar por outro através da reprodução do som da voz de uma pessoa que tenha sido previamente gravada. Uma da soluções para esse tipo de fraude é que os dispositivos de captura que fazem parte dos sistemas biométricos incluam meios para determinar se existe uma característica "viva". Um exemplo disso já pode ser encontrado em alguns sistemas de reconhecimento de face. Nesse caso, o sensor que faz a captura da imagem não é uma câmara de vídeo comum e sim um dispositivo que além de capturar a imagem da face como um matriz de valores de intensidade luz, capta também a distribuição de temperatura sobre as diferentes regiões do rosto. Dessa forma, ao se apresentar uma foto comum como entrada para o sistema, mesmo que as características referentes a intensidade de luz casem com as da base de dados, aquelas referentes à distribuição de temperatura com certeza serão diferentes e portanto o resultado do pedido de autenticação de identidade será falho.

Características Fisiológicas e de Comportamento: O ponto final da definição sobre tecnologias biométricas é a diferença entre características fisiológicas e características de comportamento. Uma característica fisiológica é uma propriedade física relativamente estável tal como as impressões digitais, geometria da mão, padrão da íris, padrão dos vasos sangüíneos do fundo dos olhos, entre outras. Esse tipo de característica é basicamente imutável. Por outro lado, uma característica de comportamento é mais um reflexo de atitudes psicológicas do indivíduo. A assinatura é a característica de comportamento mais utilizado para autenticação. Outros comportamentos que podem ser utilizados são a maneira como se digita nos teclados e a maneira de falar.

As características de comportamento tendem a variar com o tempo, por esse motivo, muitos sistemas biométricos permitem que sejam feitas atualizações de seus dados biométricos de referência à medida que esses vão sendo utilizados [8]. Em geral, ao executar a tarefa de atualização de dados, o sistema terá se tornado mais eficiente em autenticar o indivíduo.

As diferenças entre métodos de comportamento e fisiológicos são importantes por vários motivos. Primeiro, o grau de variação intra-pessoal numa característica física é menor do que em uma característica de comportamento. Exemplificando, isto significa que, com exceção de algum ferimento, suas impressões digitais são as mesmas ao longo da sua vida. Uma assinatura, por outro lado, é influenciada tanto por fatores fisicamente controláveis como por fatores emocionais. Assim, sistemas baseados em comportamento tem um grande trabalho em ajustar as variações intra-pessoais. Por esse motivo, é mais fácil construir um sistema que, por exemplo, guie o usuário a colocar a palma de sua mão sempre em determinada posição, do que implementar um algoritmo que traduza o estado emocional de uma pessoa. Tanto as técnicas de comportamento quanto as fisiológicas provêem níveis significativamente maiores de identificação e segurança do que aquelas baseadas em senhas e cartões de forma isolada.

2.2 Métodos Biométricos de Identificação

Em geral, a construção de sistemas de identificação pessoal se edifica sobre três pilares:

1. Possuir um dispositivo que seja em si a autenticação (um cartão),
2. Chaves baseadas no seu conhecimento (senhas),
3. Características biométricas (uma característica biométrica).

A partir desses três pilares é possível criar diferentes esquemas de identificação. Esses esquemas podem ser mais ou menos complexos dependendo de certas exigências, como por

exemplo, o grau de segurança que se deseja alcançar, o valor do que se deseja proteger, a facilidade com que o usuário pode ter acesso ao sistema de identificação, o custo do sistema, entre outros.

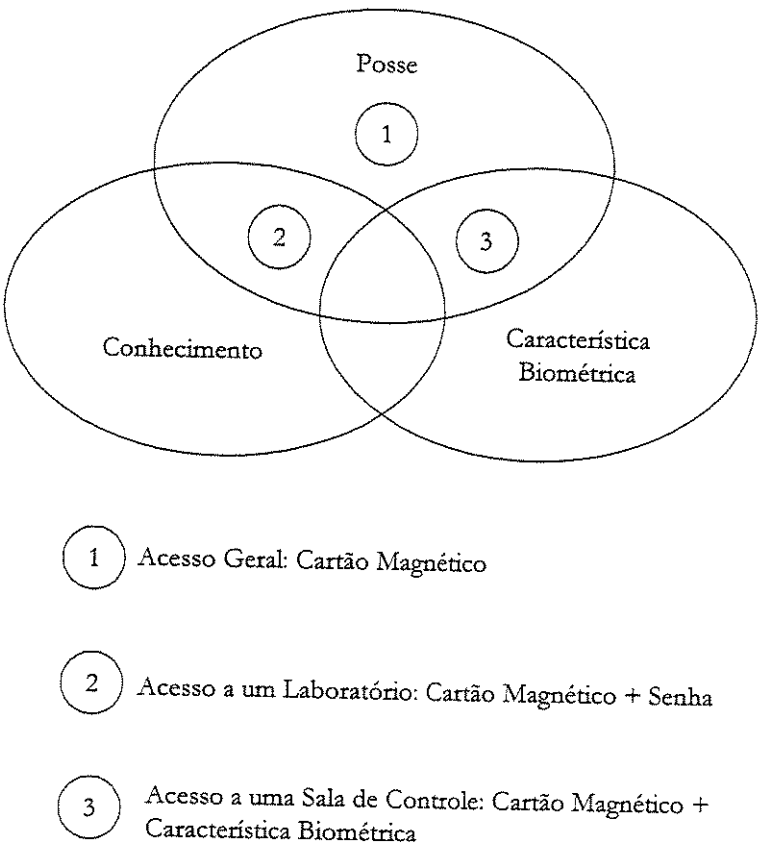


Figura 2.1: Esquemas de acesso para identificação de identificação.

A figura 2.1 apresenta uma representação desses três pilares exemplificando três esquemas de acesso a diferentes locais. No primeiro esquema, o acesso a determinado lugar é permitido simplesmente se apresentando um cartão magnético. No segundo esquema, o acesso é permitido através do conhecimento de uma senha e de possuir um cartão magnético. O terceiro caso é semelhante ao anterior, com a diferença de que o acesso só é permitido se for apresentada uma característica biométrica, a qual é inerente à pessoa que se deseja autenticar. No primeiro e no segundo esquema, tanto o cartão magnético, quanto o conhecimento da senha poderiam ser passados de uma pessoa para outra. Porém, no último caso uma característica biométrica, por exemplo uma impressão digital, impõe que a pessoa que apresente o cartão magnético realmente seja quem diz ser.

A utilização de características biométricas não exclui totalmente os atuais consagrados métodos de autenticação pessoal, mas faz substancial contribuição com respeito à qualidade do serviço de identificação.

A figura 2.2 apresenta um diagrama de blocos com a tipologia de métodos de autenticação associados a sistemas baseados em características biométricas. Nas próximas subseções descreveremos esses métodos de forma mais detalhada.

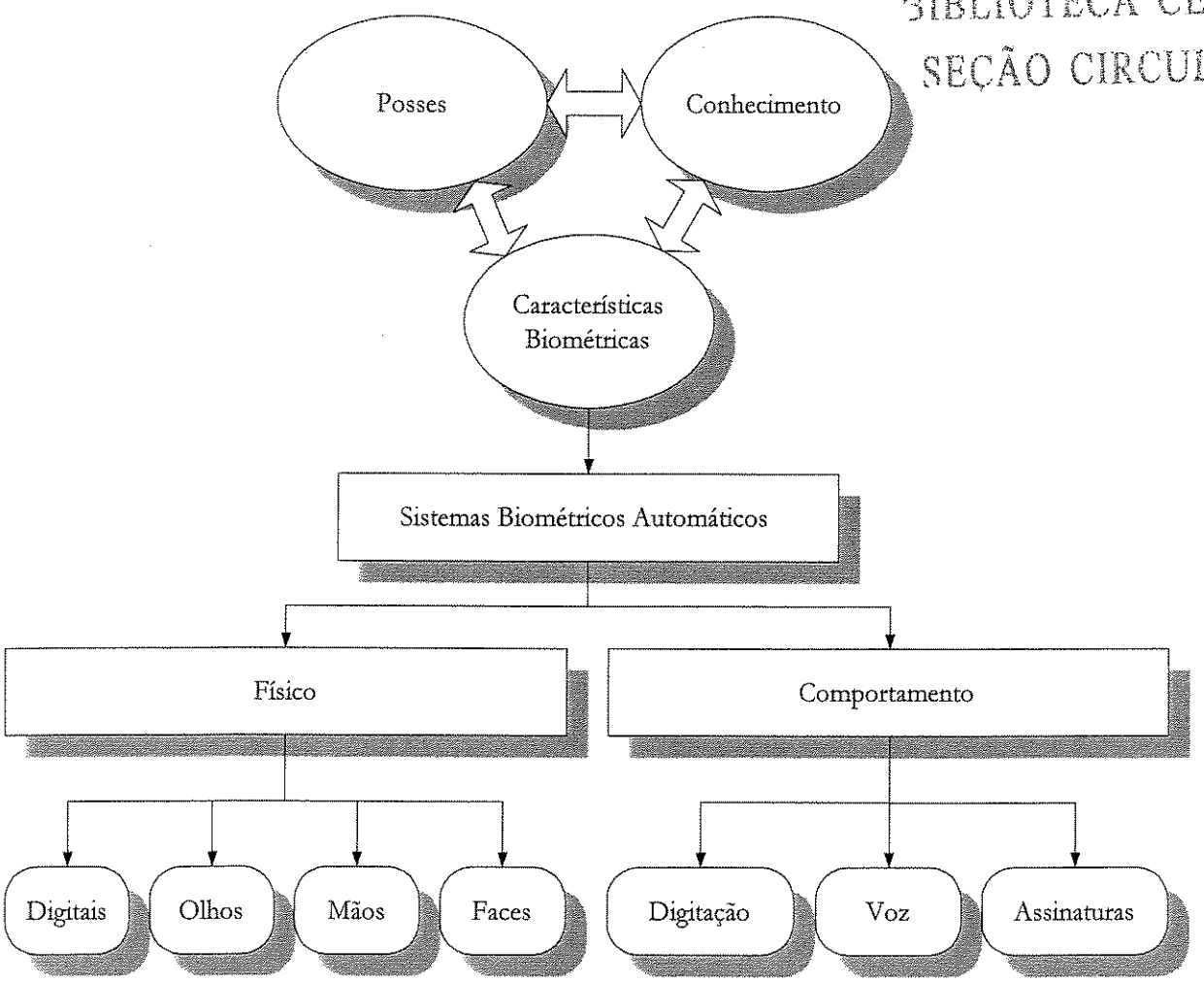


Figura 2.2: Tipologia de métodos de identificação associados a sistemas baseados em características biométricas.

2.2.1 Impressões Digitais

A estabilidade e unicidade das impressões digitais são bem estabelecidas na sociedade. Após muitos estudos [9][10][11], se estima de que a chance de duas pessoas, incluindo gêmeos, tenham a mesma impressão digital é menor do que uma em um bilhão. A extração de características sobre impressões digitais se baseia em encontrar a posição de pequenos pontos chamados de minúcias que estão presentes nas digitais, tais como, pontos de finalização de linhas e pontos de junção de linhas [12]. Outros contam o número de vales e sulcos que existem entre esses pontos [13]. Dependendo do esquema de identificação escolhido e do grau de segurança do sistema, o arquivo de referência que contêm as informações sobre a impressão digital varia de algumas centenas de bytes até milhares de bytes. Hoje em dia, a maior aplicação da tecnologia de impressões digitais é em sistemas de identificação automática utilizadas pela polícia em vários países do mundo.

2.2.2 Olhos

Tanto o padrão da íris quanto o padrão dos vasos sangüíneos do fundo do olho (retina) provêem uma base única para identificação [14]. A principal vantagem da captura de padrão da íris sobre o varredura da retina é que na primeira não se necessita que o olho do indivíduo que está sendo testado esteja focalizado em um determinado lugar. Ainda mais, segundo [15], a imagem da íris pode ser obtida pelo dispositivo de captura até a um metro de distância. No caso da varredura de retina, essa é realizada direcionando-se uma luz infravermelha de baixa intensidade na pupila e na parte posterior do olho. O padrão da retina é refletida de volta para a câmara a qual captura o padrão [16].

A varredura de retina é um dos melhores métodos biométricos existentes com taxas de erros de classificação muito baixas, base de dados de referências pequenos e processos rápidos de confirmação de identidade. O que mais dificulta a difusão desse tipo de tecnologia, continua sendo a resistência dos usuários, isto é, convencer a pessoa que vai se servir dessa técnica para a autenticação de identidade, de que a luz infravermelha que incidirá sobre seu olho não lhe irá fazer mal [17].

2.2.3 Mãos

A autenticação num sistema de identificação via geometria da mão se baseia em medidas das dimensões de partes das mãos, tais como o comprimento do dedo, sua largura e área. A

classificação utilizando esses parâmetros, leva em conta a forte correlação que existe entre essas diferentes medidas. Os primeiros sistemas baseados nessas características datam de 1960, sendo que as medidas que utilizavam eram apenas o comprimento de quatro dedos [18][19].

2.2.4 Face

Uma das áreas que está crescendo mais rapidamente na indústria da biometria em termos de novos esforços de desenvolvimento é a verificação e identificação através de faces [20]. Muitos dos trabalhos nessa área empregam tanto métodos de redes neurais como correlações estatísticas do formato geométrico da face. Nesses métodos se tenta imitar como os seres humanos reconhecem uma outra pessoa. A imagem das faces são adquiridas de forma direta pelos equipamentos de vídeo que hoje em dia estão disponíveis. Os atuais sistemas têm dificuldade de conseguir altos níveis de performance quando a base de dados aumenta para alguns milhares de indivíduos [21].

2.2.5 Digitação

A dinâmica da digitação, também chamada de ritmo de digitação, é um método biométrico que está diretamente ligado a área de segurança de computadores. Como o nome indica, esse método analisa a maneira como os usuários digitam no teclado seu *login* e sua senha. Nesse caso, as características extraídas são a seqüência de valores alfanuméricos que se está digitando, assim como o intervalo de tempo entre apertar uma tecla e outra em uma palavra [22].

Nos sistemas que se servem dessa abordagem biométrica, o mais notável é que o usuário não percebe que está sendo identificado por meio de uma característica biométrica a não ser que lhe seja dito. Por outro lado, para o sucesso desse método, quanto maior a habilidade na digitação tenha o usuário, será mais fácil e confiável a maneira como é reconhecido, visto que sua variação intra-pessoal será pequena [23].

2.2.6 Voz

A voz é utilizada em sistemas automáticos de verificação/identificação de locutor. Essa abordagem biométrica é muito atrativa visto que é considerada pouco invasiva pelos usuários.

Os humanos utilizam-se de características de "alto nível" [24], tais como sotaque, estilo do locutor, entonação, estado emocional, etc., para reconhecer uma pessoa através de sua voz. Como

esse tipo de característica é difícil de ser adquirida e mensurada de forma automática pelo computador, parâmetros de "baixo nível" derivados de medidas acústicas do sinal de voz, como freqüência fundamental, envoltória espectral, freqüência de formantes, energia, etc., são empregados [25].

2.2.7 Assinaturas

Os sistemas de reconhecimento de assinaturas se dividem em sistemas dinâmicos e sistemas estáticos. Os sistemas de reconhecimento de assinaturas dinâmicas utilizam técnicas baseadas nas pequenas diferenças do processo dinâmico da escrita da assinatura, como por exemplo, pressão, aceleração, e número de vezes que levantamos a caneta do papel. Por outro lado, os sistemas que utilizam apenas a imagem da assinatura (sistemas estáticos), utilizam características como a inclinação dos traços da escrita, o número de palavras, a razão entre a altura e o comprimento da assinatura etc. [26].

A chave do sucesso de um sistema de verificação/identificação de assinaturas é encontrar características da assinatura que sejam mais constantes, isto é, que variem pouco durante o processo de cadastramento [27].

2.2.8 Comparação entre Tecnologias Biométricas

A tabela 2.1 apresenta uma comparação entre as tecnologias biométricas apresentadas anteriormente, levando em consideração três fatores [28]:

- Desempenho: refere-se à capacidade de um sistema em autenticar corretamente um indivíduo devido a um tipo de característica biométrica.

- Aceitabilidade: indica o quanto as pessoas aceitam esse tipo de identificação biométrica na sua vida cotidiana.

- Fraudável: reflete a facilidade com que um sistema pode ser enganado por métodos fraudulentos.

Tabela 2.1: Comparação entre tecnologias biométricas

Característica biométrica	Desempenho	Aceitabilidade	Fraudável
Impressões Digitais	Alta	Média	Baixa
Olhos	Alta	Baixa	Baixa
Mãos	Média	Média	Média
Face	Baixa	Alta	Alta
Digitação	Baixa	Média	Média
Voz	Baixa	Alta	Baixa
Assinaturas	Baixa	Alta	Alta

CAPÍTULO 3

RECONHECIMENTO DE PADRÕES

Neste capítulo fazemos uma apresentação sobre reconhecimento de padrões introduzindo conceitos referentes a extração de característica e classificadores. Em seguida fazemos uma apresentação geral dos componentes de um sistema automático de verificação/identificação de assinaturas.

3.1 Introdução

Com apenas alguns poucos anos de idade, os seres humanos são capazes de reconhecer dígitos e letras, sejam essas pequenas, grandes, manuscritas, inclinadas ou rotacionadas. Esses caracteres podem estar dispersos num fundo de uma imagem ou parcialmente ocultos entre outras informações e mesmo assim temos a habilidade de reconhecê-los. O melhor reconhecedor de padrões continua sendo o ser humano, mesmo que ainda não saibamos com exatidão como a tarefa do reconhecimento ocorre internamente em nosso cérebro [29].

O reconhecimento automático de padrões é o estudo de como as máquinas podem observar o meio que as rodeiam, aprender e distinguir padrões de interesse nesse meio e serem capazes de tomar decisões corretas sobre as categorias a que pertencem tais padrões.

O reconhecimento, descrição, classificação e agrupamento de padrões feitos automáticamente (por máquinas) são problemas importantes a serem resolvidos em uma variedade de disciplinas científicas tais como biologia, psicologia, medicina, marketing, visão computacional, inteligência artificial e sensoriamento remoto. Mas, o que é um padrão?. O dicionário Aurélio [6] define padrão como "modelo oficial de pesos e medidas; protótipo,

arquétipo". Por exemplo, um padrão poderia ser a imagem de uma impressão digital, uma palavra manuscrita, uma face humana ou um sinal de voz. Dado um padrão, seu reconhecimento/classificação pode consistir em uma das tarefas a seguir:

1) Classificação supervisionada: na qual o padrão de entrada é identificado como membro de uma classe predefinida.

2) Classificação não supervisionada: na qual o padrão é associdado para uma classe não previamente definida.

Note que o problema de reconhecimento nesses casos está sendo definido com relação às tarefas de classificação ou categorização, onde as classes ou podem ser definidas *a priori* pelo projetista do sistema (no caso da classificação supervisiosada) ou estarem baseadas em um aprendizado feito sobre a similiridade dos padrões (no caso de classificação não supervisionada).

O interesse na área de reconhecimento de padrões tem se renovado recentemente devido a aplicações emergentes. Essas aplicações incluem, *data mining* (identificação de um padrão dentro milhões de padrões multidimensionais), classificação de documentos (busca eficiente de texto em documentos), organização e busca em base de dados multimídia e biometria (identificação pessoal baseada em vários atributos físicos e de comportamento).

O aumento do poder computacional permite maior rapidez no processamento de grandes volumes de dados. Isso facilita por sua vez, o emprego de diversos métodos mais complexos e elaborados para análise e classificação de dados.

O projeto de um sistemas de reconhecimento de padrões envolve essencialmente quatro aspectos:

1) Aquisicão de dados

2) Pré-preprocessamento

3) Representação dos dados

4) Tomada de decisão (Classificação)

O tipo de problema a ser resolvido dita a escolha do(s) sensor(es) para aquisição de dados, as técnicas de preprocessamento, os esquemas de representação e os modelos de tomadas de decisão. De maneira geral, um problema de reconhecimento de padrões bem definido e suficientemente delimitado (pequenas variações intra-classes e grandes variações inter-classes) nos levará a uma representação compacta do padrão e uma estratégia de decisão simples.

Vale salientar que, uma das maneiras de fazer com que o sistema conheça as classes em que terá que classificar os padrões de entrada, é apresentar ao sistema um conjunto de exemplos, também chamado de conjunto de treinamento. A partir desse conjunto, o sistema poderá delimitar o espaço de características a que pertencem os padrões.

As abordagens mais conhecidas em reconhecimento de padrões são o reconhecimento estatístico, o reconhecimento sintático ou estrutural e o reconhecimento via redes neurais. Esses modelos não são necessariamente independentes e existem vários trabalhos que utilizam sistemas híbridos envolvendo modelos múltiplos [30].

Neste trabalho iremos empregar a abordagem estatística. Veremos o reconhecimento de padrões no sentido de classificação, isto é, associar um padrão de entrada a uma determinada classe.

3.2 Modelo de Classificação

Suponha que estamos trabalhando com um padrão visual e que conheçamos *a priori* que os padrões em que estamos interessados são as 26 letras do alfabeto. Podemos dizer, nesse caso, que o problema de reconhecimento de padrões é o de associar ao padrão de entrada (letra) uma das 26 classes. Assim, limitamos o problema a decidir se a entrada pertence à classe 1, classe 2 ... classe c. Suponha a seguir que foi utilizado uma câmara para digitalizar a imagem da letra em questão como uma matriz bidimensional composta por pixels que representam a intesidade de brilho dos pontos da imagem original.

Uma das maneiras de classificar esses dados é fazendo uma comparação da imagem de entrada com os modelos padrões que representam cada uma das classes e então escolher aquele que apresente melhor "casamento".

Às vezes, o que torna difícil a classificação correta das imagens de entrada é seu elevado grau de variabilidade com relação à classe que realmente pertencem. Uma das maneiras de

minimizar esse problema é representar um padrão de entrada através de características que sejam discriminantes.

3.2.1 Características

Uma maneira de classificar um objeto ou evento é fazendo medidas de suas propriedades ou características. Por exemplo, para classificar uma letra pode ser útil saber sua área e perímetro. Podemos medir sua compressão através da razão entre sua área e o quadrado do seu perímetro. Podemos também medir seu grau de simetria com relação ao eixo horizontal fazendo a comparação entre a área que fica na sua metade superior com a da metade inferior.

Algumas características podem ser particularmente sensíveis a pequenas diferenças importantes. Por exemplo, para distinguir a letra "D" da letra "O", podemos medir o quão reto é o lado esquerdo desses padrões, isso pode ser feito calculando a razão entre a distância de um segmento de reta e a distância do arco pertencente à letra.

Claramente podemos perceber que as características estão intimamente ligadas ao problema específico que desejamos resolver. Assim sendo, pode-se dizer que encontrar um bom conjunto de características é muito mais arte do que ciência [31].

3.3.2 Vetor de Características

Na maioria das vezes, podemos medir um conjunto fixo de características de qualquer objeto ou evento que desejamos classificar. Por exemplo, podemos medir sempre:

x_1 = Área

x_2 = Perímetro

...

$$x_d = \frac{\text{Comprimento do arco}}{\text{Comprimento de linha reta}}$$

Onde x_1, x_2, ... x_d são componentes de um vetor coluna $\mathbf{x}$ de dimensão *d*. Nesse caso, podemos pensar em um conjunto de características como sendo o vetor de características $\mathbf{x}$ (figura 3.1.a). De forma semelhante, podemos pensar em $\mathbf{x}$ como sendo um ponto em um espaço de características d-dimensional (figura 3.1.b).

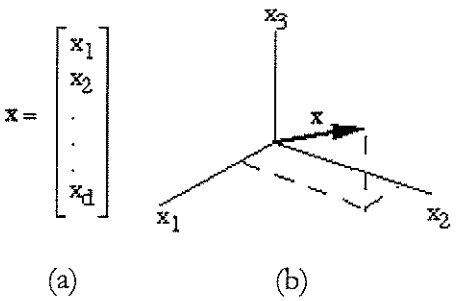


Figura 3.1: Vetor de características **x** e sua representação no espaço tri-dimensional.

Na figura 3.2 apresentemos o diagrama de blocos de um sistema de reconhecimento de padrões simplificado, onde o módulo de extração de características processa a informação de entrada com o objetivo de determinar valores numéricos para o conjunto de *d* características x_1, x_2, ..., x_d, que compõe o vetor de características **x**. A seguir, o módulo de classificação recebe **x** e associa para ele uma de suas *c* classes, classe 1, classe 2 ... classe c.

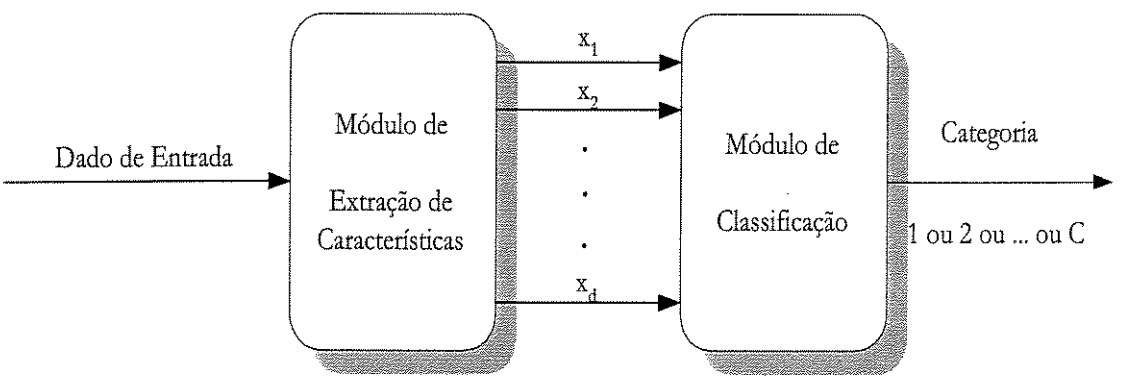


Figura 3.2: Módulos de extração e classificação de caracteristiscas.

A implementação do módulo de extração de características é dependente do problema. Um módulo extrator de características ideal deveria produzir o mesmo vetor de características **x** para todos os padrões que pertencem à mesma classe e diferentes vetores de características para padrões de classes diferentes. Na prática, dados de entrada diferentes no módulo de extração de características produzem diferentes vetores de características, porém se espera que a variabilidade dentro de uma mesma classe seja pequena.

3.3.3 Classificadores simples

O casamento de padrões (*template matching*) é uma abordagem natural para o classificação de padrões. Por exemplo, considere a letra D e a letra O adicionadas de um sinal ruidoso como mostrado na figura 3.3. As amostras sem ruído que estão à esquerda dessa figura podem ser utilizadas como *templates*. Para classificar uma das amotras ruidosas, basta compará-la com os dois *templates*. Isso pode ser feito de duas maneira equivalentes:

1. Contar o número de concordâncias (pixel preto casa com pixel preto e pixel branco casa com pixel branco). Tomar a classe que tem o maior número de concordâncias. Essa abordagem é chamada de máxima correlação.
2. Contar o número de discordâncias (pixel preto onde deveria ser pixel branco ou pixel branco onde deveria ser pixel preto). Tomar a classe que tem o menor número de discordâncias. Essa abordagem é chamada de mínimo erro.

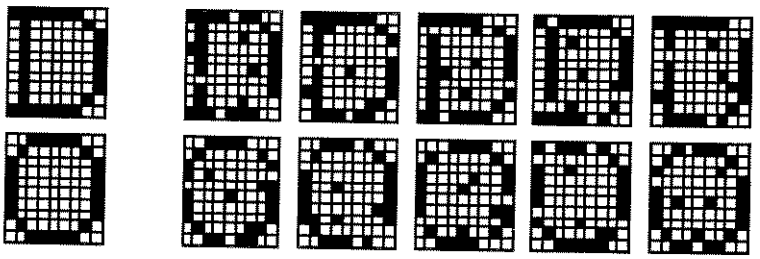


Figura 3.3: Exemplo da imagem da letra D e O "ruidosas"

O *template matching* funciona bem quando as variações na mesma classe são pequenas ou, como no caso do exemplo, quando existir "ruido aditivo". É claro que essa abordagem não funcionará bem em todos os problemas, como no caso em que existirem distorções na imagem de entrada como rotação, expansão, contração e oclusão entre outras.

O *template matching* pode ser expresso matematicamnte da seguinte forma:

Seja $\mathbf{x}$ o vetor de características de um dado de entrada desconhecido e sejam os vetores $\mathbf{m}_1$, $\mathbf{m}_2$, ... $\mathbf{m}_c$ os *templates* para cada uma das c classes. Então o erro do casamento entre $\mathbf{x}$ e $\mathbf{m}_k$ é dado por:

$$\|\mathbf{x}-\mathbf{m}_k\| \qquad \text{onde } k = 1, 2, ..., c \qquad (3.1)$$

Nesse caso $\|\mathbf{u}\|$ é uma norma do vetor **u**. O classificador de erro mínimo calcula $\|\mathbf{x}-\mathbf{m}_k\|$ para k = 1 até *c* e escolhe a classe para a qual o erro é mínimo. Como $\|\mathbf{x}-\mathbf{m}_k\|$ é também uma medida de distância de **x** até $\mathbf{m}_k$, a equação (3.1) é chamada de classificador de distância mínima.

A figura 3.4 apresenta um diagrama de blocos de um classificador de distância minima.

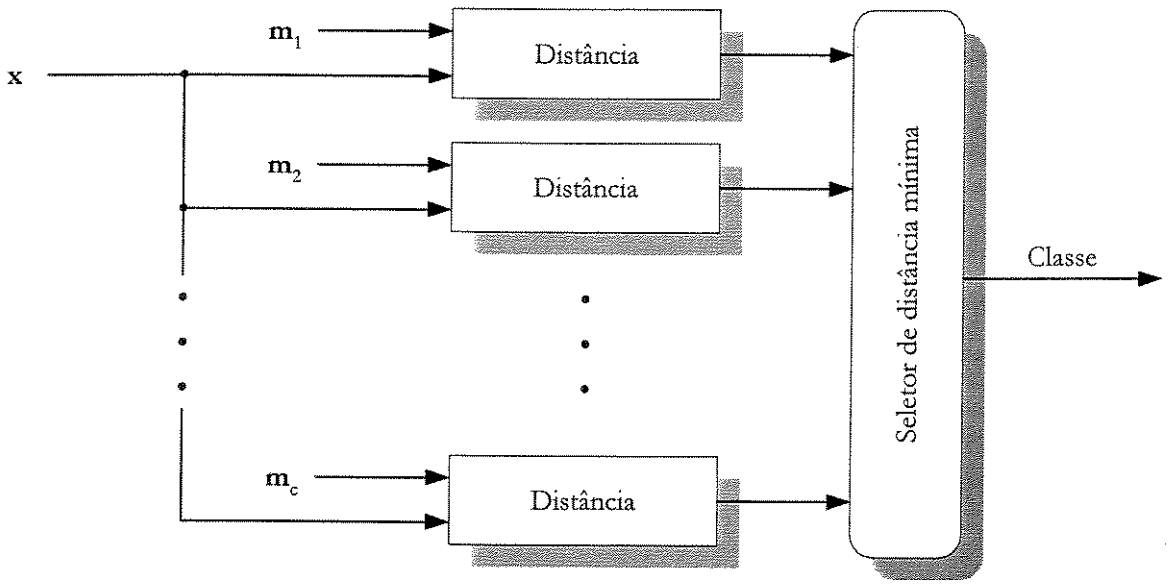


Figura 3.4: Diagrama de blocos de um classificador de distância mínima.

Existem muitas maneiras de se definir a norma $\|\mathbf{u}\|$ e isso corresponde às diferentes métricas que podem ser utilizadas: As métrica mais utilizada são:

1. Métrica Euclidiana: $\|\mathbf{u}\|_E = \sqrt{u_1^2 + u_2^2 + \ldots + u_d^2}$ (3.2)

2. Métrica Manhattan: $\|\mathbf{u}\|_M = |u_1| + |u_2| + \ldots + |u_d|$ (3.3)

3.3.4 Discriminantes Lineares

Utilizando o produto interno para expressar a distância euclidiana entre **x** e $\mathbf{m}_k$, podemos escrever:

$$\|\mathbf{x}-\mathbf{m}_k\|^2 = (\mathbf{x}-\mathbf{m}_k)'(\mathbf{x}-\mathbf{m}_k) \tag{3.4}$$

$$= \mathbf{x}'\mathbf{x}-\mathbf{m}_k'\mathbf{x}-\mathbf{x}'\mathbf{m}_k+\mathbf{m}_k'\mathbf{m}_k \tag{3.5}$$

$$= -2\left[\mathbf{m}_k'\mathbf{x}-0{,}5\mathbf{m}_k'\mathbf{m}_k\right]+\mathbf{x}'\mathbf{x} \tag{3.6}$$

Note que o termo $\mathbf{x}'\mathbf{x}$ é o mesmo para todas as classes, ou seja para todo *k*. Para encontrar o *template* $\mathbf{m}_k$ que minimiza $\|\mathbf{x}-\mathbf{m}_k\|$ é suficiente encontrar $\mathbf{m}_k$ que maximize a expressão entre colchetes, $\left[\mathbf{m}_k'\mathbf{x}-0{,}5\mathbf{m}_k'\mathbf{m}_k\right]$. Define-se a função de discriminante linear por:

$$g(\mathbf{x}) = \mathbf{m}_k'\mathbf{x}-0{,}5\|\mathbf{m}\|^2 \qquad k=1,2,...,c \tag{3.7}$$

Então, podemos dizer que o classificador euclidiano de distância mínima classifica um vetor de características de entrada $\mathbf{x}$ calculando c funções discriminantes lineares $g_1(\mathbf{x})$, $g_2(\mathbf{x})$, ... , $g_c(\mathbf{x})$ e alocando $\mathbf{x}$ à classe a qual corresponde a função discriminante máxima. Ainda, é possível demonstrar que um classificador de distância euclidiana mínima é equivalente a um classificador de correlação máxima, figura 3.5.

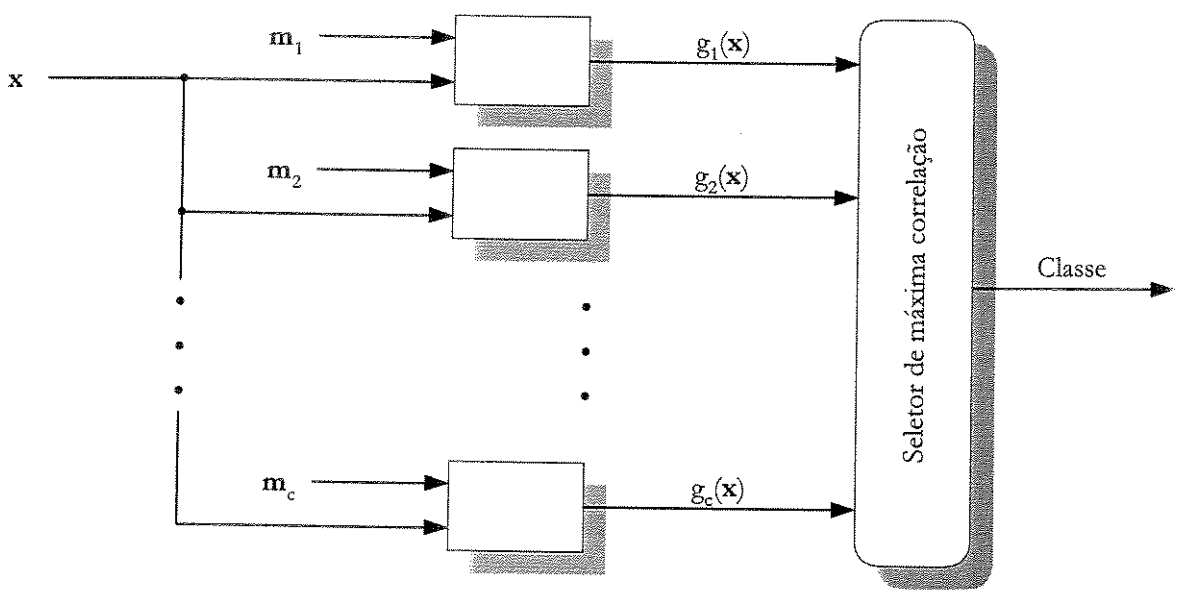


Figura 3.5: Diagrama de blocos de um classificador de correlação máxima.

Em geral, um classificador de padrões particiona o espaço de características em volumes chamados regiões de decisão. Todos os vetores de características em uma região de decisão são alocados na mesma classe. As regiões de decisão são separadas por superfícies chamadas de fronteiras de decisão. Para um classificador de distância mínima, as fronteiras de decisão são compostas pelos pontos que se encontram igualmente distantes entre dois ou mais *templates*.

Se um classificador de distância mínima produz resultados satisfatórios, não existe razão para utilizar um outro classificador mais complexo. Porém, freqüentemente acontece que os classificadores simples cometem muitos erros. Existem vários possíves motivos para isso ocorrer, entre os quais podemos mencionar:

1. As carecterísticas podem ser inadequadas para distinguir a diferença entre as classes.
2. As características podem ser altamente correlacionadas.
3. O espaço de características pode não ser particionado por hiperplanos.
4. Podem existir distintas subclasses entre os dados de treinamento.
5. O espaço de características pode ser muito complexo.

3.3.5 Classificador de Distância Padrão

Algumas das limitações dos classificadores euclidianos de distância mínima, como por exemplo, os problemas devido aos diferentes valores de escala entre medidas dos vetores de características, podem ser superados utilizando-se um classificador de distância padrão.

Considere uma característica x. Suponha que temos e exemplos de padrões pertencentes à mesma classe. Sejam os diferentes valores para a característica x, denominados de x(1), x(2), ..., x(e).

Existem duas estatísticas importantes que podemos utilizar para caracterizar essa coleção de exemplos, a média e a variância.

A média m é dada por:

$$m = \left[\frac{x(1) + x(2) + \ldots + x(e)}{e} \right] \tag{3.8}$$

A variância v é dada por

$$v = \frac{[(\mathrm{x}(1)-m)^2 + (\mathrm{x}(2)-m)^2 + ... + (\mathrm{x}(e)-m)^2]}{e-1} \tag{3.9}$$

Observa-se que m tem a mesma unidade que x, mas v tem sua unidade ao quadrado. A raiz quadrada da variância é o desvião padrão s, e possui a mesma unidade que x:

$$s = \sqrt{v} \tag{3.10}$$

O valor numérico de uma característica x depende da unidade que é utilizada, isto é, de sua escala. Se x é multiplicada pelo fator a, então tanto a média como desvio padrão são multiplicados por a. (A variância é multiplicada por a^2)

As vezes é desejavel colocar os dados numa mesma escala de modo que o desvio padrão resultante seja igual à unidade. Isso pode ser feito dividindo x pelo desvio padrão s. De modo similar, ao medir a distância entre x e m podemos ponderá-la pelo desvio padrão. Assim, chamamos p a distância padrão a qual é dada pela equação (3.11):

$$p = \left| \frac{\mathrm{x}-m}{s} \right| \tag{3.11}$$

Note que p é invariante tanto a translação quanto a escala. Isso sugere uma generalização importante para o classificador euclidiano de distância mínima. Seja x_i o valor da característica i, seja $m_{i,j}$ o valor médio da característica i da classe j, e seja $s_{i,j}$ o desvio padrão da característica i da classe j. A distância padrão entre o vetor catacterísticas $\mathbf{x}$ e o vetor de características médio $\mathbf{m}_j$ para a classe j, é dada por:

$$p(\mathbf{x},\mathbf{m}_j)^2 = \left[\frac{\mathrm{x}_1 - m_{1,\mathrm{j}}}{s_{1,\mathrm{j}}}\right]^2 + \left[\frac{\mathrm{x}_2 - m_{2,\mathrm{j}}}{s_{2,\mathrm{j}}}\right]^2 + \left[\frac{\mathrm{x}_\mathrm{d} - m_{\mathrm{d},\mathrm{j}}}{s_{\mathrm{d},\mathrm{j}}}\right]^2 \tag{3.12}$$

Essa distância tem a importante propriedade de ser invariante com a escala. Isso significa que ao utilizarmos essa medida, as unidades utilizadas nas várias características que compõe o vetor contribuem de forma equivalente no cálculo da distância.

3.4 Introdução à Verificação Automática de Assinaturas

Assinaturas são um caso particular de manuscritos, em que aparecem caracteres "especiais" ou distorcidos, floreios e desenhos. É comum não haver regularidade quanto ao tamanho e distribuição dos caracteres. Em muitos casos, as assinaturas são ilegíveis (parte semântica desconhecida). Porém, inúmeras características próprias do autor são consciente e inconscientemente depositadas no papel quando o mesmo assina. Assim sendo, é possível uma identificação posterior através do processamento de tais características [32].

O projeto de um sistema para verificação de assinaturas requer a solução de 5 tipos de problemas: aquisição de dados, pré-processamento, extração de características, processo de comparação e avaliação de desempenho.

Sistemas dinâmicos de verificação de assinaturas utilizam um digitalizador ou uma caneta instrumentalizada para produzir os sinais de entrada. Sistemas estáticos de verificação de assinaturas captam a imagem de uma assinatura com ajuda de uma câmara, *scanner*, ou digitalizador. No primeiro caso, um ou mais sinais variando com o tempo dão uma representação da assinatura escrita. Velocidade, pressão, aceleração são alguns exemplos de sinais dinâmicos. No segundo caso, uma assinatura ou texto escrito no papel aparece como uma imagem bidimensional adquirida através de meios ópticos.

Uma imagem de assinatura pode ser facilmente copiada, quer seja por meios ópticos ou mecânicos. Além disso, as informações dinâmicas são altamente degradadas em uma amostra estática. Parte dessa informação pode ser recuperada por analistas especializados em documentos, utilizando habilidades específicas, mas a maioria de seus métodos não podem ser facilmente implementados em um ambiente computacional. Esses são alguns dos problemas enfrentados em um SVAE. Entretanto, já existem tentativas de se recuperar a dinâmica de amostras estáticas. Ammar [33] tentou extrair e utilizar indiretamente características de pressão a partir de imagens de assinaturas.

O diagrama de fluxo da figura 3.6 descreve de maneira geral como as imagens de entrada são processadas em um sistema de verificação de assinaturas estáticas.

Os dados de entrada são pré-processados a fim de filtrar a imagem, a seguir, são executadas algumas tarefas de mudança de resolução, eliminação de dados não relevantes e finalmente, é validada a aquisição. O próximo passo se refere ao processo de extração de características. Um conjunto de características é computado a partir dos dados de entrada filtrados e, a partir do mesmo, é gerado o vetor de características que serve para descrever a assinatura.

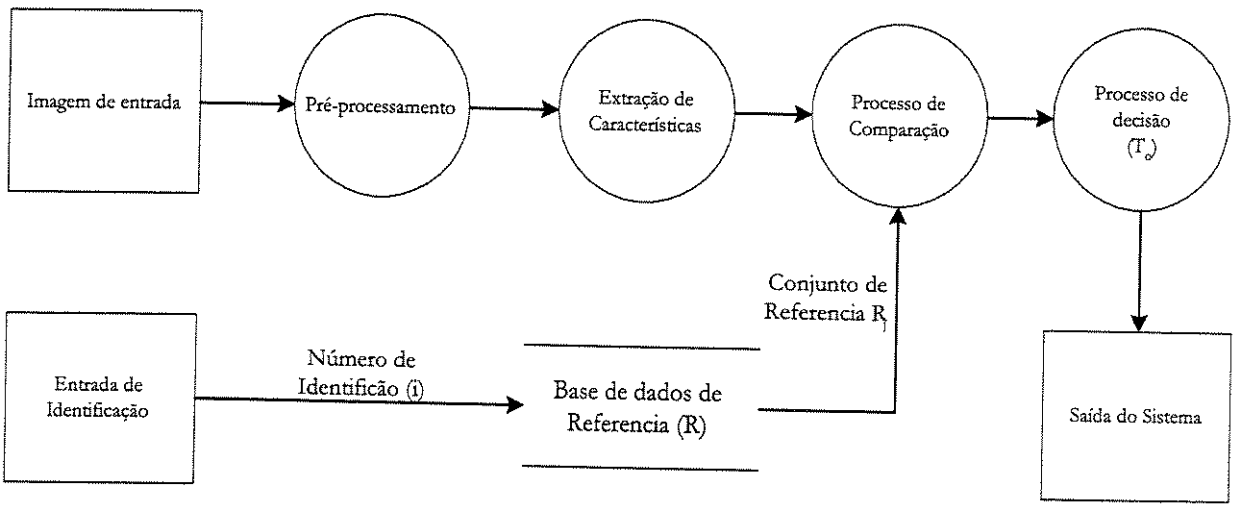


Figura 3.6: Diagrama de fluxo de dados de um sistema pala reconhecimento de assinaturas.

Antes de efetuar as comparações, um conjunto de referência de assinaturas deve ser gerado para cada usuário *i* do sistema. Esse conjunto é geralmente computado sobre algumas amostras e então é incorporado a uma base de dados de referência *R* através de uma informação de identificação (*i*). Essa identificação é depois utilizada para extrair o conjunto de referência R_i apropriado da base de dados *R*. O vetor de característica da assinatura de teste S_j recentemente coletado, é então comparado com seu conjunto de referência.

Finalmente, um processo de decisão avalia a saída do algoritmo de comparação com respeito a um limiar T_o, para determinar se a assinatura deverá ser considerada como pertencente ou não à classe (verdadeira ou falsa, no caso da verificação). Por exemplo, utilizando uma medida de distância de similaridade (quanto menor a distância, maior a semelhança) $d(S_j, R_i)$ entre uma assinatura de teste S_j e uma assinatura de referência R_i, tem-se:

$$\begin{cases} \text{aceitar a assinatura } S_j & \text{se } d(S_j, R_j) \le T_0 \\ \text{rejeitar a assinatura } S_j & \text{se } d(S_j, R_j) > T_0 \end{cases} \tag{3.13}$$

Por várias razões, a verificação de assinaturas não pode ser considerada como sendo um problema trivial de reconhecimento de padrões. De forma ideal, a verificação de assinaturas pode ser apresentada como um problema de classificação em duas classes. Seja Ω_i o conjunto de todas as assinaturas relativas a um escritor *i*. Uma decisão binária deverá permitir o particionamento de Ω_i em $\tilde{\omega}_1^i$, a classe que consiste das assinaturas verdadeiras, e $\tilde{\omega}_2^i$ a classe das assinaturas falsificadas (figura 3.7.a).

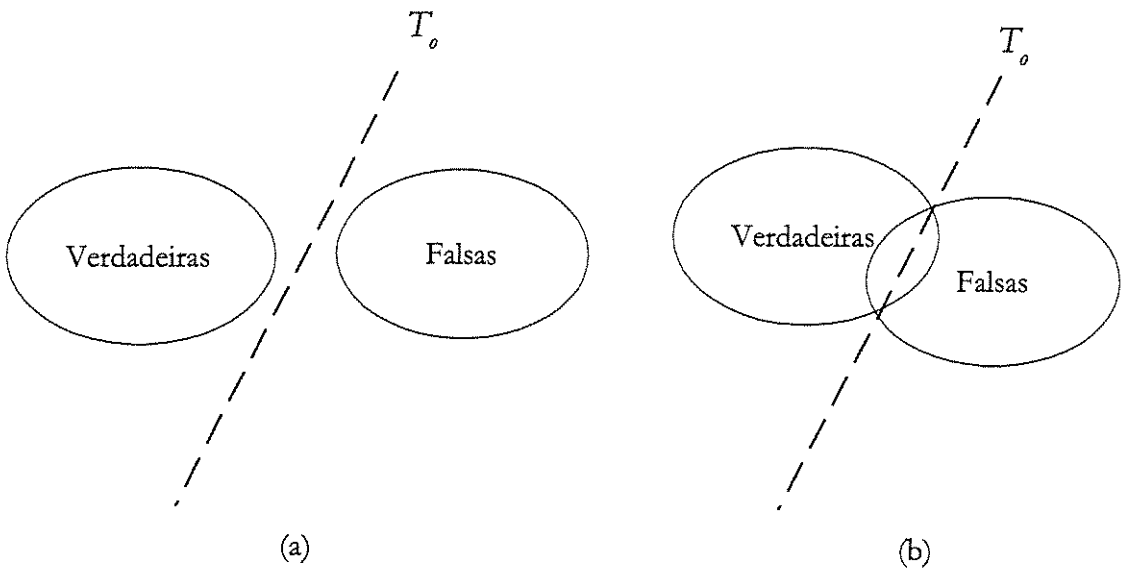


Figura 3.7: Divisão de assinaturas em verdadeiras e falsas. (a) Caso ideal, (b) Caso real.

Apesar de se observar certa estabilidade nos traços das assinaturas, assinar não é um processo que leve após sucessivas tentativas, a características que possam ser repetidas varias vezes, sejam precisas e idênticas. Assim sendo, quando duas assinaturas são idênticas é porque uma delas é verdadeira e a outra é falsificada, possivelmente uma cópia. De fato, um grande leque de variabilidade pode ser observado em assinaturas de acordo com o país, a idade, os hábitos, o estado mental ou psicológico e as condições físicas [34].

Dois tipos de variabilidade em assinaturas têm que ser distinguidos:

- $\tau_{\omega i}$: variabilidade intra-classe ou intra-pessoal, isto é, a variabilidade observada dentro de uma classe ($\tilde{\omega}_1^i$) de assinaturas genuínas de algum indivíduo *i*.
- τ_{bi}: variabilidade inter-classe ou inter-pessoal, ou seja, as diferenças existentes entre as classes de assinaturas genuínas ($\tilde{\omega}_1^i$) e ($\tilde{\omega}_1^j$), obtidas a partir de dois diferentes autores *i* e *j*.

Em teoria, a variabilidade intra-classe τ_ω deveria ser tão baixa quanto possível, e a variabilidade inter-classe τ_b, deveria ser grande o suficiente para ser utilizada na separação entre as classes. Na prática, as classes não são bem separadas (Figura 3.7.b). Uma assinatura aceita ou reconhecida como verdadeira ($\in \tilde{\omega}_1^i$) pode ser definida da seguinte forma:

- Autêntica ($\tilde{\omega}_1^i$): Se escrita pelo autor i da referência R_i e S_j tem uma boa similaridade com R_i.

$$d(S_j, R_i) < T_0 \qquad \text{com} \quad j = i \tag{3.14}$$

- Imitada ou falsa aceitação (FA): Se escrita por alguém j que não é o autor da referencia R_i e se S_j tem uma boa similaridade com R_i.

$$d(S_j, R_i) < T_0 \qquad \text{com} \quad j \neq i \tag{3.15}$$

Por sua vez uma assinatura reconhecida como falsa, pode ser:

- Degenerada ou falsa rejeição (FR): Se escrita pelo autor i da referência R_i e se S_j não for similar a R_i. O termo "dissimulada" é normalmente utilizado quando essa degeneração é voluntária.

$$d(S_j, R_i) > T_0 \qquad \text{com} \quad j = i \tag{3.16}$$

- Falsa ($\tilde{\omega}_2^i$): Se escrita por algum j que não é o autor da referência R_i e S_j não é similar a R_i

$$d(S_j, R_i) > T_0 \qquad \text{com} \quad j \neq i \tag{3.17}$$

3.4.1 Medidas de desempenho de sistemas automáticos de verificação

A performance de um sistema de verificação é medido de acordo com os erros de falsa rejeição e falsa aceitação. Na prática o erro de falsa rejeição (EFR) observado é uma estimativa da probabilidade do sistema incorretamente indicar que uma assinatura é falsa, quando de fato é

verdadeira. Enquanto que o erro de falsa aceitação (EFA) observado é uma estimativa da probabilidade do sistema incorretamente indicar que uma assinatura é verdadeira, quando de fato é falsa. O EFR e EFA são expressos em porcentagens e variam de acordo com o limiar T_0 escolhido.

Dois tipos de gráficos são comumente utilizados para ilustrar as taxas de erro EFR e EFA: o gráfico das curvas de falsa refejeição e falsa aceitação, figura 3.8 (a) e (b), e o gráfico da curva receptor de operador (ROC), figura 3.8 (c).

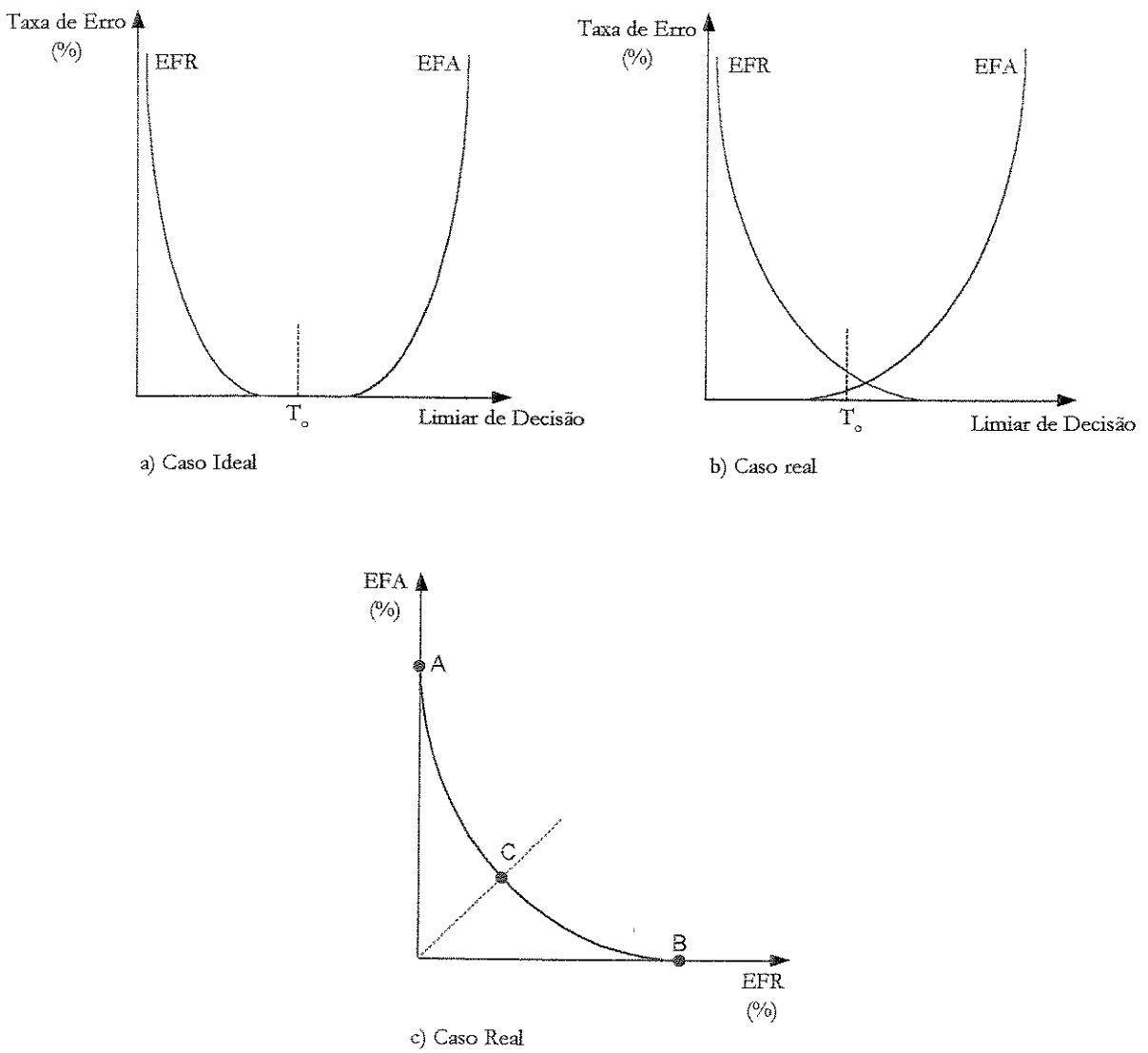


Figura 3.8: Diagramas de avaliação de desempenho em sistemas de verificação de assinaturas: (a) caso ideal, (b) e (c) caso real.

As ilustrações na figura 3.8 (a) e (b) provêem maior informação que (c) por que nelas fica explicito o limiar empregado no processo de decisão. As curvas de desempenho em (a) mostram o caso ideal de classificação, no qual taxas de erro iguais a zero são alcançadas pelas curvas EFR e EFA antes que ambas venham a se cruzar. Por outro lado. As curvas de desempenho em (b) e (c) mostram o caso que ocorre na prática, no qual pelo menos uma das taxas de erro não é igual zero.

Os três pontos de operação, A, B e C, indicados na curva (c) da figura 3.8 são apontados como os de maior relevância na literatura. Em [35] é sustentado que o ponto de operação C, o ponto no qual o valor de EFR e EFA são iguais, é o mais importante, pois especifica a separabilidade que o sistema oferece entre as assinaturas autênticas e falsas, embora em uma aplicação real um sistema de verificação raramente consiga operar exatamente nesse ponto. Na prática, sistemas são programados para trabalharem próximos aos pontos A ou B.

O ponto de operação A, também chamado do EFA_0, é o valor que EFA possui quando EFR tem valor zero. Indica a probabilidade de incorretamente o sistema aceitar assinaturas falsas como sendo verdadeiras, quando todas as assinaturas verdadeiras são detectadas.

O ponto de operação B, também chamado de EFR_0, é o valor que EFR possui quando EFA tem valor zero. Indica a probabilidade de incorretamente o sistema aceitar assinaturas verdadeiras como sendo falsas, quando todas a assinaturas falsas são dectectadas.

Um exemplo típico de um sistema de verificação de assinaturas que deve ter um desempenho próximo ao ponto A é um sistema de ponto de vendas, onde uma taxa de falsa rejeição baixa para assinaturas verdadeiras é requerida visto que a satisfação do consumidor é a principal prioridade. Similarmente, um exemplo de sistema que deve operar próximo ao ponto B é aquele que valida a identidade de uma pessoa com o propósito de permitir a entrada a uma instalação segura.

CAPÍTULO 4

ESTADO DA ARTE EM VERIFICAÇÃO DE ASSINATURAS

Neste capítulo fazemos uma apresentação sobre o processo de escrita das assinaturas, introduzindo suas características e tipos de falsificações. Mostramos também o modelo geral de um sistema de verificação automático de assinaturas e com base nele, apresentamos detalhes de cada um dos processos que compõem esse sistema.

4.1 A Assinatura Humana

Por ser considerada tradicionalmente a forma mais confiável e legítima de autenticação da identidade de um indivíduo, a assinatura manuscrita é exigida em transações financeiras, de forma que o indivíduo também ateste o conhecimento, o conteúdo e sua concordância com os termos do documento.

O motivo que permite utilizar a assinatura como um dos meios mais confiáveis de identificação é que ela contém características únicas da escrita do assinante. Essas características são o reflexo de um conjunto de fatores físicos e psicológicos desse indivíduo durante a escrita. Com base nessas características, especialistas em assinaturas procuram quantificá-la com o intuito de definir, de maneira consistente, se uma certa assinatura foi feita pelo indivíduo genuíno ou por uma outra pessoa qualquer [36].

A seguinte definição para a palavra *assinatura* é encontrada no Dicionário Aurélio: "É o ato ou efeito de subscrever o próprio sinal ou nome em documento". Especialistas em análise de documentos, e outros que se confrontam com um grande número de assinaturas, de fato

constatam a frase "subscrever o próprio sinal". Essa frase é verdadeira por que muitas vezes as assinaturas não correspondem à escrita legível do seu nome. O que ocorre, na prática, é uma junção entre componentes da escrita manuscrita com uma série de traços estilísticos, que tem por objetivo individualizar a assinatura através de um sinal gráfico. Mesmo que a assinatura seja totalmente ilegível, ela é suficiente para ser reconhecida como pertencendo a um determinado indivíduo [37].

A assinatura de uma pessoa evolui à medida que vai sendo feita repetidamente, aparecendo pequenas diferenças na sua forma e em seu estilo cada vez que o escritor se dispõe a reproduzí-la. Por isso constata-se que duas assinaturas verdadeiras de uma mesma pessoa nunca são exatamente iguais. As pequenas alterações ou variações que as assinaturas de uma mesma pessoa apresentam são chamadas de variações intra-pessoais [38].

Passamos a nos referir como assinatura verdadeira àquela que o escritor reproduz mantendo um mesmo padrão de letras e de traços, sem a necessidade de um esforço grande de concentração. Assim, através de um grupo de assinaturas verdadeiras é possível se derivar hábitos e qualidades da escrita. Esses tipos de amostras são a base do estudo da assinatura humana e é com elas que se pode determinar se a assinatura de uma pessoa é autêntica ou não.

A assinatura de uma pessoa não apresenta uma forma única e bem definida, pois aparecem variações em seus traços a cada momento em que ela é reproduzida. Ainda mais, quando nos referimos ao ato de verificação de assinaturas, a assinatura de uma pessoa só é consistente se comparada com um conjunto de assinaturas que ela espontaneamente reproduziu anteriormente.

Partindo da utilização de um conjunto de assinaturas verdadeiras, especialistas em assinaturas se valem das características de forma, de movimento e de possíveis influências externas do meio para estabelecer sua autenticidade. Esses especialistas definiram dois tipos de fatores que influenciam de maneira direta no processo de escrita de uma assinatura. O primeiro fator se refere às influências internas, que são qualidades inerentes da pessoa que assina, e o segundo fator diz respeito às influências externas ou do meio, que atuam no momento da escrita da assinatura [39].

4.2 Análise de Assinaturas

Na análise de assinaturas procura-se características de sua escrita que sejam específicas a ela. Podemos citar os toques inicias e finais da assinatura, a rapidez da execução, a forma da letra, os alinhamentos vertical e horizontal, a razão de distância entre as várias letras, o espaçamento entre

palavras da mesma assinatura, a qualidade das linhas da escrita, o tamanho total da assinatura e os traços de estilo, entre outras características [40].

Para o mesmo indivíduo, a maioria dessas qualidades variam levemente e se enquadram dentro de um limite máximo. É por causa disso que, quando se tenta determinar a legitimidade de uma assinatura, o examinador do documento tentará conduzir a verificação pela comparação da assinatura em questão, com um conjunto de assinaturas verdadeiras. Esse conjunto de assinaturas deve, de preferência, ter sido adquirido de forma semelhante e mais ou menos na mesma época da assinatura que se deseja examinar [41].

O objetivo do exame utilizando um conjunto de assinaturas verdadeiras é determinar o grau de variação, ou seja, quanto podem variar as assinaturas de uma mesma pessoa. De maneira geral, o grau de variação será diferentemente afetado por influências internas e externas que atuam no momento do assinar. Assim sendo, pode-se esperar um alto grau de variação entre as assinaturas onde influências internas e externas se apresentaram, e uma variação pequena quando as influências externas e internas se mantiveram constantes.

Podemos citar como influências externas o tamanho do instrumento de escrita, seu peso e a maneira como a ponta do instrumento desliza sobre o papel. A posição do escritor em relação ao papel que irá assinar possui uma relevância importante no grau de variação. Ou seja, se o escritor se encontra em pé ou não, se está confortavelmente sentado ou de maneira incomoda, se está numa posição mais inclinada ou reta, se a mão, pulso, braço e cotovelo estão na posição normal de escrita ou não. O tipo de papel que se está utilizando pode também criar alguns problemas, como por exemplo, se a folha de papel em que se está escrevendo é muito áspera ou lisa. A inclinação do papel com relação à posição do escritor é também importante, principalmente se ele tem algum problema físico [42].

As influências internas são principalmente do tipo psicológico. O estado emocional, a pressa, a idade do assinante ou ainda uma simples dor de cabeça influem no resultado final da escrita da assinatura.

O conjunto dessas influências resulta, de uma forma geral, em variações no traço da assinatura, dentre as quais podemos citar a proporção entre as palavras, a inclinação e arredondamento das letras, a ornamentação, a legibilidade, etc.. Ocorrem também variações nas características ligadas à dinâmica dos movimentos da escrita, como a não uniformidade da velocidade e interrupções durante a escrita das palavras [43].

4.3 Assinaturas Pessoais

Quando uma pessoa deseja criar sua assinatura, começa a fazer uma série de esboços. Depois de algum tempo de exercício constante, consegue reproduzir seus traços de forma automática.

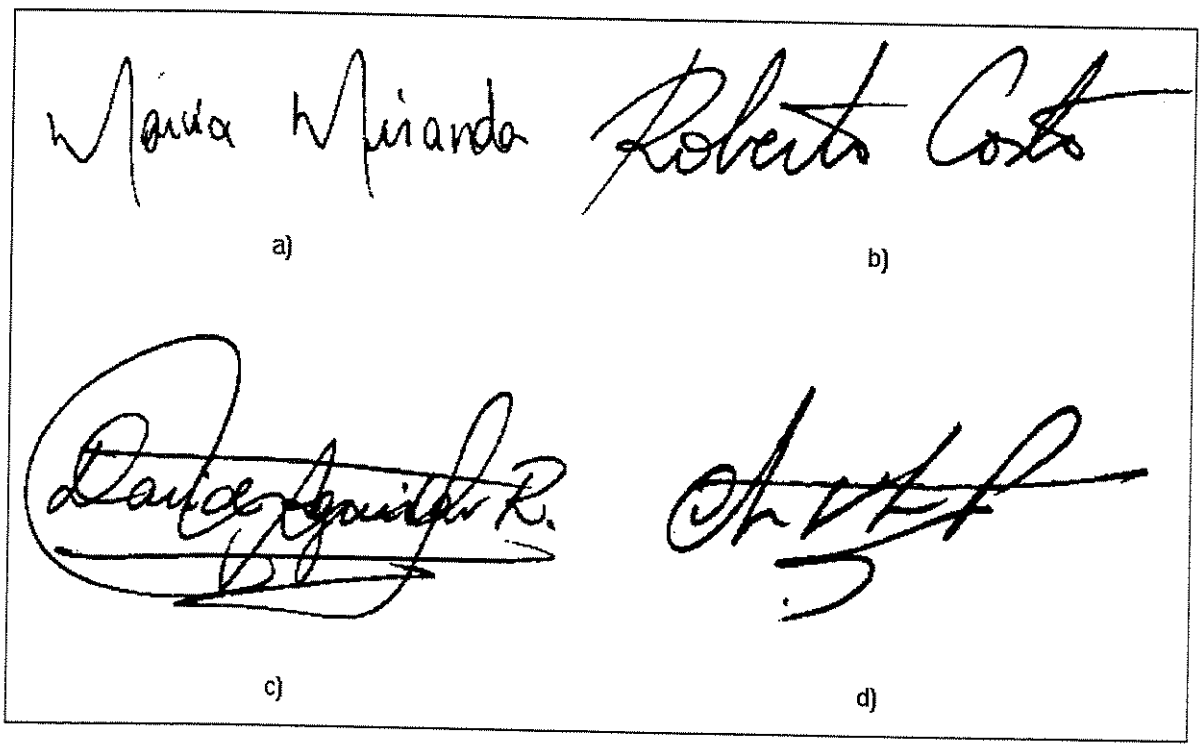


Figura 4.1: Estilos de assinaturas manuscritas.

Dependendo da aparência final que o indivíduo deseja dar para sua assinatura, ela pode ser classificada em dois grupos. O primeiro grupo é aquele no qual a aparência final reflete o próprio nome do escritor. Nesse caso, a pessoa assina se valendo quase que exclusivamente da semântica do seu nome e do seu estilo padrão de escrita, como nas assinatura a) e b) da figura 4.1. O segundo grupo é aquele em que a aparência final da assinatura toma a forma de um sinal gráfico. Nesse caso, a habilidade gráfica do escritor é em geral mais aprimorada, visto a dificuldade em tentar sempre reproduzir um grafismo que se preocupa mais com a forma dos traços do que com a semântica do próprio nome, como nas assinaturas c) e d) da figura 4.1.

Em ambos os grupos, a assinatura da pessoa irá se tornar personalizada à medida que o tempo passa e ela for produzida regularmente.

4.4 Falsificações de assinaturas

Uma assinatura falsificada é aquela feita com o intuito de imitar uma assinatura verdadeira para se passar por legítima.

Tomando como referência a semelhança existente entre uma assinatura original e sua falsificação, encontramos três tipos de falsificações: as aleatórias, as simples e as habilitadas. Pelas informações obtidas através de um banco nacional, mais de 90% das assinaturas falsificadas encontradas em documentos bancários são constituídas de falsificações aleatórias e simples.

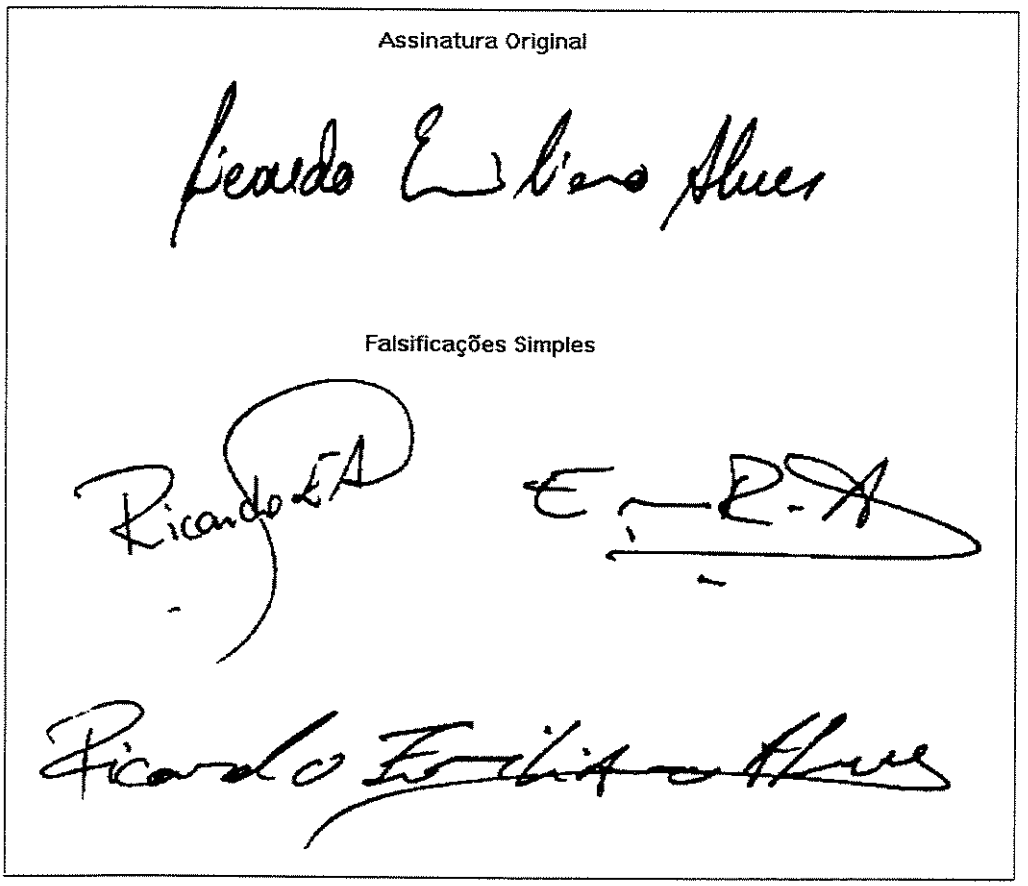


Figura 4.2: Exemplo de falsificações simples.

4.4.1 Falsificação aleatória

As falsificações aleatórias se caracterizam por ter sua forma gráfica e constituintes semânticos completamente diferentes da assinatura original. Nesse caso, o falsificador faz uma assinatura no documento sem se importar em imitar os traços básicos da assinatura original, inclusive chegando a escrever seu próprio nome ou qualquer outro grafismo para indicar que se trata da assinatura genuína.

4.4.2 Falsificação simples

Esse tipo de falsificação ocorre quando um falsificador escreve o nome da pessoa corretamente mas não consegue imitar sua forma gráfica. Dessa maneira, a falsificação pode parecer ou não com a assinatura original.

Esse tipo de falsificação geralmente ocorre quando o falsificador possui apenas o conhecimento do nome da pessoa, mas não tem nenhuma cópia impressa da assinatura verdadeira para se basear e assim poder desenhar uma falsificação mais aprimorada. A figura 4.2 mostra um exemplo de falsificação simples, onde temos a assinatura genuína na parte superior e as falsificações na parte inferior.

4.4.3. Falsificação habilidosa

Esse tipo de falsificação é produzida quando o falsificador tem acesso a uma amostra da assinatura original. O falsificador faz um esforço para obter a reprodução fiel dessa assinatura, trabalhando da maneira mais detalhada possível traço após traço, até conseguir uma falsificação de excelente qualidade. A figura 4.3 mostra o exemplo de duas falsificações habilidosas, que tiveram como modelo a assinatura que se encontra na parte superior dessa figura.

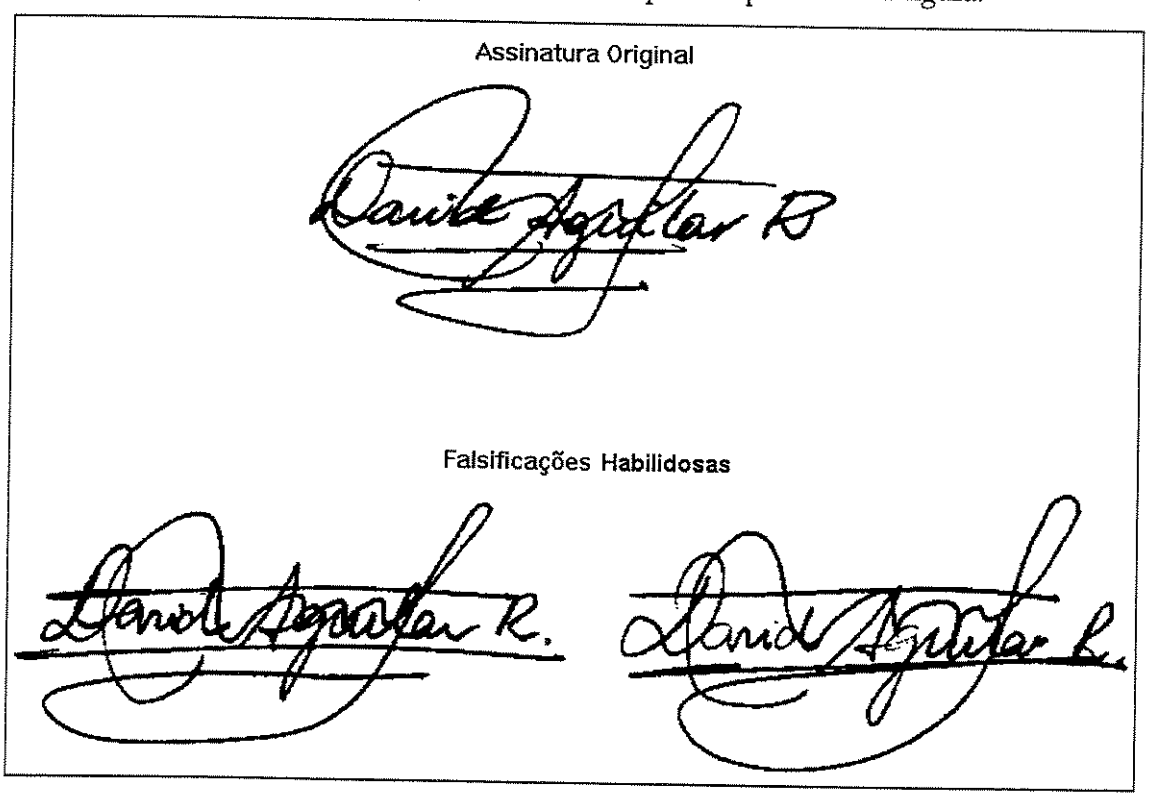


Figura 4.3: Exemplo de falsificações habilidosas.

4.5 Modelo Geral de um Sistema de Verificação de Assinaturas

Um modelo geral de sistema de verificação de assinaturas está representado na figura 4.4.

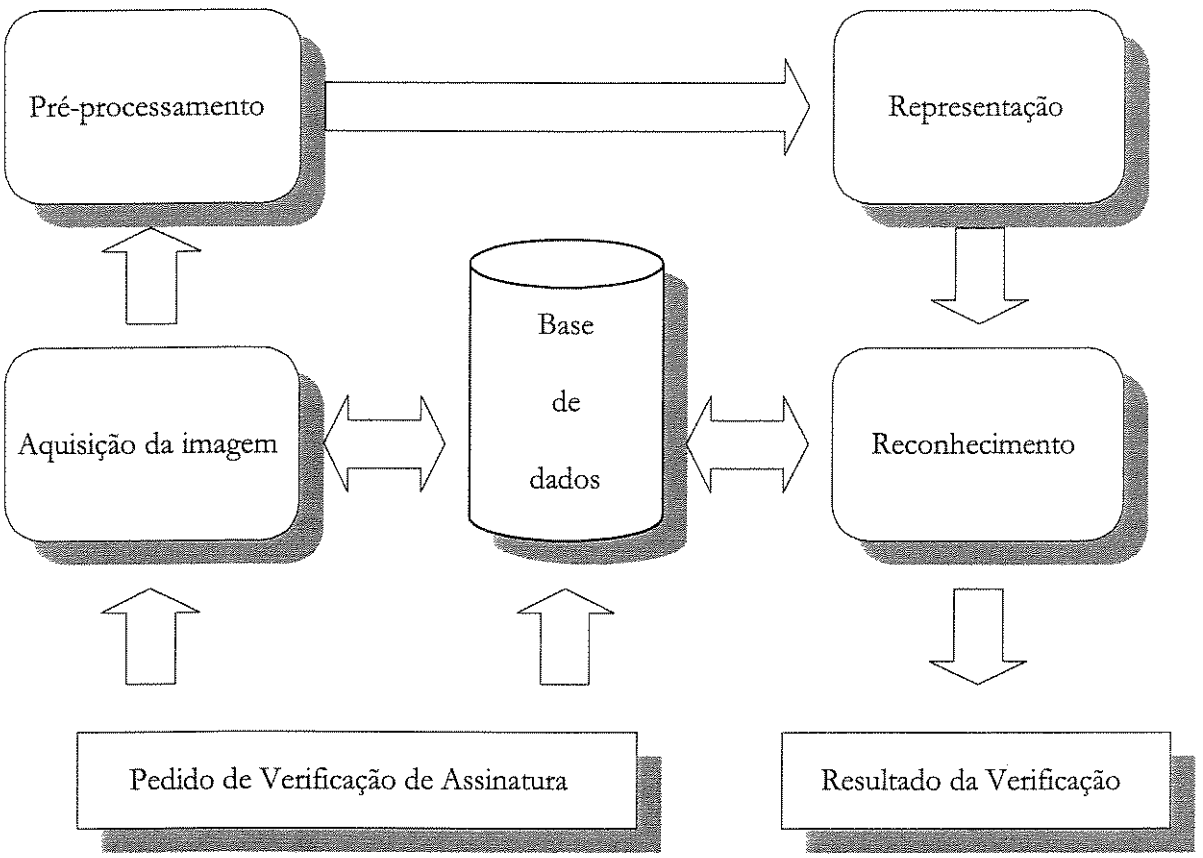


Figura 4.4: Modelo geral de um sistema de verificação de assinaturas.

Tomando como base o modelo da figura 4.4, observamos que esse modelo é composto de cinco blocos básicos:

1. Aquisição da imagem
2. Pré-processamento
3. Representação
4. Reconhecimento
5. Base de dados

A unidade de aquisição da imagem executa a operação de digitalização da imagem através de um *scanner* ou ainda, recebe diretamente uma imagem que está contida na base de dados. A unidade de pré-processamento recebe essa imagem e executa processos de filtragens, de segmentação e de normalização de tamanho. A unidade de representação é aquela encarregada de extrair as características das assinaturas, construindo um vetor de características da imagem que está sendo analisada. A unidade de reconhecimento é aquela que executa o processo de classificação da assinatura como sendo falsa ou verdadeira, através da comparação entre o vetor de características fornecido pela unidade de representação e a base de dados. Finalmente, a unidade de base de dados contém informações sobre as assinaturas de referência dos escritores e outros dados relativos.

Como pode ser visto da figura 4.4, a entrada do sistema é um pedido de verificação de uma assinatura, no qual deve constar necessariamente o número de identificação ou o próprio nome do indivíduo a quem ela é atribuída, para assim poder localizar as suas informações de referência junto à base de dados. Sem essas informações, o sistema teria que fazer a identificação da assinatura comparando-a uma a uma, entre todas as assinaturas da base de dados. Como resultado desse pedido, obtemos na saída do sistema a indicação de que a assinatura em questão foi considerada verdadeira ou falsa.

Como em qualquer sistema autônomo de reconhecimento de padrões, um sistema de verificação precisa adquirir algum conhecimento sobre as assinaturas verdadeiras de seus escritores, antes de poder executar sua tarefa. Tal processo de aquisição de conhecimento é executado durante a fase chamada de treinamento.

Na fase de treinamento, um certo número de assinaturas verdadeiras é utilizado para gerar um vetor de características, que contém a média de cada uma das características que se definiu extrair da assinatura. Somente depois que esses dados são computados o sistema poderá ser colocado em operação. Então, quando uma assinatura desconhecida é apresentada, é exigido que o sistema determine a sua autenticidade ou não, através de um processo de comparação.

4.5.1. Aquisição da imagem

Os aparelhos mais comumente usados para aquisição de imagens são o *scanner* e câmaras de vídeo CCD. A aquisição da imagem consiste em transformar a imagem existente em um documento em uma imagem digital. Pode-se considerar uma imagem digital como a matriz cujos

índices de linhas e colunas identificam um ponto da imagem, enquanto cada elemento da matriz identifica o nível de cinza naquele ponto.

4.5.2. Pré-processamento

A etapa de pré-processamento se ocupa em obter a imagem da assinatura livre do fundo em que ela está contida.

O pré-processamento tem por objetivo extrair a imagem da assinatura do fundo em que está contida e transformá-la numa imagem binária, onde os pixels pretos representariam os traços da assinatura manuscrita propriamente dita e os pixels brancos pertenceriam ao fundo.

Para chegar a esse ponto a imagem do documento passa pelas seguintes etapas: localização, segmentação, filtragem e normalização de tamanho. A figura 4.5 ilustra o resultado de cada uma destas etapas, utilizando como exemplo um cheque bancário.

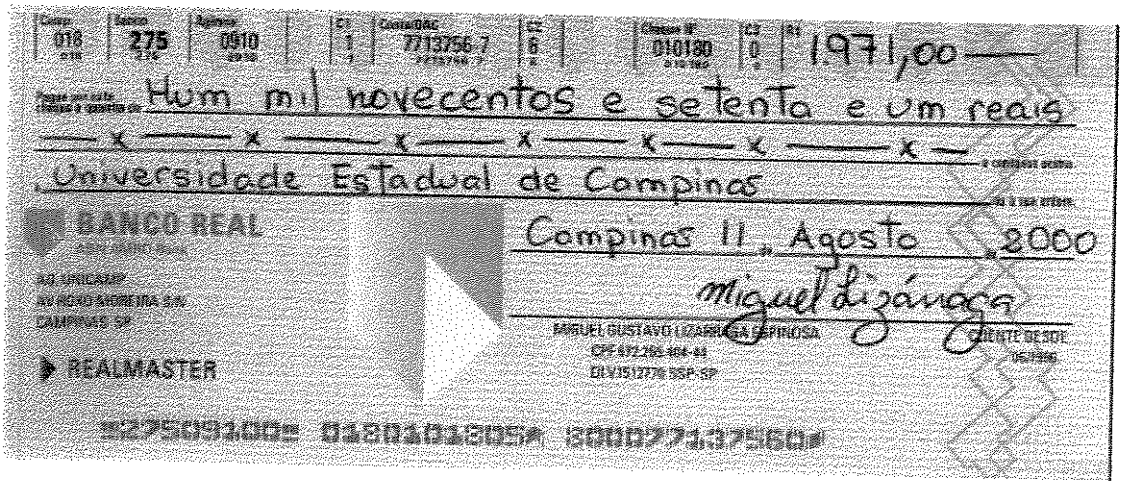
4.5.2.1 Localização

Nessa operação se executa a extração da imagem da assinatura. O mesmo processo também pode ser usado para localizar outras regiões de interesse da imagem. No caso específico de cheques bancários, existe uma padronização para as áreas que serão preenchidas manualmente no cheque. Como conseqüência, é possível definir as diferentes áreas que irão conter a informação da assinatura ou ainda o número do banco, o número do cheque, do CIC, o nome do correntista etc. A região mais importante a ser extraída num sistema automático de verificação é a da assinatura, mas extrai-se também a do nome do correntista ou do número do CIC para incrementar a informação referente ao pedido de verificação.

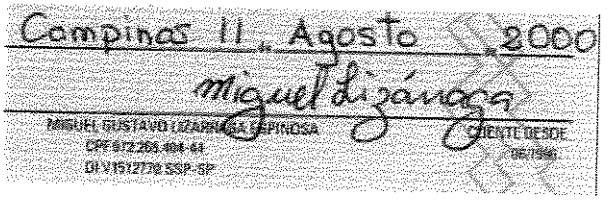
4.5.2.2 Segmentação

A segmentação é a operação que separa a assinatura propriamente dita do fundo da região em que ela está contida. O método mais comumente utilizado para tal propósito é o de limiarização. Esse método transforma a imagem original em níveis de cinza em uma imagem binária, através de um mapeamento dos seus pixels, utilizando uma função do tipo degrau, como ilustra a figura 4.6. Todos os pixels que ultrapassarem o valor de limiar L são mapeados para a imagem de saída com o valor *1*. Aqueles com valor abaixo do valor de limiar são mapeados com o valor *0*. Nas imagens binárias, os pixels de valor *1* representam o fundo e os pixels de valor *0* representam a assinatura.

Imagem de Entrada



Localização



Segmentação e Filtragem

Normalização

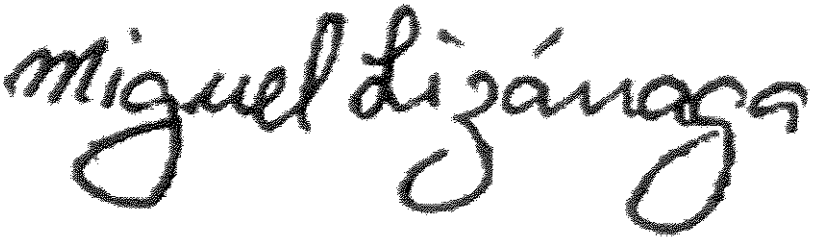


Figura 4.5: Operações da fase de pré-processamento.

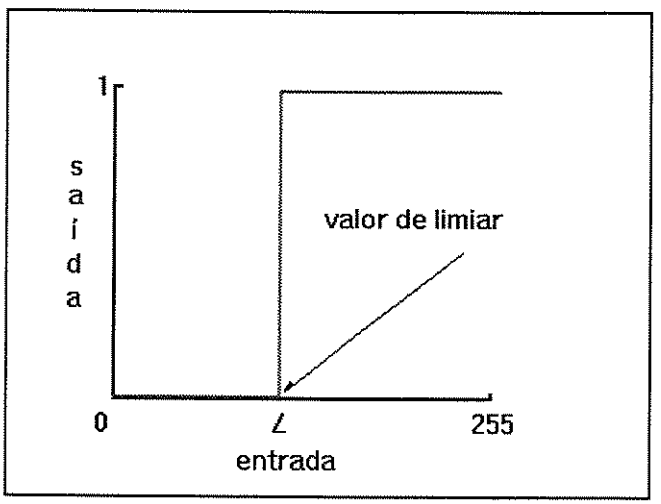


Figura 4.6: Função de mapeamento tipo degrau.

Esse método funciona bem quando a intensidade em níveis de cinza dos pixels pertencentes ao fundo da imagem forem sensivelmente mais claros ou mais escuros do que o valor dos pixels da assinatura. No caso da assinatura num cheque, observa-se que geralmente o fundo do mesmo está preenchido pelo logotipo do banco a que pertence. Ao se fazer a digitalização desse cheque, o fundo toma valores de pixels próximos aos da assinatura. Assim, uma simples limiarização dessa imagem resultará numa mancha preta ao invés da imagem da assinatura [44].

Para minimizar esse efeito, Yoshimura [45] desenvolveu um método que consiste basicamente da subtração entre a imagem de um cheque não preenchido com a imagem de um cheque preenchido, resultando numa imagem em que aparecem apenas os traços que foram feitos com a caneta. O método de Yoshimura para segmentação da assinatura compreende, primeiro, em fazer um ajuste no sentido horizontal e vertical entre o cheque preenchido e o cheque não preenchido, a fim de se conseguir o melhor casamento entre o fundo de ambas as imagens. A seguir, na imagem do cheque não preenchido é passado um filtro. Esse filtro faz com que certas porções da imagem que contenham letras, linhas e números fiquem escuras, e o restante do cheque fique claro. O histograma da imagem filtrada se caracteriza por ter aproximadamente a aparência ilustrada na figura 4.7. Aproveitando a forma bimodal desse histograma, Yoshimura define um valor de limiar C_b que se encontra no mínimo dos dois modos. Os valores de pixels menores que C_b passam a ser iguais a *0*, enquanto os valores maiores ou iguais a C_b são iguais a *1*.

A eliminação do fundo da imagem do cheque que contém a assinatura é feita através da diferença entre a imagem filtrada e imagem do cheque não preenchida.

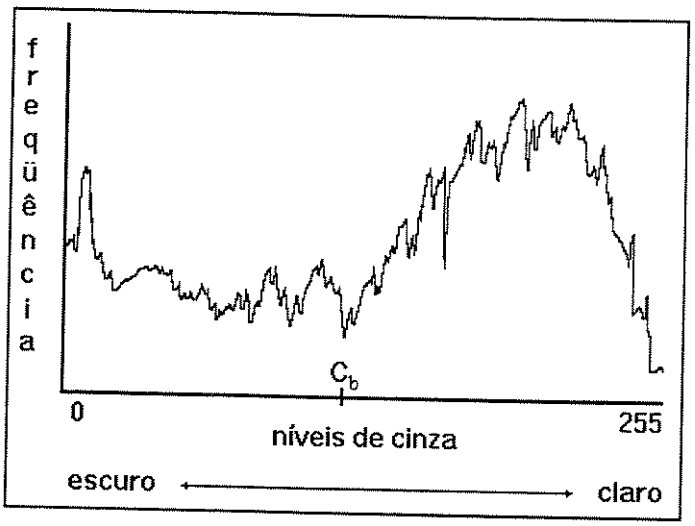


Figura 4.7: Histograma imagem filtrada.

Em [46], Lee utiliza uma abordagem semelhante. Para eliminar o padrão de fundo do cheque bancário, é feita a subtração entre a imagem do padrão de fundo previamente armazenada em uma base de dados e a imagem do cheque de entrada. Para que essa operação seja realizada com sucesso, processos de alinhamento vertical e horizontal entre as duas imagens devem ser feitos. A operação de subtração raramente consegue remover completamente o padrão de fundo do cheque. Esse problema se deve principalmente as variações dos níveis de cinza da informação impressa como também à imperfeição no alinhamento de posição entre as duas imagens. Parte do padrão de fundo que o sistema é falho em remover é chamado de ruído de fundo residual e é geralmente caracterizado pela presença de pontos isolados na imagem resultante. A seguir Lee se serve de um conjunto de operadores da morfologia matemática [47], para eliminar o ruído de fundo residual e minimizar a degradação da imagem.

4.5.2.3 Normalização de tamanho

Esse é um processo de transformação que muda basicamente o tamanho original da imagem. Ele pode também mudar sua orientação ou posição, dessa forma alterando as características geométricas originais da imagem.

A normalização de tamanho da assinatura tem por objetivo estabelecer um tamanho padrão para as assinaturas e dessa forma facilitar a sua comparação.

Nemceck normalizou as imagens das assinaturas para enquadrá-las numa área retangular de 256 pixels por 128 pixels [48]. Pender utilizou uma técnica de redução de resolução para enquadrar as imagens das assinaturas em uma área retangular de 128 pixels x 64 pixels [49]. Wilkinson fez uma redução das imagens para serem enquadradas num retângulo de 256 pixels por 128 pixels [35]. Lizárraga normalizou o tamanho da assinatura em função do seu eixo horizontal em 256 pixels, sendo que o eixo vertical variou mantendo a proporção com relação ao eixo horizontal [50].

4.5.2.4 Representação

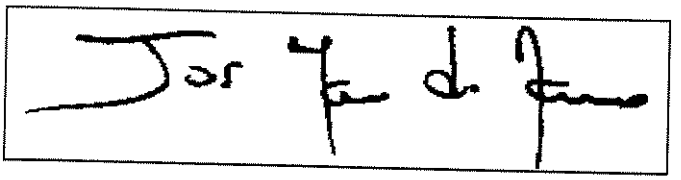
A representação da assinatura envolve a extração de propriedades da imagem ou ainda a relação existente entre partes da mesma. Cada uma dessas propriedades, ou relações, é chamada de característica. O conjunto das características extraídas de cada assinatura é denominado de vetor de características.

O processo de representação de uma assinatura na maioria das vezes não é reversível, isto é, a assinatura não pode ser reconstruída a partir do seu vetor de características. Por exemplo, se o vetor de características envolve apenas dados da proporção entre as componentes contextuais da assinatura, a reconstrução não é possível. Por outro lado, quando é utilizado algum tipo de transformação de imagem, como a transformada de Fourier ou Hadamard, e os coeficientes dessas transformadas são utilizados para compor o vetor de características, a reconstrução da imagem original pode ser feita a partir desses dados.

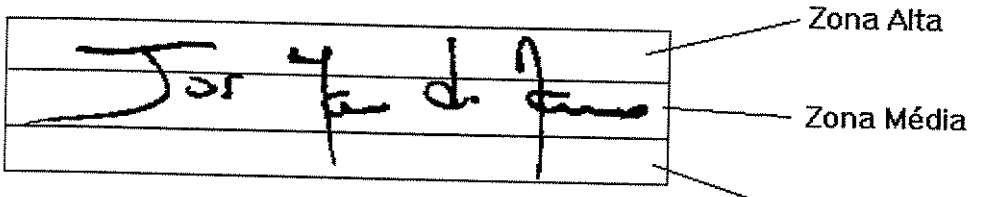
A abordagem da representação da assinatura adotada por pesquisadores no campo da verificação de assinaturas, é caracterizada como sendo global ou local [51]. A representação global é conveniente quando se estuda as características da imagem da assinatura como um todo. Um exemplo de tal abordagem é o uso dos coeficientes da transformada de uma imagem ou ainda a medida da inclinação de vários segmentos da assinatura. A representação local é conveniente quando se requer um detalhamento maior entre os componentes da assinatura. Nesse caso geralmente a assinatura é dividida em regiões onde são extraídas características referentes apenas àquela região, independentemente do contexto geral da imagem.

Numa abordagem global, Ammar [52] formou seu vetor de características com a inclinação e a razão existente entre o comprimento e a altura da assinatura, assim como a razão

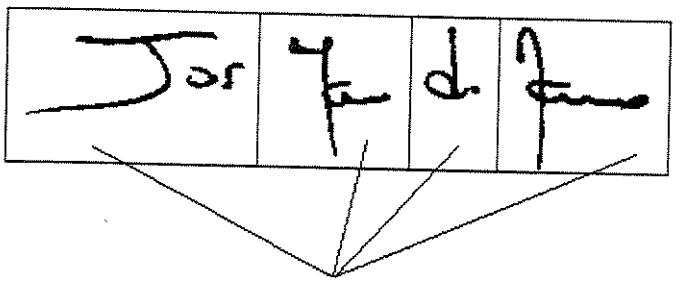
entre suas zonas alta, média e baixa [53]. Uma ilustração das diferentes zonas em que Ammar dividiu uma assinatura está mostrada na figura 4.8.b.



a) Imagem Original



b) Imagem dividida em Zonas



c) Imagem dividida em regiões

Figura 4.8: Imagem dividida em zonas e regiões.

Na abordagem local, Ammar tomou o cuidado de dividir a imagem da assinatura em regiões, cada uma geralmente constituída por uma palavra (ver figura 4.8.c). A partir daí extraiu as características para cada uma delas.

De maneira semelhante a Ammar, Nagel também dividiu a imagem da assinatura em zonas alta, média e baixa [54]. Dessa forma conseguiu diferenciar as letras que possuem hastes para cima (como as letras *t* e *d*) e as letras que tem hastes que se projetam para baixo (assim como as letras *j* e *g*). Definiu como letras longas aquelas que extrapolam a zona média e como letras curtas aquelas que estão todas contidas na zona média. Para poder facilitar esse reconhecimento, o autor recorreu às informações contidas na sua base de dados. Na abordagem global, o autor extraiu a proporção entre o comprimento total da assinatura e altura das letras longas, bem como a proporção entre o comprimento total da assinatura e a altura das letras curtas. Na abordagem local foi utilizada a proporção entre a altura de uma letra longa com a altura da letra curta que lhe segue, bem como a inclinação das letras longas.

Nemcek utilizou a transformada de Hadamard como meio para extrair as características da imagem [48]. Ao contrário de Ammar e Nagel, este método não depende de nenhuma informação textual que deve ser conhecida sobre a assinatura. Nessa implementação, cada um dos coeficientes da transformação de Hadamard é uma das características que representa essa imagem.

Brocklehurst utilizou um método de descrição de assinatura cujas características extraídas são o comprimento global da assinatura, a distância existente entre o ponto inicial no qual a assinatura começa a ser escrita e a área designada a ela, a inclinação do traço e a concavidade [55].

No caso de Pender, as características extraídas da imagem para formar o vetor de características são, na verdade, uma matriz formada por todos os pixels pertencentes à imagem da assinatura [49].

Bajaj se serviu apenas de três características globais no seu esquema de verificação de assinaturas. A primeira trata de momentos, que provê uma medida estatística da distribuição dos pixels na assinatura. O segundo e terceiro tipo de características globais concernem a distribuição dos pixels que se encontram na região superior e inferior da assinatura [56].

Deng utilizou *wavelets* para fazer a decomposição do sinal da imagem da assinatura. De maneira geral, a transformada de *wavelets* multidimensional pode decompor o sinal em informação extraída através de um filtro passa-baixas e informação extraída através de um filtro passa-altas. A informação passa-baixas representa o corpo principal da informação original, enquanto a informação passa-altas geralmente representa características que contêm variações muito abruptas [57].

Pavlidis utilizou um modelo linhas deformáveis para representar as assinaturas. Nessa abordagem as assinaturas são modeladas como um conjunto de linhas conectadas. As linhas se mantêm em equilíbrio devido a uma "força de atração" existente entre elas. A força de atração é definida a partir do mapa de gradiente da imagem [58].

Sabourin introduziu o código de sombra (*shadow code*) para extração de características de imagens de assinaturas. Essa técnica se baseia em colocar a imagem sobre um reticulado e rebater sobre os segmentos horizontais e verticais que compõe as células do reticulado, os pixels da assinatura que estejam contidos na célula correspondente [59].

4.5.3 Reconhecimento

O processo de reconhecimento consiste em classificar, através do seu vetor de características, se a assinatura é verdadeira ou falsa. Ou seja, nos deparamos com um problema de classificação de apenas dois padrões, um deles sendo as assinaturas verdadeiras e o outro, qualquer conjunto que não tenha as características da assinatura genuína.

No caso ideal, as assinaturas verdadeiras e as falsas estariam muito bem definidas e poderiam ser separadas em duas classes. Na prática, devido à variabilidade que existe numa mesma assinatura, assim como a habilidade que pessoas têm de falsificar assinaturas, os vetores de características das assinaturas verdadeiras e falsas podem chegar a valores muito próximos. Assim sendo, dependendo do limiar que se escolha para a classificação das assinaturas, poderá ocorrer um erro de classificação.

Na última década, as pesquisas que utilizam técnicas de classificação via redes neurais se desenvolveram bastante. A maioria desses estudos utilizam o classificador de percéptrons multicamada [60] [61]. Por outro lado, abordagens tradicionais como classificação utilizando o classificador de distância mínima [62], vizinhos mais próximos [63] e programação dinâmica [64], também vem sendo adotadas. Abordagens baseadas em classificadores multi-especialistas [65] e modelos ocultos de Markov tem sido recentemente descritos na literatura. A principal diferença entre esses estudos se encontra nas características utilizadas para representar uma dada assinatura [66].

A tabela 4.1 mostra os resultados obtidos por vários pesquisadores na área de verificação de assinaturas estáticas frente a falsificações simples ou aleatórias [67].

Tabela 4.1: Resultados obtidos em verificação de assinatura estáticas

Pesquisador	EFR_0 (%)	EFA_0 (%)	Erros iguais (%)
Chuang (1977)	20.00	20.00	-
Nagel (1977)	12.00	0.00	-
Ammar (1986)	6.00	4.00	-
Wilkinson (1990)	-	-	7.00
Pender (1991)	-	-	3.00
Sabourin(1993)	16.33	5.32	-
Qi (1994)	0.00	0.00	0.00
Cardot (1994)	2.00	4.00	-
Yoshimura (1994)	-	-	13.00
Martins (1995)	21.00	29.00	-
Qi - Hunt (1995)	4.00	1.30	
Murshed(1995)	9.75	7.27	-
Bajaj (1996)	1.00	3.00	-
Lizárraga (1996)	-	-	3.00
Huang(1997)	6.53	0.13	-
Abu-Rezq (1999)	0.00	3.00	-
Cordela (1999)	5.71	0.03	-
Deng (1999)	0.00	3.30	-

- = dado não disponível.

CAPÍTULO 5

VERIFICAÇÃO DE ASSINATURAS

Neste capítulo discutiremos primeiramente a aquisição das assinatura que fazem parte da nossa base de dados. A seguir nos concentraremos em apresentar os diferentes tipos de características que serão utilizados em nosso sistema de verificação. A seguir mostraremos o sistema de verificação de assinaturas proposto detalhando os estágios do modelo multi-especialista que foi implementado. Finalmente, faremos uma discussão sobre os resultados obtidos.

5.1 Aquisição de Assinaturas

A definição de uma base de dados que seja representativa no universo de assinaturas que podem ser encontradas em um problema real de reconhecimento é um requisito fundamental para a avaliação experimental das técnicas propostas neste trabalho. Além disso, a construção de tal base assume uma importância ampla à medida que se está servindo e servirá como referência para muitos outros trabalhos relacionados à área de verificação de assinaturas.

Em muitos problemas de estatísticas, técnicas de amostragem são utilizadas para extrair um subconjunto de elementos (amostra) de uma população que seja representativo, no sentido de que propriedades obtidas a partir da observação de certas variáveis ou características da amostra possam ser extrapoladas para a população como um todo.

Para se fazer tais inferências, é interessante selecionar um método de amostragem apropriado, que leve em conta a possibilidade de todos os elementos da população fazerem parte da amostra, ou então, de apenas alguns desses elementos fazerem parte dela. Se todos os componentes da população tiverem igual probabilidade de participar da amostra, diz-se que o método usado é o da amostragem causal, se esse não for o caso, fala-se de amostragem não causal.

Vários critérios podem ser utilizados num método de amostragem não causal para garantir que uma amostra não seja tendenciosa ou não representativa da população. No entanto, quando esse tipo de informação não está disponível ou é difícil de ser obtida, a adoção de tais critérios torna-se proibitiva. Nessa situação, uma opção seria obter uma amostra de conveniência, ou seja, uma amostra que esteja naturalmente disponível e que não dependa de critérios difíceis para a seleção de seus elementos. Assim, o espaço amostral poderia ser o local de trabalho, a universidade, uma cidade, etc..

Em virtude da dificuldade de acesso à população envolvida com o problema de verificação de assinaturas, adotou-se um método de amostragem de conveniência para obtenção das amostras da base de dados de assinaturas. A Faculdade de Engenharia Elétrica e de Computação da Universidade Estadual de Campinas foi o local de conveniência escolhido para a coleta das amostras.

Diante das decisões tomadas, se faz necessário fornecer respostas a algumas perguntas importantes:

(1) Que tipos de objetos deverão constituir a base de dados de assinaturas ?
(2) Qual deverá ser a quantidade de classes (autores ou escritores) ?
(3) Qual deverá ser o tamanho da amostra (nº de elementos do subconjunto) ?

A resposta à pergunta 1 é direta: os objetos da base de dados são imagens digitalizadas de assinaturas juntamente com as características de interesse extraída dessas imagens. A fim de permitir a avaliação de sistemas de verificação, além das assinaturas genuínas (verdadeiras) de cada escritor, deverão ser incluídas algumas falsificações para essas assinaturas.

Durante a realização dos experimentos, um subconjunto das assinaturas verdadeiras de um autor é utilizado como conjunto de referência para o mesmo e as assinaturas verdadeiras restantes junto com as falsas constituiriam o conjunto de teste.

É possível argumentar que assinaturas falsas também poderiam ser utilizadas na base de referência, com o objetivo de treinar os classificadores com contra-exemplos de assinaturas verdadeiras. Essa abordagem seria bastante útil caso não existisse o difícil problema de como saber antecipadamente a que tipos de falsificações um determinado autor poderia estar sujeito.

Respondendo à pergunta 2, a definição da quantidade ideal de classes a serem consideradas em uma amostra, mesmo em estatística, não segue uma regra muito precisa. Nesse contexto, costuma-se falar de conjunto amostral pequeno ou conjunto de amostral grande.

Em problemas de classificação envolvendo uma população infinita, uma amostra contendo menos de 50 padrões com variáveis de distribuição de probabilidade é considerada pequena [68]. Caso contrário, o tamanho da amostra é dito ser significativo a um certo nível que pode ser calculado. A partir desse elemento, quanto maior o tamanho da amostra, melhor será sua representatividade, desde que se tenha adotado critérios de amostragem adequados. Dentro do escopo deste trabalho e do tempo disponível, escolheu-se 50 como o número total de classes constituindo a base de dados.

A questão 3 trata da tamanho da amostra ou número de elementos por classe. Analisando a maioria dos problemas de verificação de assinaturas, pode-se identificar um certo limite prático do número de assinaturas verdadeiras utilizadas como referência. Esse limite está relacionado com a habilidade que o ser humano utiliza para reconhecer assinaturas. Num sistema bancário, ou em um sistema de reconhecimento de firmas em cartório, por exemplo, uma amostra de teste é conferida com base em três assinaturas de referência. Como em nosso trabalho, estamos tentando reproduzir em computador essa habilidade humana, não seria interessante extrapolar esse limite. Dessa forma, escolheu-se o valor três como sendo o número máximo de assinaturas verdadeiras utilizadas no conjunto de referência para cada autor.

Vale salientar que nos problemas de reconhecimento de padrões, o número de padrões utilizados como referência está estreitamente relacionado com o domínio da aplicação. No caso do reconhecimento de caracteres, por exemplo, certas aplicações no reconhecimento de escrita manuscrita podem requerer a utilização de milhares de padrões como referência para uma dada classe [69]. Assim, não descartamos a possibilidade de que em alguma aplicação possa ser requerido um número muito maior de assinaturas para compor o conjunto de referência.

Com respeito ao número de assinaturas verdadeiras e falsas utilizadas para teste, em função do tempo disponível para a realização deste trabalho e das dificuldade em se encontrar voluntários dispostos a assinarem dezenas de vezes sobre uma folha de papel, e outros mais raros, com

habilidade e disposição para imitarem ("falsificarem") centenas de assinaturas, nossa base de dados consta de um total de 3350 imagens.

As imagens das assinaturas estão divididas em três grupos: as verdadeiras, as falsificações habilidosas e as falsificações aleatórias.

O grupo de assinaturas verdadeiras totaliza 2500 imagens. Essas assinaturas foram obtidas junto a cinqüenta pessoas, sendo que cada uma delas contribuiu com 50 assinaturas. As assinaturas verdadeiras foram coletadas num período de seis meses.

Para 25 tipos de assinaturas verdadeiras foram adquiridas 30 falsificações habilidosas. Dessa forma o grupo de falsificações habilidosas consta de 750 imitações.

O grupo das falsificações aleatórias é formado por 100 assinaturas de 50 pessoas diferentes.

Assim, o número de assinaturas adquiridas para os testes do sistema é de 2500 verdadeiras e de 850 falsas, totalizando 3350 assinaturas

5.1.1 Equipamento e Coleta de Assinaturas

O formato geral do equipamento utilizado para a execução deste trabalho foram um computador pessoal e um *scanner* de mesa. O *scanner* de mesa utilizado foi o HP Jetscan II. O software que gerencia o *scanner* é o "DeskScan" e permite gerar imagens digitais em formatos de arquivo tipo PCX, JPEG, GIF e BMP. A resolução utilizada para a digitalização das assinatura é de 200 pontos por polegada.

O microcomputador utilizado foi um IBM-PC Pentium/200 Mhz, com 48 Mbytes de RAM e um monitor de vídeo com resolução de 800 x 600 pixels.

Todas as assinaturas coletadas ficam restritas a uma área retangular de 10 centímetros de comprimento por cinco centímetros de altura, que por sua vez são os parâmetros que definimos para o *scanner* fazer a digitalização das mesmas. Esses parâmetros foram estipulados empiricamente, visto que a totalidade das assinaturas coletadas pôde ser enquadrada utilizando-se essa área sem nenhuma perda de informação. A utilização de 200 pontos por polegada para a digitalização de uma área de 10 cm por 5 cm gera imagens digitais de 800 pixels por 400 pixels. A figura 5.1 mostra um exemplo de assinatura coletada.

Outro fato importante durante o processo de coleta das assinaturas foi a utilização de uma caneta com tinta de cor preta e diâmetro de ponta 0.5 mm. Esse detalhe se fez necessário para que

na digitalização da imagem conseguíssemos maior contraste entre a folha branca de papel e a assinatura, obtendo assim melhor qualidade na imagem digitalizada.

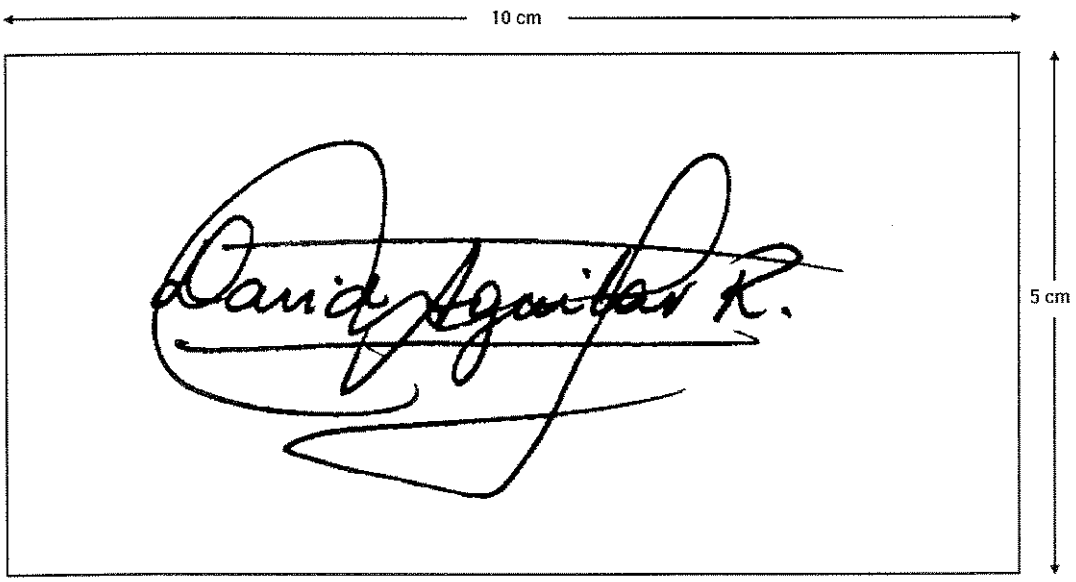


Figura 5.1: Exemplo de uma assinatura.

5.2 Extração de Características

Nesta seção apresentamos primeiramente as técnicas de pré-processamento de imagens que foram utilizadas nas assinaturas de entrada. Segundo, descreveremos as características extraídas das imagens previamente processadas que serão utilizadas no sistema de verificação.

5.2.1. Pré-processamento da Imagem da Assinatura

Com o objetivo de tratar as imagens e deixá-las num formato que permita fazer a extração de características que minimize a variabilidade intra-classe e maximize a variabilidade inter-classe, dividimos o pré-processamento de imagens em três etapas. A primeira trata do corte de traços estilísticos, a segunda da normalização de tamanho e a terceira da divisão da imagem em quadros.

A figura 5.2 mostra um diagrama com as três etapas que compõem esse processo.

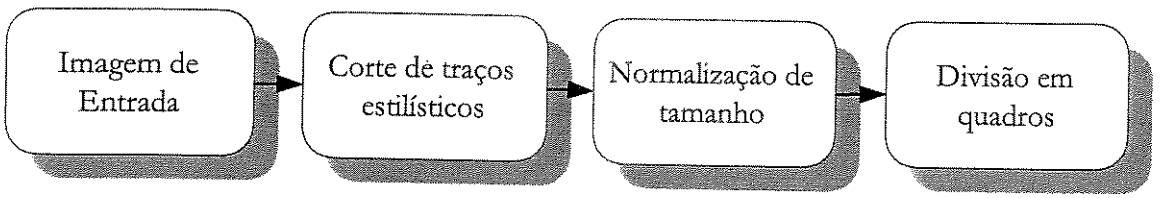


Figura 5.2: Diagrama de blocos das etapas de pré-processamento.

5.2.1.1 Corte de traços estilísticos

As assinaturas manuscritas têm menos consistência no seu início e final. Isto significa que, ao começarmos a assinar, os primeiros traços tendem a variar bastante, o mesmo acontecendo nos últimos. Constatamos também que, para aquelas assinaturas que representam um sinal gráfico, muitos dos traços que se prolongam para cima e para baixo da linha de base da assinatura costumam possuir um comprimento muito variável. Na figura 5.3 mostramos uma assinatura que apresenta algumas dessas características.

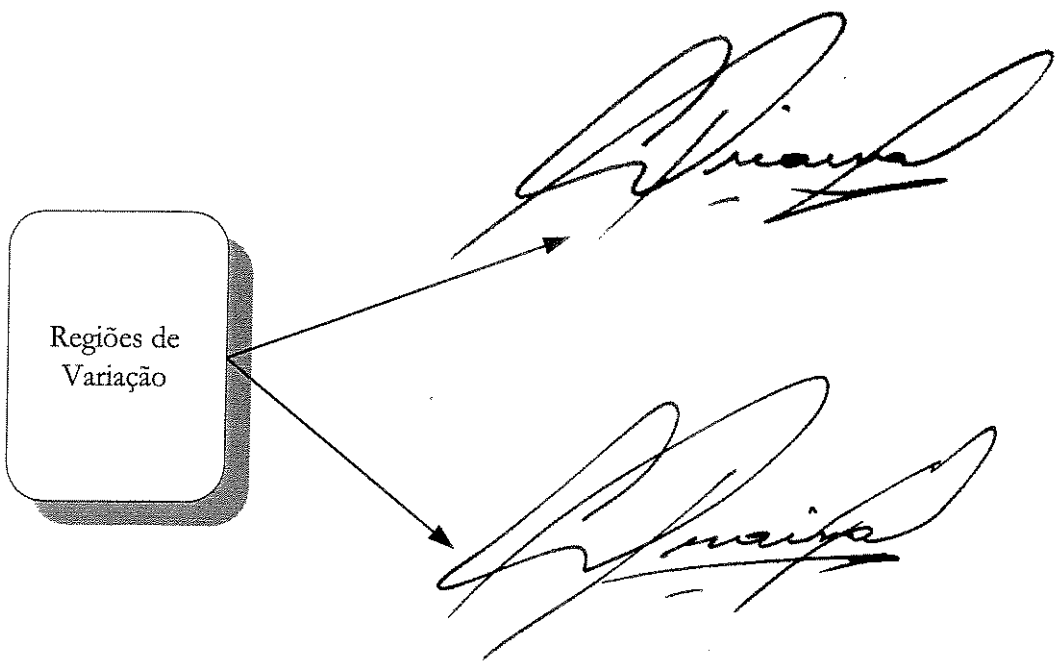


Figura 5.3: Regiões de variação de uma assinatura.

Levando em consideração esses problemas, optamos por fazer um tratamento na imagem de forma a tentar minimizar a influência desses traços.

O algoritmo para o corte dos traços estilísticos é feito da seguinte forma:

Primeiramente são calculadas as projeções nos eixos verticais e horizontais da imagem definidas por:

$$P_H[x] = \sum_{y=0}^{N-1} f(x,y) \qquad \text{para } x = 0, 1, ..., \text{M} - 1 \tag{5.1}$$

$$P_V[y] = \sum_{x=0}^{M-1} f(x,y) \qquad \text{para } y = 0, 1, ..., \text{N} - 1 \tag{5.2}$$

onde:

$P_H[x]$ = vetor de projeção no eixo horizontal.

$P_V[y]$ = vetor de projeção no eixo vertical.

$f(x,y) \in \{0,1\}$: nível do pixel na x-ésima coluna e y-ésima linha.

M = largura da imagem da assinatura.

N = altura da imagem da assinatura.

Uma representação gráfica da projeções $P_H[x]$ e $P_V[y]$ para uma dada imagem de assinatura é mostrada na figura 5.4.

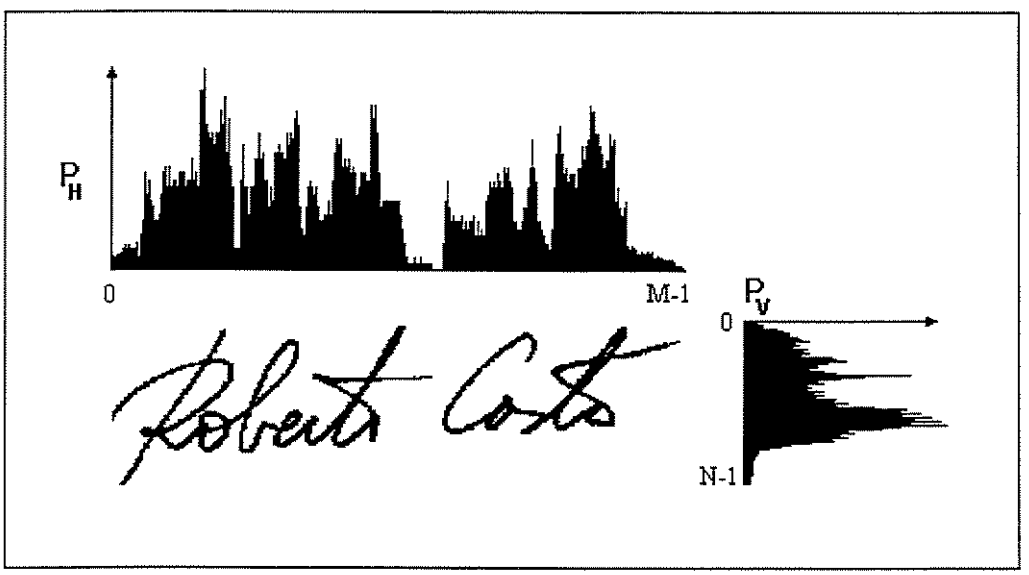


Figura 5.4: Exemplo das projeções horizontais e verticais.

Com a ajuda das projeções encontradas, são calculadas as coordenadas que definem o enquadramento da imagem. Esse enquadramento faz com que sejam cortados os chamados traços estilísticos pertencentes à assinatura.

As coordenadas são compostas por quatro valores que chamaremos x_ini, x_fin, y_ini e y_fin. A seguir, mostramos como determinar cada um desses valores:

$$\text{x\_ini} = x \text{ para o primeiro } P_H[x] = 10 \text{ dado } x = 0, 1, \ldots N-1 \tag{5.3}$$

$$\text{x\_fin} = x \text{ para o primeiro } P_H[x] = 10 \text{ dado } x = N\text{-}1, N\text{-}2, \ldots 0 \tag{5.4}$$

$$\text{y\_ini} = x \text{ para o primeiro } P_V[y] = 10 \text{ dado } y = 0, 1, \ldots M-1 \tag{5.5}$$

$$\text{y\_fin} = x \text{ para o primeiro } P_V[y] = 10 \text{ dado } y = M\text{-}1, M\text{-}2, \ldots 0 \tag{5.6}$$

A figura 5.5 mostra a região obtida pelo enquadramento através das coordenadas das projeções dos eixos vertical e horizontal.

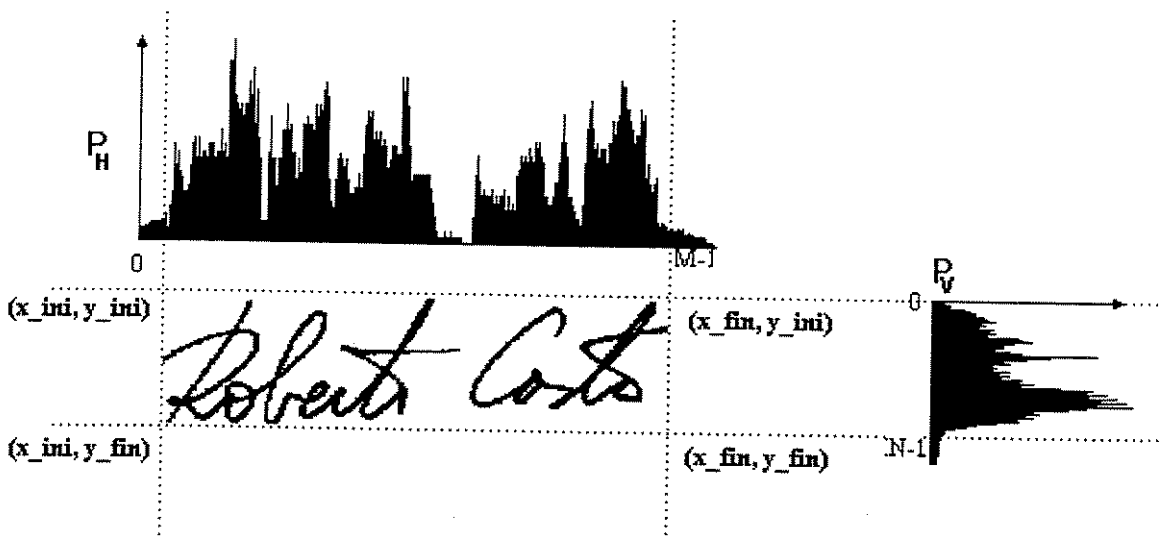


Figura 5.5: Imagem de assinatura após enquadramento e retirada dos traços estilísticos.

5.2.1.2 Normalização de tamanho

Constatamos que em uma escala de resolução muito baixa todas as assinaturas são semelhantes. Por outro lado, em escalas muito altas, assinaturas de um mesmo indivíduo podem apresentar variações bastante significativas. Portanto, não podemos trabalhar em nenhum desses dois extremos. Pois, se a escala de resolução é baixa, o sistema tende a errar pela falta de poder de

discriminação. Em contrapartida, numa escala muito detalhada, o sistema pode rejeitar assinaturas genuínas pela variabilidade existente entre elas.

Utilizando o conceito de multiresolução [70] decidimos adotar 4 escalas de resolução. As escalas a que nos referimos estão relacionadas com a normalização no número de pixels no eixo horizontal da imagem. Com relação aos pixels no eixo vertical, esses mantêm o *aspect ratio* com o eixo horizontal. Dessa forma, passamos a denominar de escala ao número de pixels que uma imagem foi normalizada no eixo horizontal. Os quatro valores de escala escolhidos para essa normalização foram de 64 pixels, 128 pixels, 256 pixels e 512 pixels.

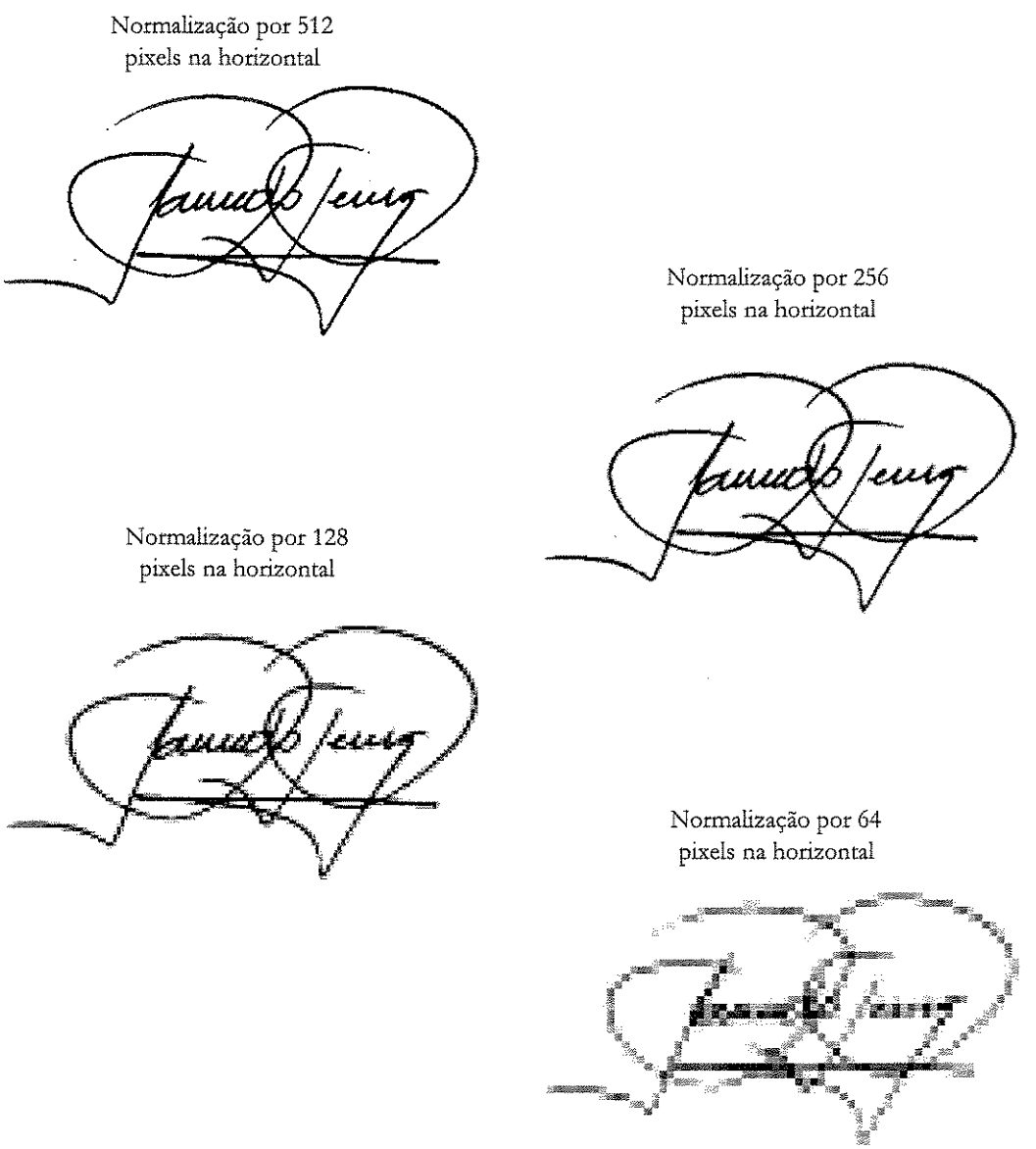


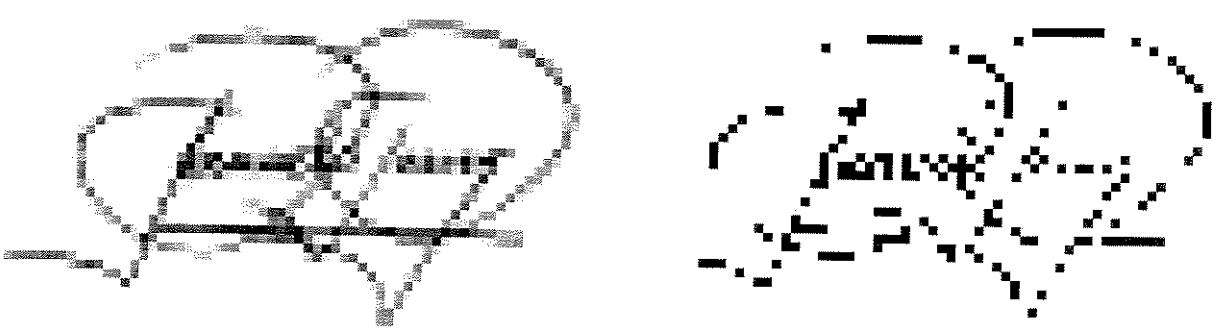
Figura 5.6: Imagem de uma assinatura em diferentes escalas.

A idéia básica da abordagem em várias escalas é representar a sensação que uma pessoa tem ao começar a visualizar um objeto que inicialmente está longe, por tanto com poucos detalhes (escala 64), e ir aumentando a percepção de seus detalhes à medida que vai se aproximando, por tanto com maior resolução (escala 512).

A figura 5.6 apresenta uma mesma assinatura em várias escalas, mostrando a perda da qualidade da imagem à medida em que a resolução vai diminuindo.

Vale ressaltar que no processo para diminuir a resolução de uma imagem, deve ser feito uma sub-amostragem dos pixels que a compõe, e a partir dos pixels sub-amostrados gerar a nova imagem. No caso de querermos aumentar a resolução, deve-se realizar um processo de réplica de pixels. As imagens de entrada de nosso sistema são imagens binárias digitalizadas originalmente com 200 pontos por polegada. Durante o processo de mudança de escala, primeiramente é passado um filtro passa-baixas sobre a imagem da assinatura fazendo com que a imagem que inicialmente era binária se transforme em uma imagem em níveis de cinza. Essa imagem tem como característica ser uma versão desfocada da imagem original. Sobre a imagem de níveis de cinza é feita a sub-amostragem ou réplica de pixels.

O processo anteriormente descrito se faz necessário para que não ocorra perda de informação relevante, principalmente na imagem resultante da sub-amostragem. A figura 5.7 (a) apresenta uma assinatura na escala de valor 64 que utilizou o processo de filtragem passa-baixas e (b) uma assinatura que não foi filtrada.



(a) (b)

Figura 5.7: Imagem de assinaturas (a) filtrada e sub-amostrada, (b) sub-amostragem sem filtragem.

A seguir a imagem em níveis de cinza é novamente binarizada através de um limiar para passar para o próxima etapa de pré-processamento.

5.2.1.3 Divisão em quadros

A divisão da imagem da assinatura em quadros tem como intuito repartir a imagem em porções menores. Cada uma dessas porções poderá depois ser utilizada no processo de extração de características para gerar vetores que carreguem consigo informações locais da imagem.

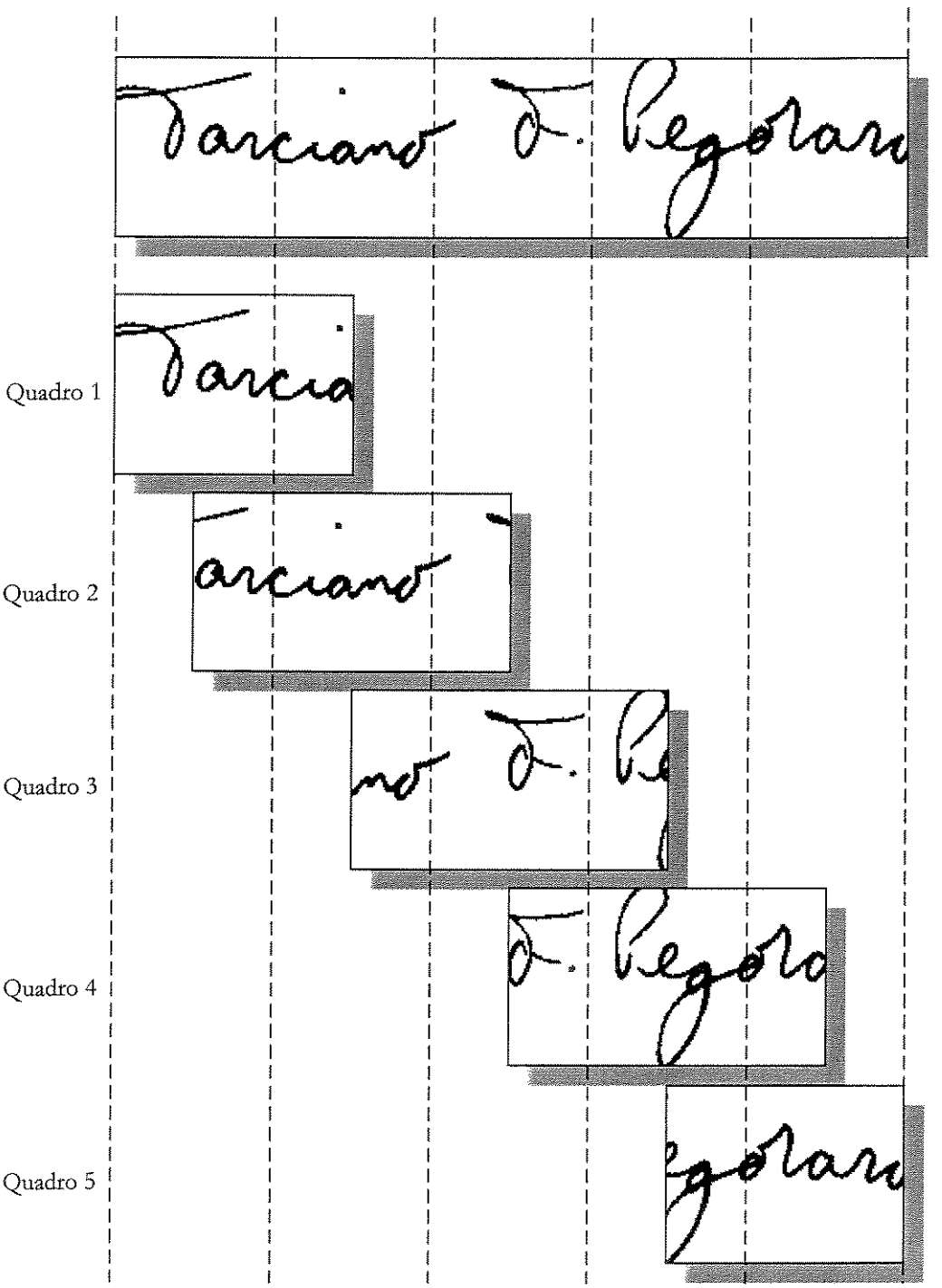


Figura 5.8: Divisão de uma assinatura em cinco quadros.

A divisão da imagem é feita apenas no sentido vertical e para este trabalho optamos em fazer a divisão das assinaturas em 1 quadro (sem divisão), 3 quadros, 5 quadros e 10 quadros.

Um atributo importante nesse tipo de divisão é que os quadros possuem uma sobreposição de 50% da sua área com os quadros anterior e posterior. A figura 5.8 exemplifica a divisão de uma assinatura em 5 quadros, mostrando a sobreposição entre os mesmos.

5.2.1.4 Morfologia matemática

Dois dos vetores de características que serão apresentados nas seções seguintes se servem da morfologia matemática para extrair características da imagem. Assim sendo, optamos por fazer uma breve introdução sobre a morfologia matemática a fim de facilitar a compreensão dos termos e técnicas utilizadas.

A palavra morfologia normalmente denota uma área da biologia que trata com a forma e a estrutura de animais e plantas. Usamos a mesma palavra no contexto de morfologia matemática como sendo uma ferramenta para a extração de componentes de imagens que sejam úteis na representação e descrição da forma de uma imagem. A linguagem da morfologia matemática é a teoria de conjuntos. Os conjuntos em morfologia matemática representam as formas dos objetos em uma imagem. Por exemplo, o conjunto de todos os pixels pretos em uma imagem binária é uma descrição completa dessa imagem. Em imagens binárias, os conjuntos em questão são membros do espaço bidimensional de números inteiros Z^2 em que cada elemento do conjunto é um vetor bidimensional cujas coordenadas são as coordenadas (x, y) dos pixels pretos da imagem [71].

Algumas definições básicas:

Sejam A e B conjuntos em Z^2 com componentes $a=(a_1,a_2)$ e $b=(b_1,b_2)$, respectivamente. A translação de A por $x=(x_1,x_2)$, denotada por $(A)_x$, é definida como:

$$(A)_x = \{b \mid b = a + x, \text{ para } a \in A\} \tag{5.7}$$

A reflexão de B, denotado por $\hat{B}$, é definida como:

$$\hat{B} = \{x \mid x = -b, \text{ para } b \in B\} \tag{5.8}$$

O complemento do conjunto A é definido como

$$A^C = \{x \mid x \notin A\} \tag{5.9}$$

Finalmente a diferença entre dois conjunto A e B, denotada por $A-B$, é definida como

$$A-B = \{x \mid x \in A, x \notin B\} \quad = \quad A \cap B^c \tag{5.10}$$

Dilatação:

Tomando-se A e B como conjuntos de Z^2 e $\varnothing$ como conjunto vazio, define-se dilatação de A por B, denotada por $A \oplus B$, como

$$A \oplus B = \left\{ x \mid \left(\hat{B}\right)_x \cap A \neq \varnothing \right\} \tag{5.11}$$

O conjunto B é normalmente chamado de *elemento estruturante.*

Dessa forma, o processo de dilatação começa na obtenção da reflexão do elemento estruturante B em torno de sua origem. Seguido da translação dessa reflexão por x. A dilatação A por B é então o conjunto de todos os deslocamentos x tais que $\hat{B}$ e A se sobreponham em pelo menos um elemento não nulo.

Erosão:

Para conjuntos A e B em Z^2, a erosão de A por B, denotada por $A \Theta B$, como:

$$A \Theta B = \{x \mid (B)_x \subseteq A\} \tag{5.12}$$

O que significa que a erosão de A por B é o conjunto de todos os pontos x tais que B, quando transladado por x, fique contido em A

Extração de Contornos:

O contorno de um conjunto A, denotada por $\beta(A)$, pode ser obtida através da dilatação de A por B, seguida da diferença entre sua dilatação e A. Ou seja,

$$\beta(A) = (A \oplus B) - A \tag{5.13}$$

onde B é um elemento estruturante adequado.

Elementos estruturantes:

Elementos estruturantes (EEs) são na prática, pequenas imagens utilizadas pelos operadores de morfologia matemática para desempenhar o papel de extratores de características da imagem. A utilização de tipos específicos de EEs é o que nos permite extrair consistentemente uma determinada característica de uma imagem.

Cada elemento estruturante (EE) possui uma coordenada de origem, a qual serve como ponto de referência durante sua utilização numa operação. Dependendo dessa origem, os EEs podem ser classificados como simétricos ou não-simétricos.

A figura 5.9 mostra alguns elementos estruturantes clássicos.

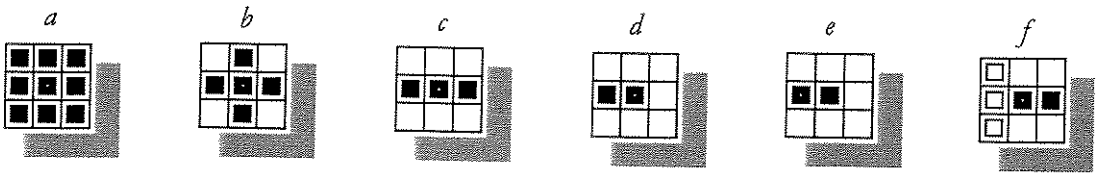


Figura 5.9: Exemplos de elementos estruturantes.

Na notação utilizada cada um dos elementos estruturantes está colocado dentro de uma grade 3 x 3 para facilitar sua representação. Os quadrados pretos dentro da grade indicam a presença de pixels pretos, enquanto os quadrados brancos representam pixels brancos e os espaços vazios da grade representam o estado irrelevante (*don't care state*). Temos ainda que a coordenada (0,0) dessas imagens se encontra representada pelo ponto branco dentro de um dos quadrados pretos.

Na figura 5.9 os elementos *a*, *b*, e *c* são exemplos de elementos simétricos, isto é, se fizermos uma reflexão dessas imagens sobre suas origens, elas continuarão as mesmas. Em contrapartida, os elementos *d*, *e*, e *f* são elementos não-simétricos, isto é, se fizermos uma reflexão dessas imagens sobre suas origens, obteremos imagens diferentes das originais.

5.2.2 Características

Como já mencionado anteriormente, a escolha de um conjunto de características que consiga representar de forma satisfatória os padrões de entrada que desejamos classificar é fundamental para a resolução de um problema de reconhecimento de padrões.

Neste trabalho optamos por representar a imagem da assinatura através de sete vetores de características. Cada um desses vetores se baseia nos seguintes atributos da imagem.

1. Projeção Horizontal.
2. Projeção Vertical.
3. Momentos de Hu.
4. Momentos de Tsirikolias-Mertzios.
5. Curtose e Assimetria.
6. Inclinação dos contornos das assinaturas dilatadas.
7. Inclinação dos traços das assinaturas.

A seguir descreveremos cada um dos vetores de características.

5.2.2.1 Projeção Horizontal

O vetor de projeção horizontal está definido na equação (5.1). Com base nesse vetor são extraídos quatro parâmetros:

- O valor máximo do vetor.
- A posição do valor máximo.
- A média do vetor.
- A variância do vetor.

Assim, o vetor de características baseado na projeção horizontal, que passaremos a chamar de vetor de características 1, possuirá quatro elementos por quadro. Isto é, se a imagem for dividida em apenas um quadro (imagem original), o vetor terá quatro elementos. De maneira geral, se a imagem for dividida em q quadros, onde $q = \{1, 3, 5, 10\}$, o número de elementos do vetor será $q * 4$.

Para obter o desempenho que a característica 1 teria sobre a base de dados, foi definido uma seqüência de passos que denominamos de procedimento para análise de desempenho de vetores de características. Esse procedimento sobre o vetor de características 1, é descrito a seguir:

1. Escolher três assinaturas verdadeiras de cada indivíduo. A essas três assinaturas passaremos a chamar de conjunto de treinamento.
2. Para cada uma das assinaturas do conjunto de treinamento, extrair o vetor de características 1 para 1, 3, 5 e 10 quadros nas escalas 64, 128, 256 e 512.
3. Gerar o vetor de características 1 médio para 1, 3, 5 e 10 quadros nas escalas 64, 128, 256 e 512.

   A média de cada elemento que compõe esse vetor é calculado pela equação (3.8).
4. Gerar o vetor de variâncias médio da característica 1 para 1, 3, 5, e 10 quadros nas escalas 64, 128, 256 e 512.

   A variância de cada elemento que compõe esse vetor é calculado pela equação (3.9).
5. Extrair o vetor de características 1 das 47 assinaturas verdadeiras restantes que não fazem parte do conjunto de treinamento para 1, 3, 5 e 10 quadros nas escalas 64, 128, 256 e 512.
6. Extrair o vetor de características 1 das 100 assinaturas falsas aleatória que fazem parte da base de dados para 1, 3, 5 e 10 quadros nas escalas 64, 128, 256 e 512.
7. Calcular as distâncias padrões, utilizando a equação (3.12), entre o vetor de características 1 médio e cada vetor de características 1 das 47 assinaturas verdadeiras para 1, 3, 5 e 10 quadros nas escalas 64, 128, 256, 512.
8. Calcular as distâncias padrões, utilizando a equação (3.12), entre o vetor de características 1 médio e cada vetor de características 1 das 100 assinaturas falsas aleatórias para 1, 3, 5 e 10 quadros nas escalas 64, 128, 256 e 512.
9. Variando o valor de limiar sobre o valor das distâncias encontradas junto às 47 assinaturas verdadeiras, encontrar a curva de falsa rejeição através da equação (3.13).
10. Variando o valor de limiar sobre o valor das distâncias encontradas junto às 100 assinaturas falsas aleatórias, encontrar a curva de falsa aceitação através da equação (3.13).
11. Determinar se existe um valor diferente de zero, em que o erro de falsa rejeição é igual ao erro de falsa aceitação.

11.1 Em caso afirmativo, determinar o valor do erro de falsa rejeição quando o erro de falsa aceitação é nulo (EFR_0). A seguir determinar o valor do erro de falsa aceitação quando o erro de falsa rejeição é nulo (EFA_0).

11.2 Em caso negativo, EFR_0 é igual a zero, EFA_0 é igual a zero e a taxa de erros iguais é igual a zero.

12. Armazenar os valores de EFR_0, EFA_0 e taxa de erros iguais e refazer os passos de 1 a 12 seis vezes. No passo 1 utilizar outras 3 assinaturas verdadeiras que não tenha sido previamente utilizadas como conjunto de treinamento.
13. Tirar a média dos valores EFR_0, EFA_0 e taxa de erros iguais armazenados nos seis experimentos realizados para 1, 3, 5 e 10 quadros nas escalas 64, 128, 256, 512.

A tabela 5.1 apresenta a síntese dos resultados obtidos pela característica 1 nos experimentos realizamos para 1, 3, 5, e 10 quadros nas escalas 64, 128, 256, 512.

Tabela 5.1 : Taxas médias de erros para o vetor de característica 1

Escala	**Quadros**	**EFR_0 (%)**	**EFA_0 (%)**	**Erros Iguais (%)**
64	1	28.24	22.45	7.46
	3	19.65	18.94	7.02
	5	19.08	20.55	8.14
	10	18.34	19.04	6.35
128	1	27.39	24.16	7.23
	3	21.62	21.79	6.72
	5	17.30	21.58	8.31
	10	21.02	27.10	8.81
256	1	29.02	25.35	8.34
	3	23.15	20.81	7.24
	5	20.02	23.93	7.45
	10	21.10	25.12	8.79
512	1	27.58	28.29	8.57
	3	22.08	21.38	7.38
	5	18.01	25.18	8.50
	10	18.74	28.83	9.55

5.2.2.2 Projeção Vertical

O vetor de projeção vertical está definido na equação (5.2). Com base nesse vetor são extraídos quatro parâmetros:

- O valor máximo do vetor.
- A posição do valor máximo.
- A média do vetor.
- A variância do vetor.

Assim, o vetor de características baseado na projeção vertical, que passaremos a chamar de vetor de características 2, possui quatro elementos por quadro. Para obter o desempenho que a característica 2 teria sobre a base de dados, foi utilizado o procedimento para análise de desempenho dos vetores de características. A síntese dos resultados obtidos por esse procedimento sobre o vetor de características 2 pode ser visto na tabela 5.2.

Tabela 5.2: Taxas médias de erros para o vetor de características 2

Escala	Quadros	EFR_0 (%)	EFA_0 (%)	Erros Iguais (%)
64	1	34.03	14.51	6.06
	3	27.04	14.97	6.36
	5	25.15	22.49	8.64
	10	31.16	47.18	13.22
128	1	31.53	13.92	7.18
	3	22.19	15.43	5.27
	5	20.58	18.42	5.74
	10	26.17	32.56	10.90
256	1	30.34	14.60	5.92
	3	21.97	17.34	5.33
	5	20.25	20.30	6.94
	10	22.61	26.59	9.22
512	1	26.49	14.02	5.63
	3	19.41	15.28	4.83
	5	18.91	20.83	6.55
	10	24.91	24.91	8.12

5.2.2.3 Momentos de Hu

O vetor de características que se baseia nos momentos de Hu [72], que passaremos a chamar de vetor de características 3, é composto de sete elementos por quadro.

Diversas técnicas baseadas no conceito de momentos têm sido desenvolvidas para reconhecimento de imagens de objetos, através da extração de características invariantes a escala, posição e orientação [73][74].

Os momentos têm-se apresentado com uma técnica robusta para decomposição de uma imagem de forma arbitrária em um conjunto finito de características, uma vez que a técnica é baseada na aplicação direta de transformações lineares, não havendo a necessidade de heurísticas específicas da aplicação. Em estatística, os momentos são utilizados para caracterizar a distribuição espacial de massa. Considerando que uma imagem pode ser tratada como uma função de distribuição de densidade, é possível aplicar momentos para análise de imagens.

Para uma imagem digital representada como uma matriz bidimensional, o momento de ordem $p+q$ é dado por:

$$m_{pq} = \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} x^p y^q f(x,y), \quad p,q = 0,1,2,...,\infty \tag{5.14}$$

onde M e N são as dimensões horizontal e vertical respectivamente, e $f(x,y)$ é a intensidade (nível de cinza) no ponto (x,y) da imagem.

Os momentos centrais de uma imagem são dados por

$$\mu_{pq} = \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} (x-\bar{x})^p (y-\bar{y})^q f(x,y) \tag{5.15}$$

onde

$$\bar{x} = \frac{m_{10}}{m_{00}}, \quad \bar{y} = \frac{m_{01}}{m_{00}} \tag{5.16}$$

são as coordenadas do centróide ou centro de gravidade da imagem. Esses momentos centrais são invariantes à translação da imagem.

Os momentos centrais normalizados de uma imagem são dados por:

$$\eta_{pq} = \frac{\mu_{pq}}{\mu_{00}^{\gamma}} \tag{5.17}$$

onde

$$\gamma = \frac{p+q}{2} + 1, \quad p+q = 2, 3, \ldots \tag{5.18}$$

Na abordagem que é dada em nosso trabalho, utilizamos os momentos invariantes de Hu baseados em momentos até a terceira ordem. O conjunto dos sete momentos invariantes de terceira ordem e menores como proposto por Hu é dado por:

$$\phi_1 = \eta_{20} - \eta_{02} \tag{5.19}$$

$$\phi_2 = (\eta_{20} - \eta_{02})^2 + 4\eta_{11}^2 \tag{5.20}$$

$$\phi_3 = (\eta_{30} - 3\eta_{12})^2 + (3\eta_{21} - \eta_{03})^2 \tag{5.21}$$

$$\phi_4 = (\eta_{30} + 3\eta_{12})^2 + (\eta_{21} + \eta_{03})^2 \tag{5.22}$$

$$\begin{aligned}\phi_5 = {} & (\eta_{30} - 3\eta_{12})(\eta_{30} + \eta_{12})\left[(\eta_{30} + \eta_{12})^2 - 3(\eta_{21} + \eta_{03})^2\right] \\ & + (3\eta_{21} - \eta_{03})(\eta_{21} + \eta_{03})\left[3(\eta_{30} + \eta_{12})^2 - (\eta_{21} + \eta_{03})^2\right]\end{aligned} \tag{5.23}$$

$$\phi_6 = (\eta_{20} - \eta_{02})\left[(\eta_{30} + \eta_{12})^2 - (\eta_{21} + \eta_{02})^2\right] + 4\eta_{11}(\eta_{30} + \eta_{12})(\eta_{21} + \eta_{03}) \tag{5.24}$$

$$\begin{aligned}\phi_7 = {} & (3\eta_{21} - \eta_{30})(\eta_{30} + \eta_{12})\left[(\eta_{30} + \eta_{12})^2 - 3(\eta_{21} + \eta_{03})^2\right] \\ & + (3\eta_{12} - \eta_{30})(\eta_{21} + \eta_{03})\left[3(\eta_{30} + \eta_{12})^2 - (\eta_{21} + \eta_{03})^2\right]\end{aligned} \tag{5.25}$$

onde η_{pq} é dado pela equação (5.17).

Os sete elementos que compõe o vetor de características 3, por quadro, são $\phi_1, \phi_2, \phi_3, \phi_4, \phi_5, \phi_6$ e ϕ_7, respectivamente.

Para obter o desempenho que a característica 3 teria sobre a base de dados, foi utilizado o procedimento para análise de desempenho de vetores de características. A síntese dos resultados obtidos pelo procedimento sobre o vetor de características 3, pode ser vists na tabela 5.3.

Tabela 5.3: Taxas médias de erros para o vetor de característica 3

Escala	Quadros	EFR_0 (%)	EFA_0 (%)	Erros Iguais (%)
64	1	31.47	19.39	20.38
	3	21.90	16.27	7.45
	5	21.01	16.10	6.48
	10	24.57	37.77	10.88
128	1	36.19	21.43	9.48
	3	25.26	20.74	10.16
	5	21.03	20.44	7.71
	10	27.50	39.01	13.36
256	1	35.92	30.01	9.39
	3	26.25	27.50	8.97
	5	24.73	27.50	9.13
	10	28.72	48.69	14.26
512	1	36.02	35.44	10.79
	3	29.24	35.59	11.25
	5	25.63	33.92	11.11
	10	33.69	56.86	17.34

5.2.2.4 Momentos de Tsirikolias-Mertzios

O vetor de características que se baseia nos momentos de Tsirikolias-Mertzios, que passaremos a chamar de vetor de características 4, é composto de 12 elementos por quadro.

Os momentos de Tsirikolias-Mertzios [75] utilizam uma modificação dos momentos definidos na equação (5.14) os quais passam a ser normalizados em relação a seu desvio padrão. Esses momentos são invariantes à rotação, translação, e tamanho da imagem.

No caso de momento unidimensional, dado H elementos $\alpha_1, \alpha_2, \ldots, \alpha_H$

$$m_k = \frac{1}{H}\sum_{j=1}^{H}\left[\frac{\alpha_j - \overline{\alpha}}{\sigma}\right]^k, \quad k = 1, 2, 3, \ldots \tag{5.26}$$

onde

$$\overline{\alpha} = \frac{1}{H}\sum_{j=1}^{H}\alpha_j \tag{5.27}$$

é a média aritmética e

$$\sigma = \sqrt{\left[\frac{1}{H-1}\sum_{j=1}^{H}(\alpha_j - \overline{\alpha})^2\right]} \tag{5.28}$$

é o desvio padrão.

A forma geral bidimensional dos momentos de Tsirikolias-Mertzios é dada pela equação (5.29).

$$m_{pq} = \frac{1}{MN}\sum_{x=1}^{M}\sum_{y=1}^{N}\left[\frac{x-\overline{x}}{\sigma_x}\right]^p\left[\frac{y-\overline{y}}{\sigma_y}\right]^q f(x,y), \quad p = 0,1,2,\ldots \; q = 0,1,2,\ldots \tag{5.29}$$

onde M e N são as dimensões horizontal e vertical da imagem, $f(x,y)$ é a intensidade no ponto (x,y) na imagem, $\overline{x}$, $\overline{y}$ são as coordenadas do centróide da imagem, e σ_x, σ_y são os desvios padrões da imagem em relação às coordenadas x e y dados por:

$$\sigma_x = \sqrt{\left[\frac{1}{MN}\left(\sum_{x=1}^{M}\sum_{y=1}^{N}(x-\overline{x})^2 f(x,y)\right)\right]} \tag{5.30}$$

$$\sigma_y = \sqrt{\left[\frac{1}{MN}\left(\sum_{x=1}^{M}\sum_{y=1}^{N}(y-\overline{y})^2 f(x,y)\right)\right]} \tag{5.31}$$

A versão simplificada da equação (5.29) para imagens binárias é dada por:

$$m_{pq} = \frac{1}{L}\sum_{i=1}^{N}\left[\frac{x_i - \bar{x}}{\sigma_x}\right]^p\left[\frac{y_i - \bar{y}}{\sigma_y}\right]^q, \quad p = 0,1,2,..., \qquad q = 0,1,2,... \tag{5.32}$$

onde L é o número total de pixels pretos pertencentes a imagem.

Os momentos de Tsirikolias-Mertzios são invariantes em escala e translação. Neste trabalho utilizaremos os momentos m_{30}, m_{40}, m_{50}, m_{60}, m_{70}, m_{80}, m_{03}, m_{04}, m_{05}, m_{06}, m_{07} e m_{08}, que por sua vez, são os 12 elementos que compõe o vetor de características 4 por quadro.

Para obter o desempenho que a característica 4 teria sobre a base de dados, foi utilizado o procedimento para análise de desempenho do vetor de características. A síntese dos resultados obtidos pelo procedimento sobre o vetor de características 4, pode ser vista na tabela 5.4.

Tabela 5.4: Taxas médias de erros para o vetor de características 4

Escala	**Quadros**	**EFR_0 (%)**	**EFA_0 (%)**	**Erros Iguais (%)**
64	1	26.12	25.70	7.20
	3	19.94	31.19	7.55
	5	22.18	43.96	11.06
	10	33.12	66.40	17.40
128	1	24.51	23.14	6.48
	3	17.34	27.45	6.37
	5	18.50	41.90	11.31
	10	34.79	70.30	19.17
256	1	20.74	20.79	5.16
	3	14.66	28.56	5.67
	5	17.99	39.48	8.09
	10	32.98	71.30	18.56
512	1	19.90	18.99	5.55
	3	16.63	29.39	6.10
	5	16.59	37.73	10.14
	10	30.39	68.93	18.29

5.2.2.5 Curtose e Assimetria

O vetor de características que se baseia na curtose e assimetria da distribuição dos pixels da imagem [76] [77], que passaremos a chamar de vetor de características 5, é composto de seis elementos por quadro.

Os primeiros dois elementos do vetor de características 5 são dados por medidas de curtose, as quais expressam o espalhamento da distribuição dos pixels na imagem:

$$K_V = \frac{\mu_4^V}{\left(\mu_2^V\right)^2} \tag{5.33}$$

$$K_H = \frac{\mu_4^H}{\left(\mu_2^H\right)^2} \tag{5.34}$$

onde μ_r é definido como:

$$\mu_r = \sum_i (x_i - \bar{x}) G(i) \tag{5.35}$$

e $G(i)$ pode ser P_H ou P_V como definidos nas equações (5.1) e (5.2). O sobrescrito V e H denotam que as medidas foram derivadas utilizando as projeções vertical e horizontal, respectivamente.

O terceiro e o quarto elementos do vetor de características 5 são dados por medidas de assimetria da distribuição dos pixels da imagem:

$$S_V = \frac{\mu_3^V}{\left(\mu_2^V\right)^{1.5}} \tag{5.36}$$

$$S_H = \frac{\mu_3^H}{\left(\mu_2^H\right)^{1.5}} \tag{5.37}$$

O quinto e sexto elementos do vetor de características 5 são dados por medidas relativas entre curtose e assimetria da distribuição dos pixels da imagem:

$$R_V = \frac{\mu_3^V}{\left(\mu_4^V\right)^{0.75}} \tag{5.38}$$

$$R_H = \frac{\mu_3^H}{\left(\mu_4^H\right)^{0.75}} \tag{5.39}$$

Para obter o desempenho que a característica 5 teria sobre a base de dados, foi utilizado o procedimento para análise de desempenho do vetor de características. A síntese dos resultados obtidos pelo procedimento sobre o vetor de características 5, pode ser visto na tabela 5.5.

Tabela 5.5: Taxas médias de erros para o vetor de características 5

Escala	**Quadros**	**EFR_0** (%)	**EFA_0** (%)	**Erros Iguais** (%)
64	1	78.61	56.21	24.36
	3	52.54	30.48	13.55
	5	39.18	21.13	9.55
	10	18.08	10.21	4.83
128	1	79.94	45.55	18.22
	3	56.64	31.44	13.61
	5	42.33	25.92	12.82
	10	23.71	15.07	7.18
256	1	82.89	39.67	18.43
	3	56.53	30.91	15.06
	5	43.20	32.41	12.80
	10	25.95	19.99	8.99
512	1	83.35	39.19	19.70
	3	58.29	34.23	15.58
	5	44.84	35.30	13.54
	10	28.57	22.88	9.01

5.2.2.6 Inclinação do contorno dilatado da assinatura

O vetor de características que se baseia na inclinação do contorno dilatado da assinatura, que passaremos a chamar de vetor de características 6, é composto de 20 elementos por quadro. A técnica utilizada para fazer extração dos elementos que compõe esse vetor foi a morfologia matemática.

Primeiramente, definimos o elemento estruturante EE-1 como sendo um quadrado de 3 x 3 pixels pretos e de coordenada de origem no seu centro (ver figura 5.10).

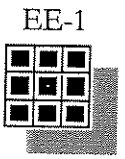


Figura 5.10: Elemento estruturante de 3 x 3 pixels pretos.

Ao realizar a operação de extração de contorno pelos elementos estruturante EE-1 sobre uma imagem qualquer, obteremos uma imagem composta principalmente de linhas de espessura de um pixel. Um exemplo dessa operação pode ser vista na figura 5.11

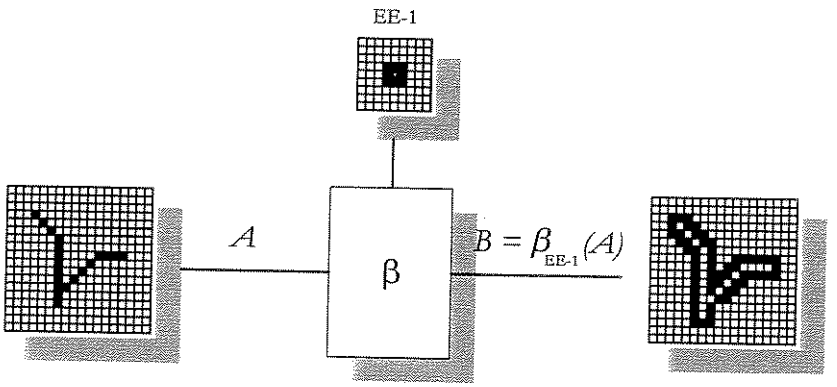


Figura 5.11: Exemplo da aplicação do EE-1 sobre uma imagem.

Para acharmos a inclinação da imagem do contorno, definimos os elementos estruturantes EE-2, EE-3, EE-4, EE-5 como se vê na figura 5.12.

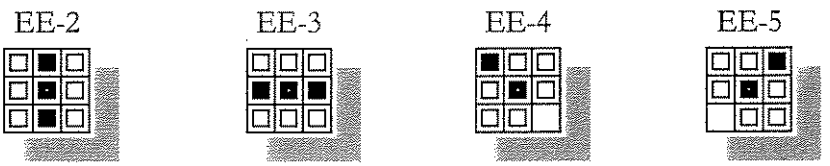


Figura 5.12: Elementos estruturantes para extração da inclinação do contorno de uma imagem.

Pode-se mostrar que utilizando certos EEs numa operação de erosão, é possível detectar a inclinação dos traços que compõe a imagem de uma assinatura [50]. Para apresentar esse fato intuitivamente, nos serviremos da figura 5.13.

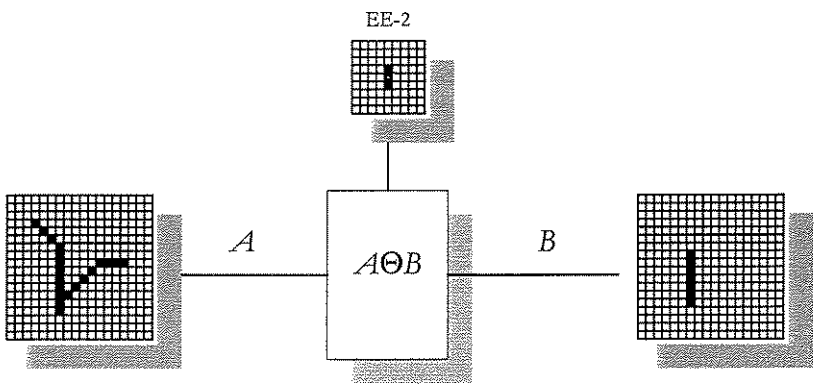


Figura 5.13: Exemplo de uma imagem erodida pelo EE-2

A figura 5.13 mostra a operação de erosão feita pelo EE-2 sobre uma imagem genérica. Nesse exemplo, a imagem resultante consta de 7 pixels pretos. Observa-se claramente que os pixels que fazem parte dos segmentos de reta que não possuem a mesma inclinação que EE-2, não tem nenhum pixel mapeado na imagem *B*. Se utilizarmos outro elementos estruturante, por exemplo EE-3, e fizermos uma nova erosão em *A*, obteremos 2 pixels mapeados em *B*, porém em posições diferentes daquelas obtidas com EE-1. Dessa forma, observa-se que para cada um dos diferentes EEs obteremos uma imagem erodida com um número particular de pixels mapeados.

Assim, para a composição do vetor de características 6 foi utilizado o seguinte procedimento: Para uma imagem de assinatura *A*, tomamos EE-1 e fazemos a operação extração de contorno obtendo *B*. Sobre a imagem resultante *B*, aplicamos a operação de erosão pelos

elementos estruturantes EE-2 a EE-5. O número de pixels mapeados através de cada um desses EEs representa uma característica. A seguir, fazemos uma adição entre as A e B, obtendo a imagem C, que na prática é a imagem da assinatura A dilatada por EE-1. A ilustração desse processo é mostrada na figura 5.14.

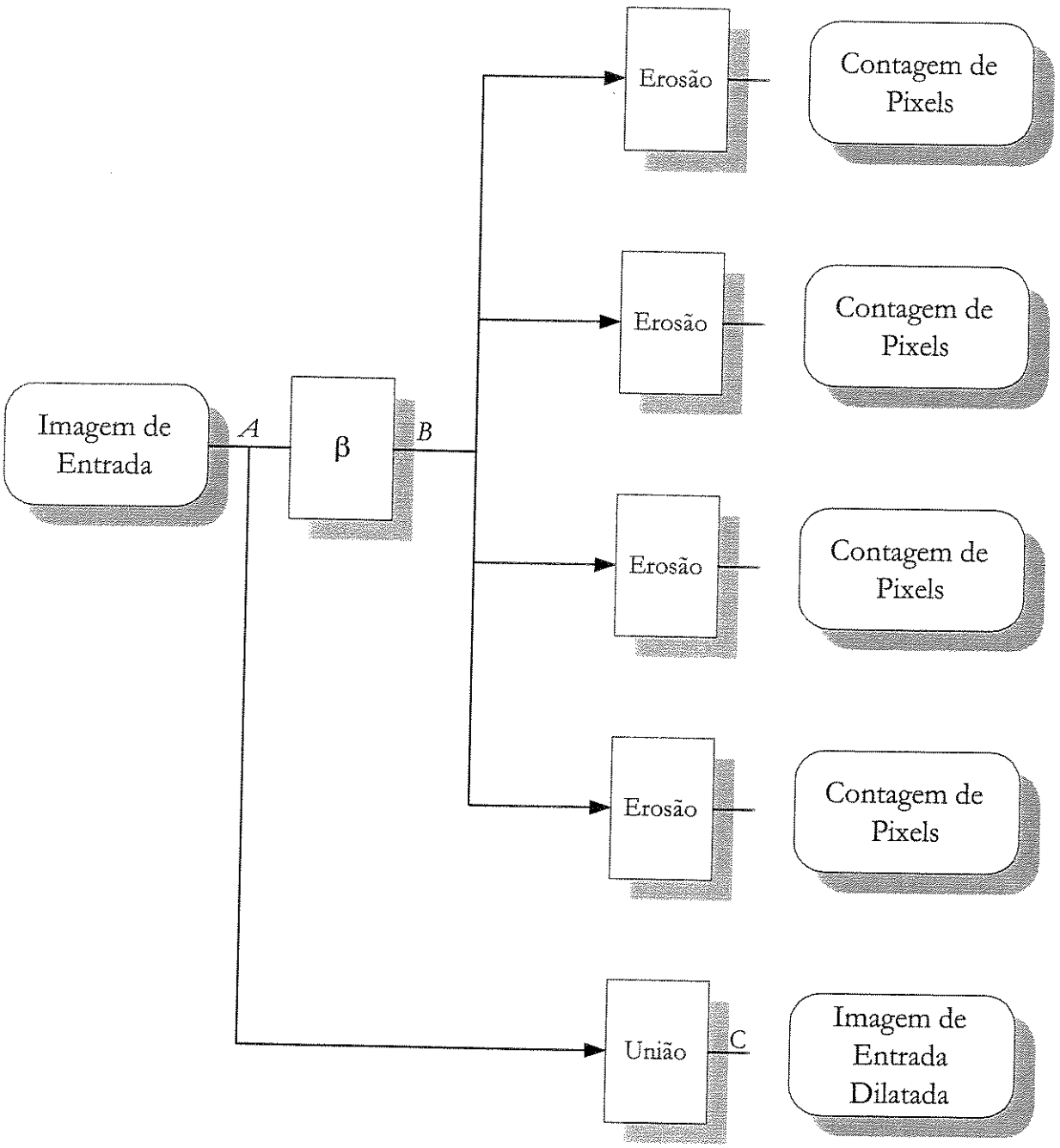


Figura 5.14: Processo da extração das características de inclinação dos contornos da assinatura.

Esse ciclo é repetido quatro vezes mais, com a diferença de que para cada nova repetição, a imagem de entrada passa a ser a imagem dilatada *C* do ciclo anterior. Como esse processo é composto por um total de cinco ciclos, obteremos no final desse processo 20 elementos.

Para obter o desempenho que a característica 6 teria sobre a base de dados, foi utilizado o procedimento para análise de desempenho de vetores de características. A síntese dos resultados obtidos pelo procedimento sobre o vetor de características 6, pode ser visto na tabela 5.6.

Tabela 5.6: Taxas médias de erros para o vetor de característica 6

Escala	Quadros	EFR_0 (%)	EFA_0 (%)	Erros Iguais (%)
64	1	26.04	21.38	7.52
	3	17.15	18.33	8.53
	5	13.20	21.35	6.61
	10	10.32	17.67	4.44
128	1	20.08	12.69	5.26
	3	12.12	11.75	6.49
	5	8.79	11.43	4.66
	10	9.83	11.38	5.75
256	1	16.85	9.23	5.38
	3	10.38	6.94	2.91
	5	7.54	5.86	3.50
	10	7.50	6.82	2.17
512	1	13.18	6.13	3.08
	3	10.07	5.87	5.32
	5	9.36	5.54	2.85
	10	9.87	11.20	4.73

5.2.2.7 Inclinação dos traços da assinatura

O vetor de características que se baseia na inclinação dos traços da assinatura, que passaremos a chamar de vetor de características 7, é composto de 16 elementos por quadro. A técnica utilizada para fazer extração dos elementos que compõe esse vetor foi a morfologia matemática.

Na extração da inclinação dos traços da assinatura são utilizados 16 elementos estruturantes. A figura 5.15 mostra os 16 EEs, onde cada um deles foi denominado seqüencialmente de EE-6 até EE-21.

Os 16 EEs escolhidos representam segmentos de retas compostos de cinco pixels. Cada um desses EEs representa uma inclinação diferente. A diferença do ângulo de inclinação entre um elemento estruturante e o seu sucessor é de aproximadamente 11 graus. O elemento estruturante EE-6, por exemplo, representa um segmento de reta com ângulo de inclinação de 0 grau em relação ao eixo horizontal. Da mesma forma o EE-8 representa o segmento de reta com ângulo de aproximadamente 22 graus em relação ao eixo horizontal. Uma representação da medida desse ângulo é mostrada na figura 5.16.

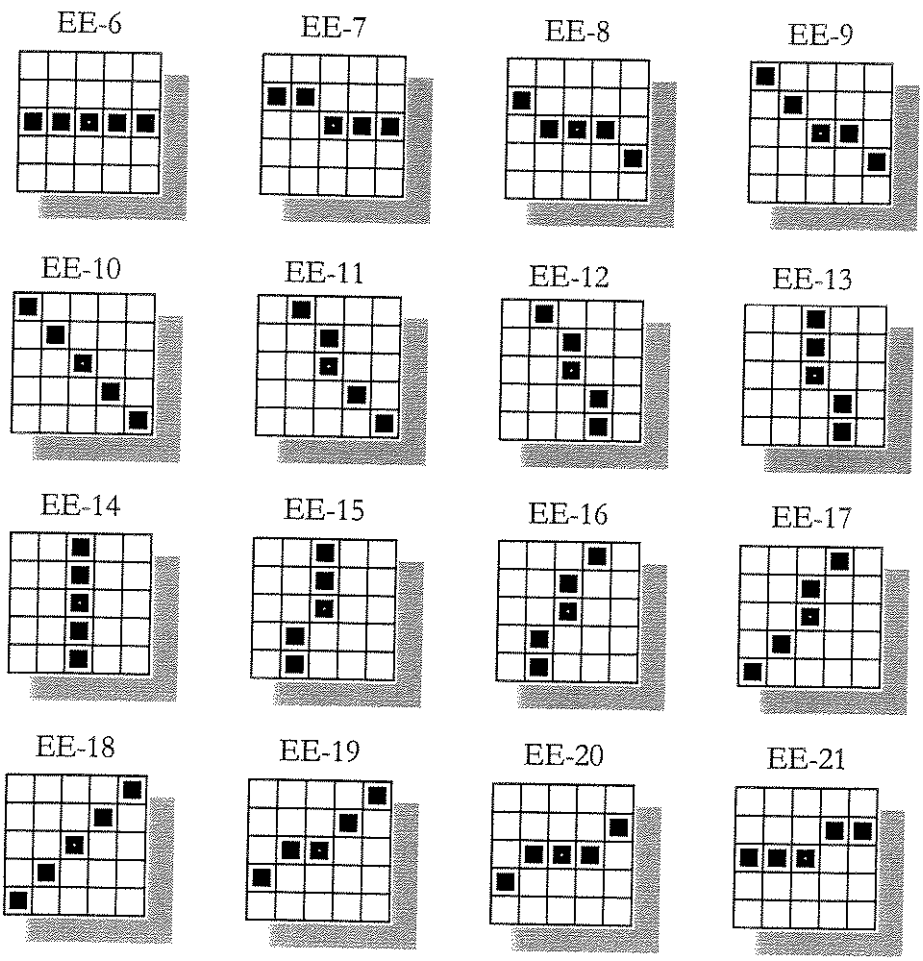


Figura 5.15: Os 16 elementos estruturantes utilizados para extração de características de inclinação dos traços da assinatura.

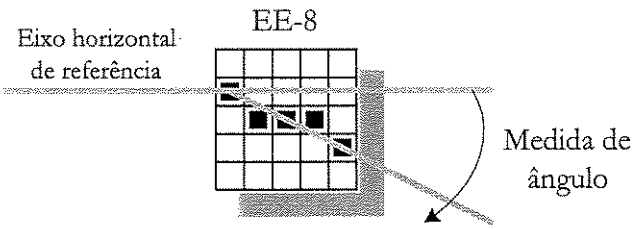


Figura 5.16: Medida do ângulo de inclinação dos segmentos de reta que compõe os EEs.

Seguindo o mesmo princípio descrito na extração da inclinação dos contornos dilatados da assinatura, em operações de erosão os EEs de 6 a 21, podem ser utilizados para detectar a inclinação dos traços da assinatura.

Tabela 5.7: Taxas médias de erros para o vetor de características 7

Escala	**Quadros**	**EFR_0** (%)	**EFA_0** (%)	**Erros Iguais** (%)
64	1	23.09	11.12	8.92
	3	15.45	11.17	6.62
	5	12.56	9.14	4.82
	10	7.89	9.32	6.60
128	1	20.15	10.36	4.76
	3	13.52	9.54	3.56
	5	11.42	10.43	3.40
	10	8.36	9.53	3.05
256	1	29.84	13.68	6.08
	3	20.06	12.08	5.07
	5	19.42	11.92	5.19
	10	13.05	10.90	5.35
512	1	38.08	15.82	9.13
	3	27.62	14.55	6.93
	5	21.78	13.17	6.03
	10	17.98	13.81	5.33

Assim sendo, para uma imagem de assinatura A, tomamos um EE e fazemos a operação de erosão. Sobre a imagem resultante B é feita a contagem de todos os seus pixels. O número de

pixels de B indica quantas vezes aquele EE esteve contido na imagem A. Essa operação é repetida para cada um dos 16 EEs, sempre tomando a imagem da assinatura A como entrada.

Dessa forma, os elementos que compõe o vetor de características 7 é o número de pixels resultante da operação de erosão para cada um dos 16 EEs apresentados na figura 5.15 por quadro.

Para obter o desempenho que a característica 7 teria sobre a base de dados, foi utilizado o procedimento para análise de desempenho de vetores de características. A síntese dos resultados obtidos pelo procedimento sobre o vetor de características 7, pode ser visto na tabela 5.7.

5.3 Sistema de Verificação Proposto

O proposto sistema automático de verificação de assinaturas estáticas é um sistema multi-especialista de dois estágios [78].

O primeiro estágio tem por objetivo eliminar as falsificações aleatórias e simples. O segundo estágio se encarrega de eliminar as falsificações habilidosas.

Uma visão geral desse sistema é apresentado na figura 5.17. Cada estágio pode atribuir à assinatura em teste uma das duas classes possíveis, isto é, genuína ou falsa. Essa atribuição se baseia na comparação da distância calculada sobre os vetores de características da assinatura, que chamaremos de φ, e um limiar de decisão que chamaremos de λ. O processo de verificação se inicia ao apresentar uma assinatura na entrada do primeiro estágio. Se a distância φ_1 for maior que o limiar de decisão λ_1, o sistema conclui que a assinatura é uma falsificação e o processo termina. Caso contrário a assinatura é passada para o segundo estágio, no qual é calculado uma nova distância φ_2 e aplicado um novo limiar λ_2.

5.3.1 Selecionando os Vetores de Características para cada Estágio

Os vetores de características escolhidos para serem utilizados no primeiro estágio são os de número 1 a número 5. Esses vetores se baseiam na distribuição dos pixels da imagem. Esse tipo de atributo fornece uma idéia geral de como os pixels que fazem parte das assinatura estão presentes na imagem. Porém não fornecem informação da estrutura e forma dos traços. Assim, esses vetores fornecem apenas informações globais da imagem. Em nosso caso especifico, em que utilizamos a divisão da imagem em quadros, pode-se dizer que essa informação é global dentro do quadro, porém local na imagem como um todo.

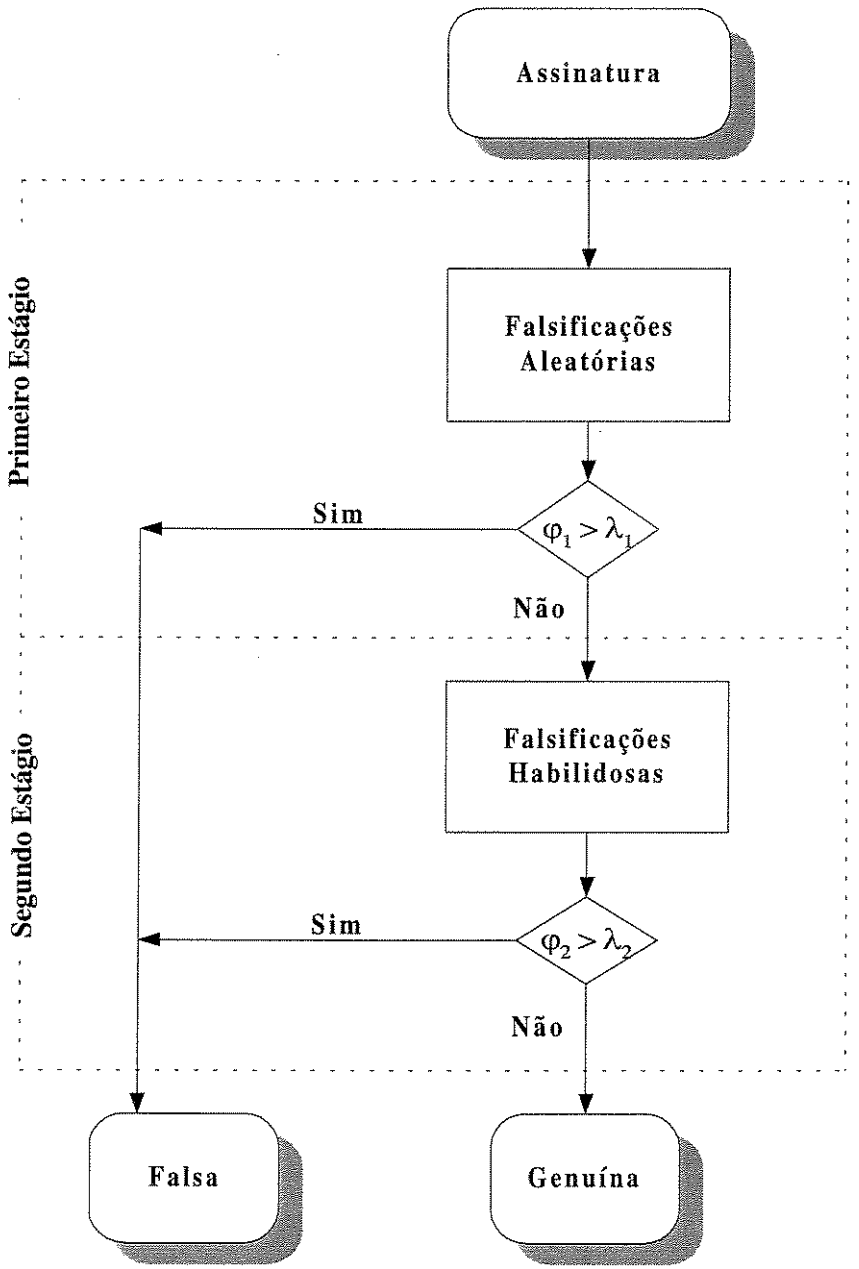


Figura 5.17: Visão geral do sistema de verificação automático de assinaturas proposto.

Por outro lado, os vetores de características escolhidos para serem utilizados no segundo estágio são os de número 6 e número 7. Esses vetores possuem como principal atributo extrair informação estrutural dos contornos e traços da assinatura. A informação estrutural é muito importante quando pensamos em fazer uma distinção entre assinaturas verdadeiras e falsificações habilidosas, visto que nos permite obter informação diretamente da forma dos traços que compõem a assinatura.

Fazendo tanto parte do primeiro como do segundo estágio, existe um módulo que calcula a correlação entre a imagem da assinatura que se deseja fazer a verificação e o conjunto de 3 assinaturas verdadeiras que fazem parte do conjunto de treinamento.

Uma apresentação mais detalhadas dos dois estágios será feita a seguir.

5.3.2 Primeiro Estágio

O primeiro estágio está destinado a tentar descobrir se a assinatura de entrada é uma falsificação aleatória.

Um diagrama de blocos dos componentes que fazem parte desse estágio pode ser vista na figura 5.18. Uma imagem de assinatura serve de entrada para cada um dos 5 módulos de extração de vetores de características. Além dos módulos de extração de características de 1 a 5 que foram anteriormente descritos, aparece o módulo extrator de características de correlação. Esse último módulo tem por objetivo encontrar um vetor de características que expresse a semelhança entre a imagem da assinatura de entrada e as imagens que fazem parte do conjunto de treinamento.

A seguir, são encontradas as distâncias dos vetores de características de 1 a 5 assim como também a distância do vetor de correlação com relação ao conjunto de assinaturas de treinamento. As distâncias dos vetores de características 1 a 5 são somados e a seguir esse resultado é multiplicado pela distância do vetor de correlação. Ao valor da distância resultante é chamado de φ_1. Se φ_1 for maior que o limiar λ_1 então a assinatura é considera falsa, caso contrário passa para o segundo estágio.

A seguir descreveremos o módulo de extração do vetor de correlação.

5.3.2.1 Extração do vetor de correlação

Nesse processo desejamos fazer o casamento (*match*) de uma imagem $w(x, y)$ de dimensão J x K com uma imagem $f(x, y)$ de dimensão M x N, onde assumimos que $J \leq M$ e $K \leq N$.

Na sua forma mais simples, a correlação entre $f(x, y)$ e $w(x, y)$ é dada por:

$$C(s,t) = \sum_{s=0}^{M-1} \sum_{t=0}^{N-1} f(x, y) w(x - s, y - t) \tag{5.40}$$

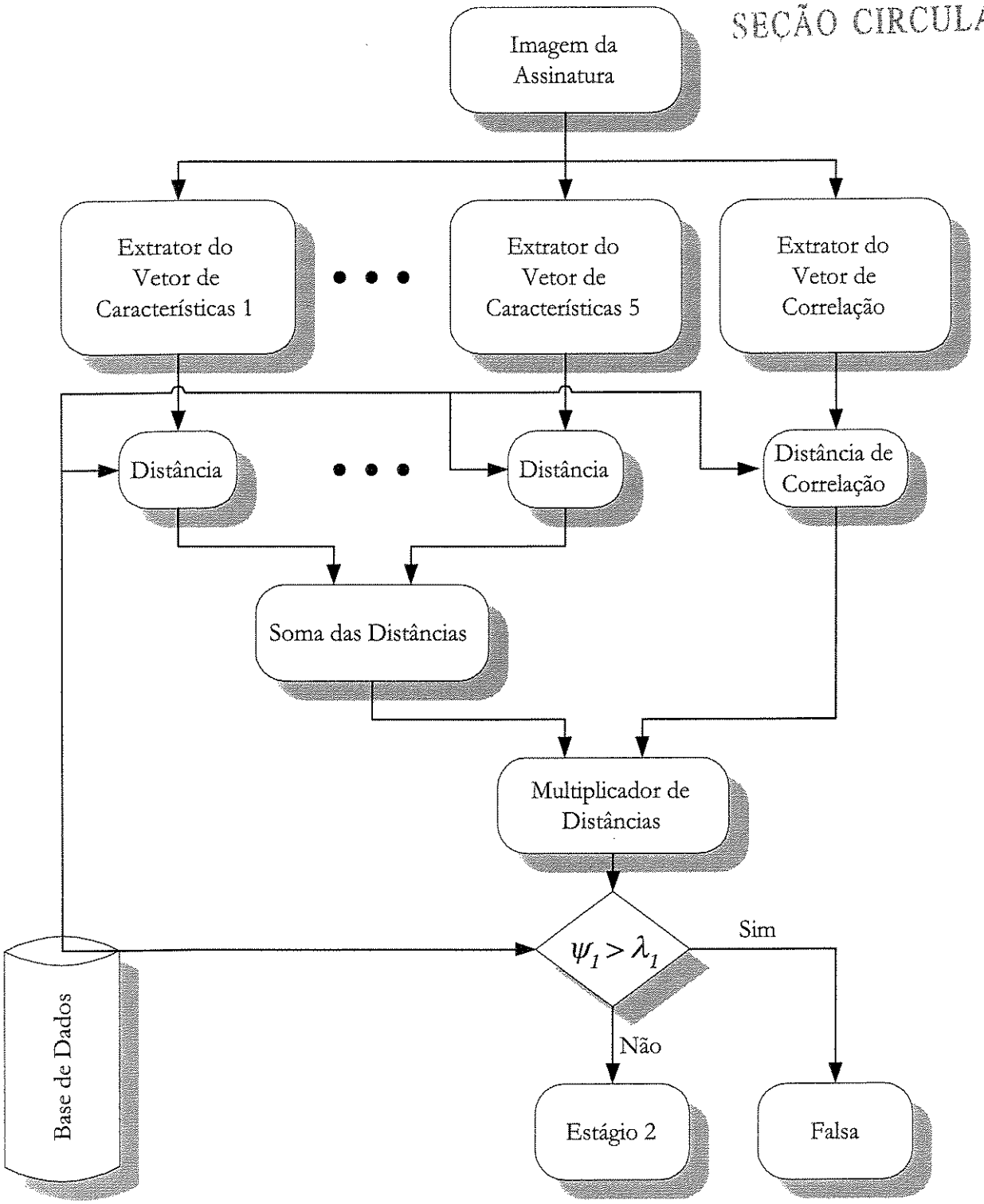


Figura 5.18: Estagio 1.

Onde $s = 0, 1, 2, \ldots, M-1$ e $t = 0, 1, 2, \ldots, N-1$, e que a somatória se produz na região da imagem onde $f(x,y)$ e $w(x,y)$ se sobrepõem. Para qualquer valor de (s,t) dentro de $f(x,y)$ aplicando a equação (5.40) encontramos os valores da função $C(s,t)$. O valor máximo de $C(s,t)$ indica a posição onde $w(x,y)$ melhor casa com $f(x,y)$.

Em nosso caso, a imagem de *template* $f(x,y)$ é uma das assinaturas que faz parte do conjunto de referência e a imagem que desejamos casar $w(x,y)$ é a assinatura em teste. O valor da escala da imagem para esse processo é de 64 pixels na horizontal. Diferentemente do vetores de características 1 a 7, nesse procedimento não dividimos as imagens em quadros. Para evitar problemas com bordas, a assinatura de referência é previamente colocada sobre uma imagem em branco de dimensões muito maiores aos dela própria. Outro detalhe importante é fazer o negativo das imagens, isto e, pixels pretos (valor 0) passam a ter valor 1, e os pixels brancos (valor 1) passam a ter valor 0.

Servindo-se da equação (5.40) encontra-se a posição em que a assinatura de referência e a assinatura de teste casam melhor. Os valores da coordenada onde $C(s,t)$ é máximo serão chamados de s_max e t_max. Esses dois valores compõem o primeiro e o segundo elemento do vetor de correlação.

Uma vez encontrada a posição de melhor casamento entre as duas imagens fazemos a soma das imagens pixel a pixel dada por:

$$z(x,y) = f(x,y) + w(x - s\_\max, y - t\_\max) \tag{5.41}$$

Em seguida fazemos a contagem de quantos valores iguais a 1 e quantos valores iguais a 2 possui $z(x,y)$. Isto é, contar o número de pixels da imagem de referência que não foram sobrepostos aos pixels da imagem de entrada (valores iguais a 1) e contar o número de pixels da imagem de referência que ficaram sobrepostos aos da imagem de entrada (valores iguais a 2). O número de pixels iguais a 1 em $z(x,y)$ e o número de pixels iguais a 2 em $z(x,y)$ compõe o terceiro e quarto elementos do vetor de correlação, respectivamente.

O quinto elemento do vetor de correlação é o número de pixels pretos que originalmente faziam parte dos traços da assinatura de teste.

O sexto elemento do vetor de correlação é razão entre o número de pixels com valores iguais a 1 e os de valores iguais a 2.

Uma vez definidos os seis elementos que compõe o vetor de correlação, passamos a calcular o seu vetor médio.

O vetor de correlação médio é calculado da seguinte maneira:

1. Escolher três assinaturas verdadeiras de cada indivíduo, as quais chamaremos de A_1, A_2 e A_3
2. Calcular o vetor de correlação para A_2 e A_3, sendo que a imagem *template* é A_1.
3. Calcular o vetor de correlação para A_1 e A_3, sendo que a imagem *template* é A_2.
4. Calcular o vetor de correlação para A_1 e A_2, sendo que a imagem *template* é A_3.
5. O vetor de correlação médio é obtido utilizando a equação (3.8) para cada um dos seis elementos que compõe esse vetor.

A distância do vetor de correlação é calculado da seguinte maneira:

1. Calcular a distância euclidiana dada pelos cinco primeiros elementos do vetor de correlação da assinatura de entrada com os respectivos elementos do vetor de correlação médio. A essa distância chamaremos de D_1.
2. Calcular a distância euclidiana entre os sextos elementos do vetor de correlação da assinatura de entrada e do vetor de correlação médio. A essa distância chamaremos de D_2.
3. A distância do vetor de correlação D_c é dada por:

$$D_c = D_1 * D_2 \tag{5.42}$$

É importante ressaltar o fato de realizarmos a multiplicação entre D_1 e D_2. Da análise dos dados, constatou-se que na grande maioria dos vetores de correlação de uma mesmo indivíduo, o sexto elemento desse vetor mantinha-se constante. Assim sendo, a sua distância euclidiana medido com relação ao mesmo elemento no vetor de correlação médio é pequeno. Por outro lado, para vetores de correlação de indivíduos diferentes, esses valores eram muito distintos, o que por conseqüência levaria a uma medida de distância elevada. Essa distância, muitas vezes ficava na ordem de 100 vezes maior que a calculada sobre vetores do mesmo indivíduo. Dessa forma concluímos que poderíamos utilizar D_2 para minimizar a distância de correlação entre assinaturas verdadeiras e maximizar essa distância no caso de estar avaliando uma assinatura falsa.

Note que a multiplicação entre a distância do vetor de correlação e a somatória dos vetores de características 1 a 7 é feita independentemente do valor da escala e do número de quadros que os vetores de características estejam expressando.

Uma síntese do desempenho obtido pelo estágio 1 sobre um conjunto de falsificações aleatórias está descrito na tabela 5.8.

Tabela 5.8: Taxas médias de erros para o estágio 1

Escala	Quadros	EFR_0 (%)	EFA_0 (%)	Erros Iguais (%)
64	1	8.87	11.90	2.60
	3	7.71	7.59	2.19
	5	8.04	6.68	1.94
	10	9.73	5.64	2.16
128	1	7.76	5.09	2.33
	3	4.71	3.08	1.49
	5	4.63	2.26	1.16
	10	7.34	2.89	1.48
256	1	5.73	3.31	1.43
	3	4.15	2.08	1.17
	5	3.82	2.58	0.97
	10	4.69	3.13	1.59
512	1	9.14	6.74	2.41
	3	9.64	12.59	3.00
	5	7.41	14.72	2.50
	10	8.54	16.60	2.94

5.3.3 Segundo Estágio

O segundo estágio está destinado a tentar descobrir se a assinatura que passou do primeiro estágio é uma falsificação habilidosa ou se de fato é verdadeira.

Um diagrama de blocos das componentes que fazem parte desse estágio pode ser visto na figura 5.19. Uma imagem de assinatura que passou pelo primeiro estágio serve de entrada para os módulos de extração de características 6 e 7 e para o extrator de características de correlação.

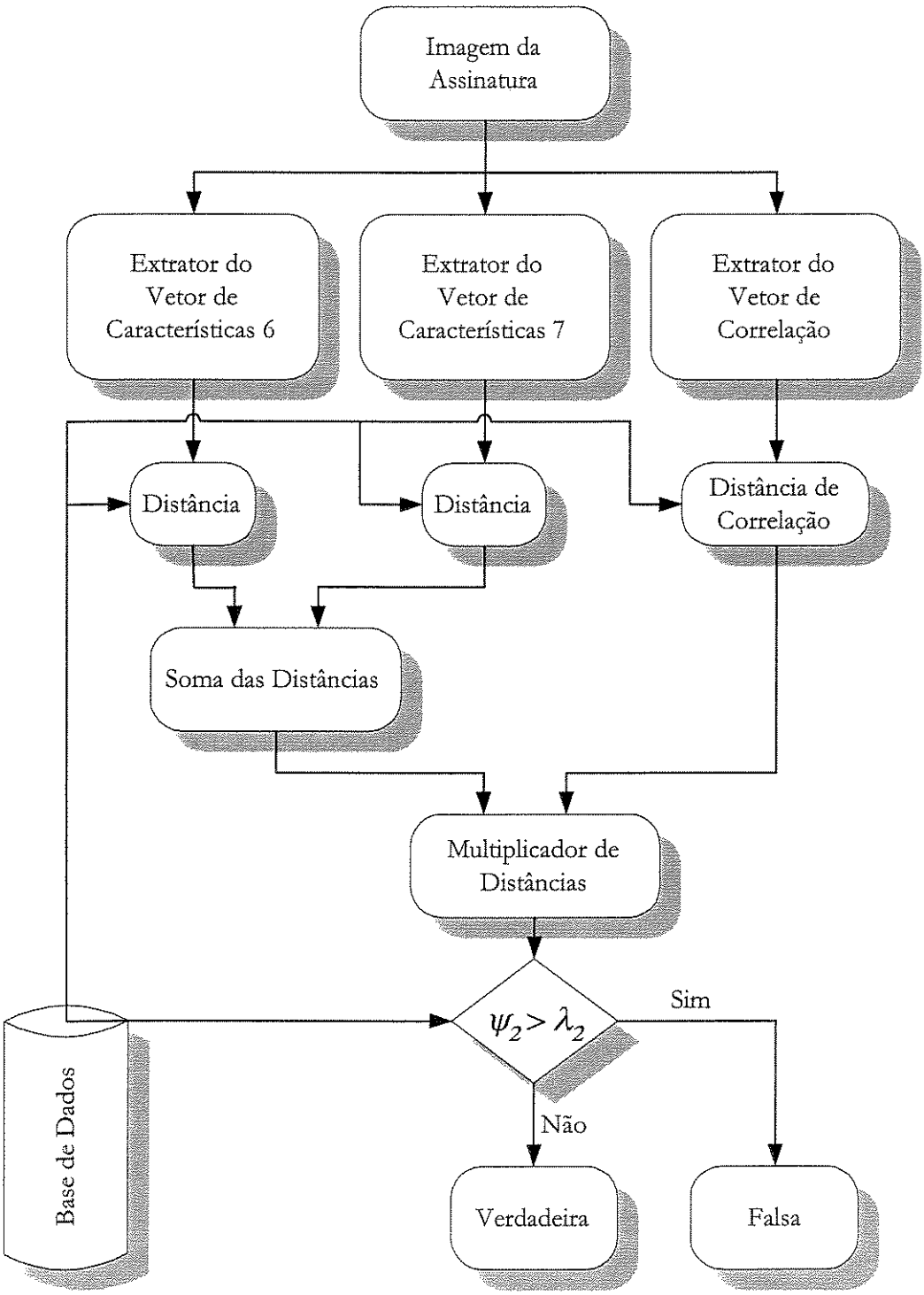


Figura 5.19: Estagio 2.

A seguir, são encontradas as distâncias dos vetores de características 6 e 7 assim como também a distância do vetor de correlação com relação ao conjunto de assinaturas de treinamento. As distâncias dos vetores de características são somados e a seguir esse resultado é multiplicado pela distância do vetor de correlação. O valor de distância resultante é chamado de φ_2. Se φ_2 for maior que o limiar λ_2 então a assinatura é considerada falsa, caso contrário é considerada verdadeira.

Visto que no estágio 1, a menor taxa de erros iguais ocorreu no caso em que foram utilizados 5 quadros com escala de 256, optamos por fazer a análise do desempenho do segundo estágio apenas para essa configuração. Assim sendo, o desempenho obtido pelo estágio 2 sobre um conjunto de falsificações exclusivamente habilidosas pode ser visto na tabela 5.9.

Tabela 5.9: Desempenho do estágio 2 sobre falsificações habilidosas

Escala	**Quadros**	**EFR_0 (%)**	**EFA_0 (%)**	**Erros Iguais (%)**
256	5	25.62	32.65	9.72

Tanto a tabela 5.8 quanto a tabela 5.9 foram construídas variando os limiares de decisão λ_1 e λ_2 de maneira a varrer todas as distância das assinaturas de teste. Por outro lado, num sistema real, não é possível ter um número grande de amostras verdadeiras assim como um conjunto de assinaturas falsas para obter as curvas de erros de falsa rejeição e falsa aceitação, respectivamente. Assim sendo, apresentamos a seguir o método que é utilizado para determinar os limiares de decisão λ_1 e λ_2 a partir de apenas três amostras de assinaturas verdadeiras.

5.3.4 Determinação dos Limiares de Decisão λ_1 e λ_2

A determinação dos limiares de decisão λ_1 e λ_2 são dependentes da distância de correlação. Sejam A_1, A_2 e A_3 as três assinaturas que fazem parte do conjunto de treinamento. Calcula-se o vetor de correlação médio como descrito na seção 5.3.2. A seguir, acha-se as distâncias de

correlação para cada um dos vetores de correlação A_1, A_2 e A_3 com relação ao vetor de correlação médio. Sejam as distâncias encontradas, D_{A1}, D_{A2} e D_{A3} para cada uma das assinaturas. Então:

$$\lambda = \alpha * \left(\frac{D_{A1} + D_{A2} + D_{A3}}{3} \right) \tag{5.43}$$

Onde α é uma constante e é obtida empiricamente podendo ser qualquer número inteiro maior que 1.

Em nosso caso particular, encontramos que α deve ter o valor igual a 1000 no caso de desejarmos ter uma taxa baixa de falsa rejeição contra falsificações aleatórias. A tabela 5.10 apresenta o resultado obtido com esse valor de α.

Tabela 5.10: Desempenho do estágio 1 para $\alpha = 1000$

α	$\mathbf{EFR_0}$ (%)	$\mathbf{EFA_0}$ (%)
1000	0.47	2.35

No caso de desejarmos nos aproximar do desempenho obtido pelo segundo estágio do sistema, no qual foram utilizadas falsificações habilidosas, devemos utilizar um valor de α igual a 100. A tabela 5.11 apresenta o resultado obtido com esse valor de α.

Tabela 5.11: Desempenho do estágio 1 para $\alpha = 100$

α	$\mathbf{EFR_0}$ (%)	$\mathbf{EFA_0}$ (%)
100	12.75	19.22

O desempenho do sistema como um todo utilizando-se tanto falsificações habilidosas como falsificações aleatórias para o sistema multi-especialista de dois estágios com valor de escala = 256, número de quadros = 5, $\alpha = 1000$ no cálculo de λ_1 e $\alpha = 100$ no cálculo de λ_2 é apresentado na tabela 5.12.

Tabela 5.12: Desempenho geral do sistema

EFR_0 (%)	EFA_0 (%)
13.95	7.52

5.4 Análise do Sistema Automático de Verificação de Assinaturas

Neste capítulo apresentamos o pré-processamento e as características que foram utilizadas para representar uma assinatura. Na etapa de pré-processamento, tanto a mudança de escala quanto a divisão da assinatura em quadros, foi idealizada para encontrar qual seria o melhor conjunto de parâmetros que pode minimizar a distância intra-pessoal e maximizar a distância inter-pessoal. Da tabela 5.8 ficou claro que esses parâmetros seriam a normalização do tamanho da assinatura em 256 pixels na horizontal e a divisão da mesma em 5 quadros.

Uma vez definido esses parâmetros passamos a pensar na determinação dos limiares de decisão. Esses limiares além de serem dependentes da distância de correlação das assinatura do conjunto de treinamento - a qual fornece a informação da variabilidade intra-classe desse tipo de assinatura - está relacionada a uma constante α que foi calculada empiricamente a partir da análise dos dados do sistema.

Os resultados apresentados nas tabelas 5.10 e 5.11 são bastante satisfatórios, principalmente se tomamos em consideração que no sistema proposto são utilizadas apenas três assinaturas no conjunto de treinamento. O pequeno conjunto de treinamento é um dos principais pontos a favor de nosso sistema, pois obtemos taxas de erros próximas a de outros sistemas que em geral utilizam dez ou mais assinaturas na fase de treinamento.

Outro ponto importante é que nosso sistema utiliza classificadores lineares simples, ao contrário de outros sistemas que se servem, por exemplo, de classificadores baseados em redes neurais. Dessa forma, nosso sistema leva apenas alguns segundos para ser treinado, ao contrário de outros em que a fase de treinamento leva um tempo maior, podendo se estender muito mais no caso de ocorrer o problema de convergência (classificadores neurais).

CAPÍTULO 6

REDES DE COMPUTADORES

Neste capítulo fazemos a introdução aos componentes de uma rede de computadores, Protocolos TCP/IP e HTTP, mecanismos de uma aplicação para redes de computadores, Servidor Web, Navegador Internet e programas CGI. O objetivo dessa introdução é formar a base para a implementação do sistema de identificação pessoal via internet

6.1 Objetivos de uma rede de Computadores

O principal objetivo de uma rede de computadores é compartilhar recursos e fornecer um meio para estabelecer comunicação entre os computadores pertencentes à rede. Um recurso de rede pode ser tanto um dispositivo (impressora, câmara de vídeo, *scanner*, etc.) quanto um programa (software) que esteja disponível para utilização dos usuários. O computador ao qual os recursos da rede estão vinculados é chamado de servidor. Os outros computadores que acessam esses recursos sobre a rede são chamados de clientes.

A figura 6.1 apresenta o diagrama de uma rede de computadores onde os computadores A, B, C são clientes e o computador servidor possui dois dispositivos (*plotter* e impressora) que podem ser acessados através da rede.

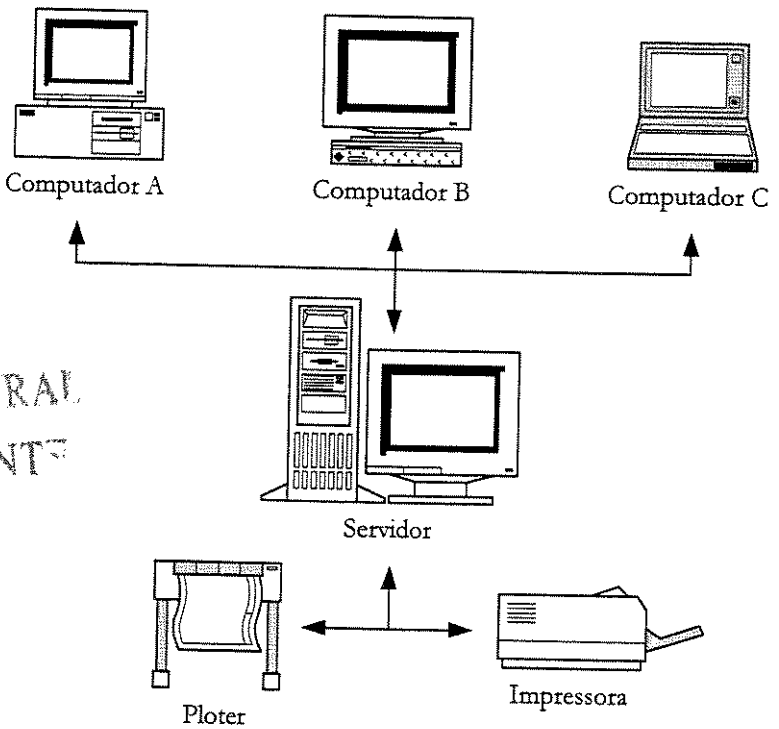


Figura 6.1: Um diagrama de uma rede de computadores.

6.2 Visão Geral do Protocolo TCP/IP

O protocolo TCP/IP é um acrônimo para Protocolo de Controle de Transmissão/Protocolo de Internet e se refere a dois dos primeiros protocolos de comunicação que fazem parte do *Internet Protocol Suit*. O conjunto de protocolos (também designado como família de protocolos) utilizados na internet é o TCP/IP. A família TCP/IP é composta por diversos protocolos de comunicação, dos quais destacamos (além de TCP e IP que dão nome à família) o DNS, o SMTP, FTP e Telnet. O TCP/IP é capaz de estabelecer uma conexão de rede entre quaisquer sistemas de computadores, sobre diferentes meios de transmissão e sob possíveis condições adversas [79].

6.2.1 Modelo de Arquitetura ISO/OSI e TCP/IP

A *International Organization for Standardization* (ISO) [80] que é uma das organizações internacionais que tem por missão promover o desenvolvimento da padronização nas áreas científicas e tecnológicas, apresentou o *Open Systems Interconnection* (OSI), um modelo de arquitetura de rede em camadas, com o objetivo de padronizar os protocolos internacionais de

redes de computadores. Nesse modelo, os sistemas de computadores conectados não precisam ser do mesmo fabricante e/ou executar aplicações sobre o mesmo sistema operacional. São sete as camadas que fazem parte do modelo de arquitetura definido pela OSI: 1) Camada física; 2) Camada de enlace de dados; 3) Camada de rede; 4) Camada de transporte; 5) Camada de sessão; 6) Camada de apresentação; 7) Camada de aplicação [81]. Uma representação gráfica das sete camadas pode ser vista na figura 6.2 (a). Por outro lado, o modelo de arquitetura de redes do protocolo TCP/IP não segue diretamente o modelo OSI. Embora o modelo OSI e o TCP/IP sejam diferentes, é prático utilizar o modelo de sete camadas como referência ao se discutir comunicações de dados. A figura 6.2 (b) mostra as camadas que compõem o protocolo TCP/IP.

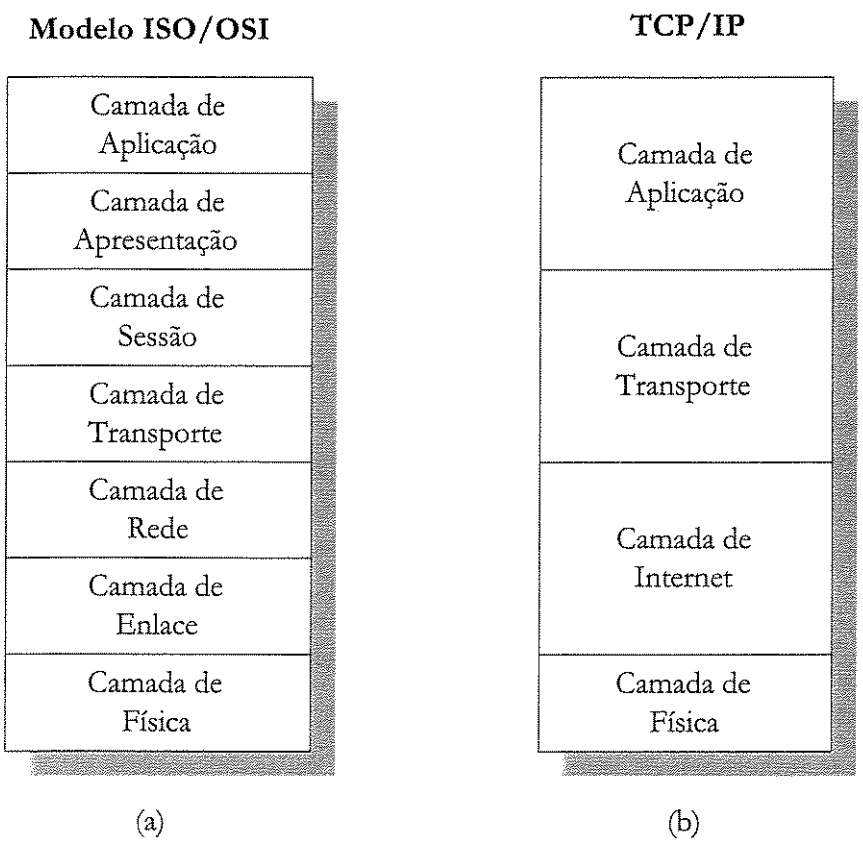


Figura 6.2: Camadas que compõem o modelo OSI (a) e TCP/IP (b).

A seguir descrevemos cada uma das quatro camadas que compõe esse protocolo fazendo referência ao seu correspondente no modelo OSI:

1. Camada de aplicação: consiste de aplicativos que utilizam a rede. As camadas de aplicação e apresentação do modelo OSI se ajustam nessa camada na arquitetura TCP/IP.

2. Camada de transporte: Faz a entrega de dados de um extremo ao outro da rede. Isso é feito através de um mecanismo chamado de *Socket* TCPI/IP, que é um enlace lógico estabelecido entre o computador de origem e o de destino. As camadas de sessão e de transporte do modelo OSI se ajustam nessa camada na arquitetura TCP/IP.

3. Camada internet: Define um pacote de dados que é manipulado pelo protocolo IP. Esse pacote de dados é chamado de datagrama. Um datagrama contém o endereço fonte, o endereço de destino e os dados, assim como outros campos de controle. A função dessa camada é equivalente a das camada de enlace e de rede do modelo OSI.

4. Camada física: O TCP/IP não realiza esforços para definir a conectividade física da rede básica. Pelo contrário, o TCP/IP faz uso dos padrões existentes fornecidos por organizações como *Institute of Electrical and Electronical Engineers* (IEEE), o qual define o RS232, Ethernet e outras interfaces eletrônicas utilizadas nas comunicações de dados.

6.2.2 Aplicações sobre Protocolo TCP/IP

Um serviço sobre o protocolo TCP/IP se inicia quando uma aplicação faz um pedido de transferência de informação através da camada de mais alto nível do protocolo. A seguir, o pedido segue pelas camadas inferiores, faz o intercâmbio de dados com outros computadores que também utilizam o protocolo TCP/IP, e finalmente os dados retornam e são recebidos pelo aplicativo que fez inicialmente o pedido. A figura 6.3 mostra um diagrama de blocos da comunicação entre duas aplicações que utilizam o protocolo TCP/IP como descrito anteriormente [82].

O protocolo TCP provê uma interface de alto nível de confiabilidade para transferência de dados via IP. O protocolo TCP/IP é baseado em pacotes. Isso significa que uma mensagem é segmentada em pacotes antes de ser transmitida. Ao chegar ao seu destino, os pacotes são remontados na ordem correta e a mensagem contida neles é passada para um aplicativo. Além disso, o protocolo TCP/IP garante que todos os pacotes que compõem a mensagem chegarão ao seu destino sem nenhum tipo de erro ou perda dos mesmos durante seu tráfego pela rede. Assim, aplicações que se servem do protocolo TCP/IP podem confiar no fluxo de dados, isto é, não precisam implementar qualquer teste de erros ou se preocupar com dados corrompidos durante o envio. Se um pacote durante seu tráfego pela rede for mutilado, o TCP/IP receptor não informa à sua aplicação esse acontecimento, e pede ao TCP/IP do endereço de origem que lhe seja enviado uma nova cópia desse pacote.

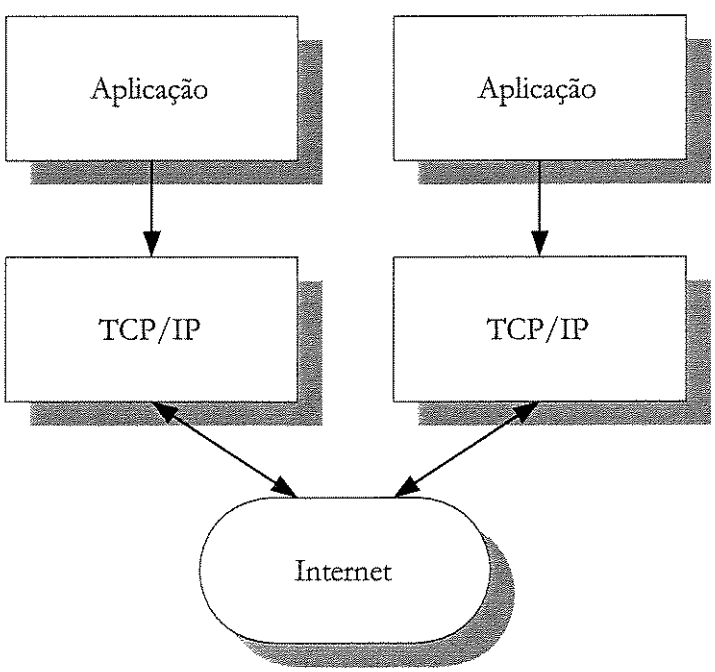


Figura 6.3: Comunicação entre aplicações sobre protocoloc TCP/IP.

Uma das principais características do protocolo TCP/IP é a de abstrair-se do nível do meio físico da transferência de dados. Isso significa que oferece uma interface comum para todo tipo de hardware, seja IBM-PC, Macintosh, estação UNIX, VAX, etc..

O protocolo TCP/IP se baseia em conexões ponto a ponto, ou seja, conexões que se realizam entre um computador de origem e um de destino. O computador de origem não precisa estar fisicamente ligado a outro computador para que possa existir a comunicação entre eles. A mensagem enviada através do TPC/IP possui um endereço o qual permite que ao chegar em máquinas intermediárias, possa ser roteada para outras máquinas que se acreditam estar mais próximas do destino final. Todos os computadores que utilizam o protocolo TCP/IP possuem um único endereço, constituído por um número inteiro de 32 bits, o qual é geralmente representado por quatro palavras de oito bits, cada uma separada por pontos, por exemplo: 143.106.50.4.

6.3 Modelo Computacional Cliente/Servidor

No modelo computacional cliente/servidor, uma aplicação é dividida em duas partes: um cliente, chamado de *front-end*, que tanto apresenta quanto capta informações do usuário, e um servidor, chamado *back-end*, que armazena, recupera, manipula dados e que geralmente trata da maior parte das tarefas de computação para o cliente. O modelo computacional cliente/servidor é uma aplicação de um sistema computacional distribuído onde um programa de aplicação (cliente) interage com um outro programa de aplicação (servidor).

O cliente se encarrega principalmente da interface com o usuário oferecendo as seguintes funções: interpretação do pedido do usuário em comandos apropriados, envio de comandos para o servidor, espera pela resposta do servidor, interpretação da resposta do servidor e apresentação do resultado para o usuário. O servidor por outro lado, aceita o pedido do usuário, o processa e retorna o resultado para o cliente. O programa servidor oferece serviços e recursos, enquanto o programa cliente permite que os usuários os utilizem [83]. O programa cliente também oferece a interface entre o usuário e a máquina que está sendo utilizada, isto é, pode permitir interpretar a digitação de teclas, apresentar menus, enviar comandos via teclado, etc..

6.4 Internet e Web

A internet é um conjunto de redes de computadores conectando um grande número de redes de computadores que estão fisicamente distribuídas pelo mundo que utilizam o protocolo TCP/IP. Nos últimos anos o número de computadores conectados à internet tem aumentado

muito. Da mesma forma, o quantidade de usuários assim como provedores de informação seguiram o mesmo caminho. Isso por sua vez, elevou a demanda de serviços presentes na internet, encorajando o desenvolvimento de uma ampla gama de aplicações para suprir as necessidades dos atuais usuários [84][85].

Nesse contexto, a *World-Wide-Web* (*Web*) com um dos serviços da internet, é colocada como a principal plataforma para o desenvolvimento de sistemas de informação distribuído. Tal proposta surge naturalmente, uma vez que o propósito da *Web* é o de oferecer um mecanismo para agregar informações fisicamente dispersas [86]. Oficialmente, a Web é descrita como uma "ampla iniciativa de recuperação de informação hipermídia objetivando dar acesso universal a uma vasta quantidade de documentos."[87]. De fato, a *Web* implementou, através de mecanismos uniformes de descrição e acesso, um espaço abstrato de conhecimento no topo da internet, de forma que integra milhões de usuários espalhados pelo mundo.

A *Web* foi inicialmente proposta em 1989 [88], pelo Dr. Tim Berners-Lee, um pesquisador do laboratório de física e alta energia da Organização Européia de Pesquisa Nuclear (CERN) com sede em Genebra. Essa iniciativa espalhou-se de tal forma que a *Web* vem tendo taxas de crescimento superior a qualquer outro serviço suportado pela internet.

O *Mosaic* foi a primeira interface gráfica de interação com a *Web* desenvolvida no Centro Nacional para Aplicações em Supercomputação (NCSA) dos Estados Unidos, cuja primeira versão foi disponibilizada no início de 1993. Desde então, surgiram diversos navegadores (*browsers*) para a apresentação de documentos da *Web*. Em geral, esses *browsers* interagem com o usuário através de interfaces gráficas permitindo a apresentação de documentos do tipo hipertexto. Mais recentemente, os *browsers* permitem a apresentação de outros tipos de mídia, tais como imagens vídeo e áudio incorporados ao hipertexto.

6.4.1 Princípio de Operação da *Web*

A *Web* opera segundo o modelo cliente/servidor de aplicações distribuídas. Um servidor *Web*, também chamado de servidor de HTTP, é uma aplicação (programa) sendo executada em um computador cujo propósito principal é enviar documentos a outros computadores que lhe tenham feito tal pedido. Um cliente *Web* é qualquer programa que interage com o servidor *Web* através de requisições via protocolo *HyperText Transfer Protocol* (HTTP). Tradicionalmente, o

cliente é um *browser*, que suporta a interface com o usuário e requisita documentos a servidores.

A principal funcionalidade do servidor *Web* é localizar recursos específicos e ativar a transferência do recurso solicitado para o processo cliente. O mecanismo de identificação do recurso é o *Uniform Resource Locator* (URL), que permite identificar de forma única sobre toda a rede internet, o protocolo, o servidor (endereço IP e porta), o diretório e o arquivo associado ao recurso. O recurso é um arquivo contido no *espaço Web*, isto é, contido no conjunto de diretórios acessíveis a partir do servidor. Entre as outras tarefas realizadas pelo servidor Web estão os mecanismos para criptografia, autenticação de usuários e interação com programas residentes no servidor através de CGI ou *applets* Java.

A seguir apresentaremos os passos típicos que envolvem a transferência de um arquivo entre um *browser* e um servidor *Web*.

Primeiramente, o cliente através de um *browser* abre um *socket* sobre o protocolo TCP/IP, conecta-se ao servidor *Web* através de uma porta (comumente a porta de número 80) e a seguir envia um pedido de envio de arquivo. Esse pedido é levado até o servidor *Web* via internet. O servidor recebe o pedido e passa a procurar dentro do seu *espaço Web* o arquivo que foi pedido, ver figura 6.4.

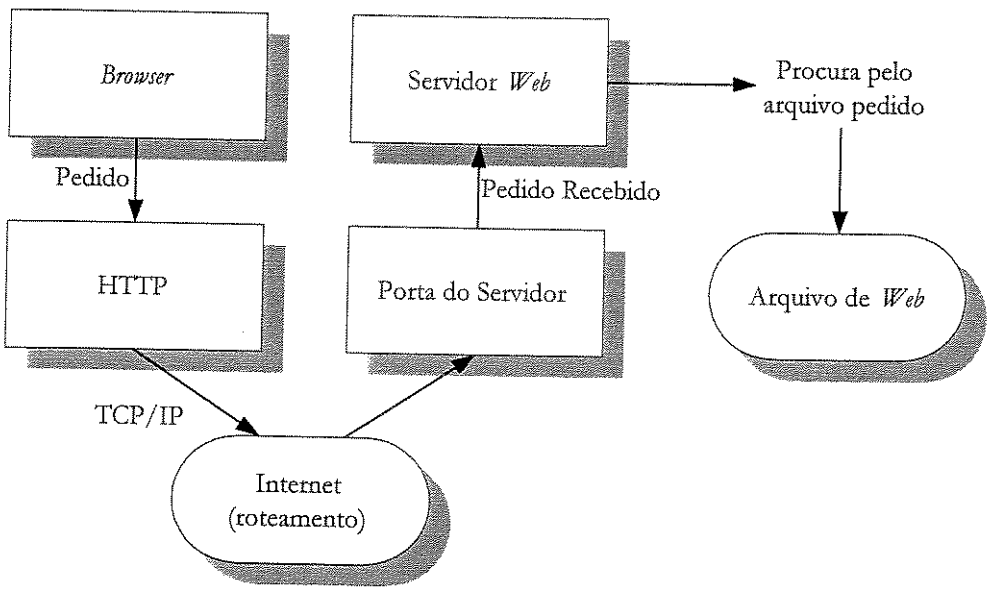


Figura 6.4: Pedido feito por um cliente.

A segunda parte dessa transação ocorre quando o servidor codifica os resultados do pedido como um documento HTML, o envia de volta pelo *socket* originalmente aberto pelo cliente, e finalmente fecha a conexão, ver figura 6.5.

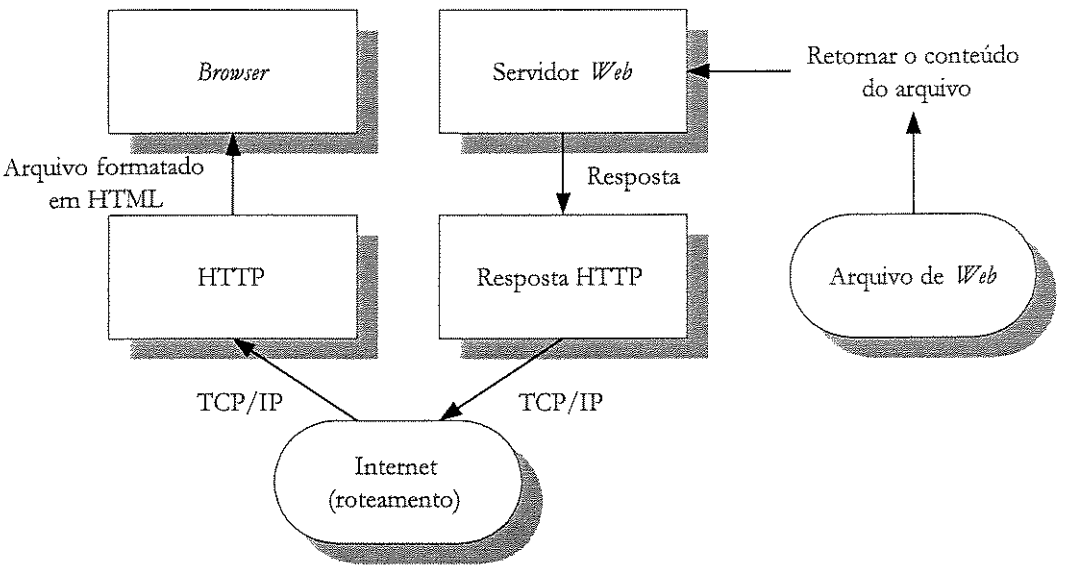


Figura 6.5: Resposta de um Servidor *Web*.

6.5 Utilizando a Internet/Web num Sistema de Identificação

Como um dos objetivos deste trabalho, inicialmente estamos interessados em criar um sistema que permita clientes cadastrados acessarem uma base de dados a qual contenha características biométricas de certas pessoas. Esse sistema poderia começar sendo implementado num único computador, onde a verificação da identidade deveria ser feita exclusivamente nesse local. A partir daí, seria possível que novas necessidades surgissem, como por exemplo, diversificar os lugares de captura das características biométricas ou que as informações contidas na base de dados fossem disponíveis para outros computadores em tempo real.

Uma melhoria que poderia ser feita no sistema anteriormente descrito é colocar o computador que possui a base de dados numa rede contendo alguns computadores. Isso implicaria por sua vez, em treinar pessoas que possam entender a interface que se utiliza no acesso à base de dados, assim como os protocolos de comunicação da rede local.

À medida que o tempo passa é possível que seja necessário fazer sucessivas atualizações no sistema de identificação implementado para atender as novas necessidades crescentes dos usuários. As atualizações no software que oferece o suporte à rede local e à base de dados podem criar outros problemas, tais como, incompatibilidade com versões anteriores e lentidão no acesso à base de dados.

Para resolver esse problema o que se necessita é uma plataforma de desenvolvimento que trabalhe de maneira igual em qualquer tipo computador, que não se importe com o tipo de dados que se está utilizando e nem com o sistema operacional no qual o servidor de base de dados esteja sendo executado. Nesse contexto, a internet pode ser uma solução, no que diz respeito à plataforma de desenvolvimento desse sistema através da *Web* utilizando o modelo cliente/servidor.

Uma aplicação que seja desenvolvida sobre a *Web* pode permitir que usuários possam interagir de forma simples e intuitiva através de interfaces gráficas com os algoritmos de reconhecimento de padrões, com o acesso a base de dados e à transferência de informações pela rede. Quando passamos a pensar em utilizar a internet como meio de transporte de dados num sistema de identificação, nos deparamos com certas características inerentes ao conceito da internet que permite que a implementação do sistema proposto seja mais simples e menos custosa. As características a que nos referimos são as seguintes:

- Escrita de aplicações numa linguagem padrão
- Interface gráfica com usuários
- Suporte multiplataforma
- Suporte de rede

A seguir descreveremos sucintamente cada uma dessas características, destacando suas vantagens junto ao sistema de identificação implementado.

6.5.1 Escrevendo Aplicações em Linguagem Padrão

O código *HyperText Markup Language* (HTML), permite escrever aplicações que são acessíveis a partir da maioria dos tipos de computadores através de *browsers* [89]. A utilização desse código nos limita a ter que aprender uma única linguagem, os componentes necessários para criar aplicações utilizando HTML são geralmente disponíveis a baixo custo, e qualquer tipo de mudança pode ser feita de maneira rápida.

Porém existem algumas limitações ao uso do HTML, visto que não é uma linguagem de programação "real". Isso significa que não executa instruções que respondem a uma entrada de dados ou que realizam cálculos. O HTML é eficiente para criar aplicações gráficas rapidamente as quais necessitem de uma funcionalidade simples.

Para aplicações mais complicadas, o HTML contém uma porta de entrada para programas, denominada de *Common Gateway Interface* (CGI), a qual permite chamar programas externos a partir do código HTML e enviar de volta o resultado dessa operação.

6.5.2 Interface Gráfica com Usuários

Em qualquer sistema que vise sua utilização por um usuário final, é extremamente necessário uma interface amigável que permita a esse usuário o fácil manuseio dos dados dentro do sistema. Assim, a utilização de uma interface gráfica com o usuário (Graphical User Interface - GUI) nos permite fazer isso, como também pode prevenir a entrada de dados errados, ou no mínimo limitá-los.

Os *browsers* são os aplicativos que interpretam o código escrito em HTML. Existem *browsers* disponíveis para a maioria dos sistemas operacionais. Programas escritos em HTML para um tipo de máquina podem ser executados por outra máquinas no *browser* específico daquele computador. Ao se utilizar um *browser*, em vez de investir tempo em desenvolver uma nova GUI para cada plataforma em que desejarmos colocar o sistema, gastamos apenas um curto tempo na elaboração de um código funcional e o *browser* se encarrega de todas as funções de interface final com os usuários - o *front end*. Essas funções podem ser: reações a seleções de menus, a movimentação, diminuição ou aumento do tamanho de janelas, a mudança do formato do cursor do *mouse* dependendo de sua posição na janela, entre outras.

Uma das principais vantagens ao se utilizar um *browser*, é que o código que ele executa é

sempre uma cópia do código que se encontra no servidor *Web*. Dessa forma é possível que, ao escrevermos um programa no servidor *Web* (programa CGI) e fazermos uma modificação posterior no código desse programa, fica garantido que o *browser* sempre executará a versão atualizada. Assim sendo, evitamos de nos preocupar com o problema de controlar diferentes versões de programas que são executadas em máquinas diferentes.

6.5.3 Suporte Multiplataforma

Uma característica dos *browsers* é que eles são disponíveis para os mais variados sistemas operacionais. Assim sendo, ao manter os programas CGI sendo executados no servidor *Web*, máquinas de sistemas operacionais como UNIX, Windows ou Macintosh podem ter acesso às informações sem nos preocuparmos em criar programas específicos para essas plataformas.

6.5.4 Suporte de Rede

Tanto os *browsers* quantos os servidores *Web* tem embutidos neles funções para transferência de dados via rede de computadores (Protocolo HTPP sobre TCP/IP). Esses aplicativos foram projetados para enviar e receber informação via internet ou intranet, de uma máquina para outra sem a necessidade de outro programa específico. Essa característica nos libera da necessidade de aprender outros protocolos de comunicação entre redes ou entre máquinas, o que poupa uma grande quantidade de tempo durante o desenvolvimento do sistema.

6.6 Common Gateway Interface (CGI)

Como mencionado na seção 6.5.1, o código HTML possui uma porta de entrada/saída de comunicação com programas mais complexos que podem realizar as mais diferentes tarefas no servidor *Web*. Essa interface de comunicação é chamada de Common Gateway Interface (CGI). Os programas que utilizam CGI para executar alguma tarefa são chamados de *Programas CGI* ou *Programas de Gateway*.

O código HTML que o servidor *Web* envia para o *browser* é um documento estático, isto é, o arquivo texto associado a uma determinada página não muda. Por outro lado, um programa CGI que é executado em tempo real, permite que lhe sejam enviadas informações, realize algum tipo de operação e retorne uma página HTML atualizada segundo as informações que lhe foram

enviadas como entrada. Ou seja, programas CGI podem gerar páginas HTML dinamicamente.

6.6.1 Programas CGI

A figura 6.7 mostra o acesso a um programa CGI graficamente.

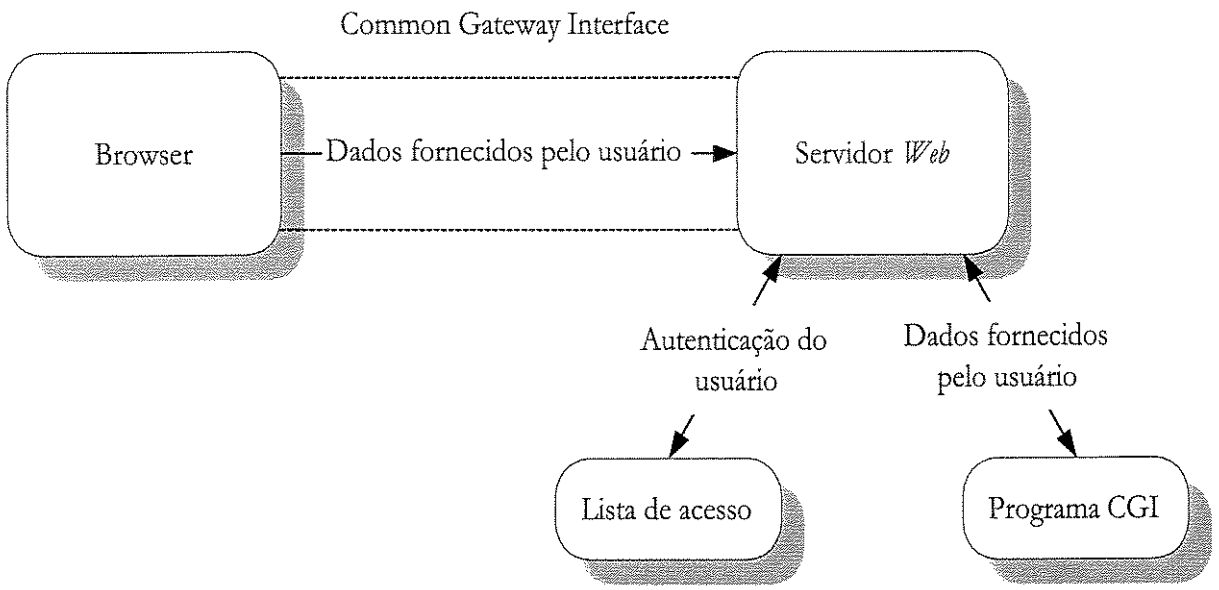


Figura 6.6: Processo de acesso a um programa CGI

Várias processos devem ocorrer para que um programa CGI possa ser executado com sucesso:

1. O usuário chama o programa CGI clicando em um *link* ou pressionando um botão.
2. O *browser* contata o servidor *Web* perguntando se ele tem permissão para executar o programa CGI.
3. O servidor *Web* verifica seus arquivos de configuração e acesso para descobrir se o usuário tem permissão para executar o programa CGI.
4. O servidor *Web* verifica se o programa CGI que está sendo requisitado existe. Se ele existir, o programa CGI é executado.
5. Qualquer resultado produzido pelo programa CGI é retornado para o *browser*.
6. O *browser* mostra a saída do programa CGI.

A informação passada do *browser* para o programa CGI pode ser feita de várias maneiras e o resultado dessa operação pode retornar resultados do tipo: código HTML, texto puro, imagens ou uma mistura deles todos.

No contexto de um sistema de identificação pessoal via internet, os programas CGI executam a extração de característica biométricas, cadastramento de dados e interface de acesso à base de dados. O servidor *Web* faz a interface entre os comandos dados pelo usuário através do *browser* e os programas CGI.

CAPÍTULO 7

UM SISTEMA DE IDENTIFICAÇÃO PESSOAL

Neste capítulo descrevemos o sistema biométrico de identificação pessoal via internet que foi implementado. Apresentamos o gerenciador de base de dados, o servidor Web, os programas CGI e a interface com o usuário que compõem o sistema de identificação.

7.1 Introdução

Desde o final do século XIX, as evoluções tecnológicas nos campos da eletrônica e comunicação vêm causando grande impacto na sociedade. Esse impacto quase sempre se traduz na forma de mudanças nos costumes, no comércio, indústria, educação, política, etc.. Foi assim com o surgimento do telex, do telefone, do rádio, da televisão, dos satélites e, mais recentemente, da telefonia celular. Na aurora do século XXI, uma nova evolução tecnológica no campo de redes de comunicações se consagrou e motivou profundas transformações em todos os setores da sociedade: *a internet.*

Através da internet é possível realizar os mais diversos tipos de troca de informações e receber serviços, como correio eletrônico, envio e recebimento de arquivos, propaganda, conversação *on-line* (em tempo real), acesso a base de dados remotos, transações comerciais, dentre outras. Assim, estamos no início de uma nova era, onde não há mais fronteiras para a comunicação.

Na chamada era da informação, na qual a informação toma lugar ao lado do capital, como principal valor para a sociedade, é natural a busca e até mesmo a disputa pelo maior número de

informações possíveis. Como conseqüência, é previsível o aparecimento de atividades ilegais e criminosas no que diz respeito a obtenção de informação. Nesse contexto, surge a figura do ladrão de informação ou *hacker*, especializado em furtar informações de terceiros e utilizá-las em proveito próprio. Os danos causados por esse tipo de atividade toma uma dimensão muito maior quando a informação que é furtada pode ser utilizada para desfalcar financeiramente seu legítimo proprietário. Um exemplo típico é o caso da realização de transações comerciais através de redes de computadores com uso de cartões de crédito. Durante a transação, o *hacker* pode introduzir-se sem ser percebido e obter informações do número e senha do cartão e posteriormente efetuar compras como se fosse o titular da conta.

Em outras palavras, hoje um servidor de rede de computadores pode afirmar a conta utilizada, a máquina (computador), a sub-rede, a rede, a instituição e o país a que determinado usuário está conectado na rede. Porém, não pode efetivamente identificar quem é a pessoa (usuário) que está utilizando essa máquina. Um caminho, ainda pouco explorado, que deve ser seguido no sentido de oferecer serviços de proteção via internet, não somente para os usuários dessa grande rede, mas para toda a população, diz respeito a Identificação Pessoal via Internet.

7.2 Gerenciador de base de dados

Para manter as informações referentes ao cadastro de usuários e aos dados necessários para implementar as várias formas de identificação pessoal, propomos a utilização de um gerenciador de base de dados (GBD). Com essa abordagem podemos excluir dos módulos referentes aos diferentes métodos de identificação pessoal a tarefa de lidar com os detalhes relativos ao armazenamento de informações e assim, deixar o sistema portável para outros ambientes.

Uma das propriedades do GBD utilizado em nosso trabalho é a de suportar ambientes tanto em redes locais como em redes a longa distância, onde vários usuários poderão solicitar o serviço de identificação pessoal ao mesmo tempo e de diferentes pontos geográficos. Além disso, esse processo pode ser realizado em tempo real.

Outra propriedade que o GBD possui é a possibilidade de desenvolver aplicativos independentes para cada tipo de características usadas na identificação. Essa independência possibilita a utilização do mesmo sistema para diversos fins e ao mesmo tempo. Por exemplo, imagine que o sistema esteja sendo utilizado em uma agência bancária que possui um sistema automatizado disposto em uma rede local, interligado a uma rede de longa distância onde se localiza a base de dados com as informações sobre todos os clientes e funcionários. Nessa

agência, poder-se-ia utilizar ao mesmo tempo, com finalidades diferentes, pelo menos três aplicativos de verificação de identidade. Nos caixas, poder-se-ia utilizar o módulo de verificação de assinaturas que junto à base de dados, comprovaria a validade da assinatura em um cheque ou documento recebido. Entre os funcionários, poder-se-ia utilizar o módulo de verificação por impressões digitais para autorizar operações de mais alta importância. E ainda, os próprios clientes poderiam utilizar o módulo de verificação de faces ligados aos caixas eletrônicos para efetuar saques em dinheiro, solicitar transferências, etc.. Nesse exemplo, fica claro que há maior ganho de eficiência deixando para o GBD o controle das informações centralizadas de clientes e funcionários, pois não é necessário manter os mesmos registros em vários locais diferentes, o que acarreta inúmeros problemas de integridade de dados. A interação entre alguns módulos de identificação pessoal e o GBD pode ser vista na figura 7.1.

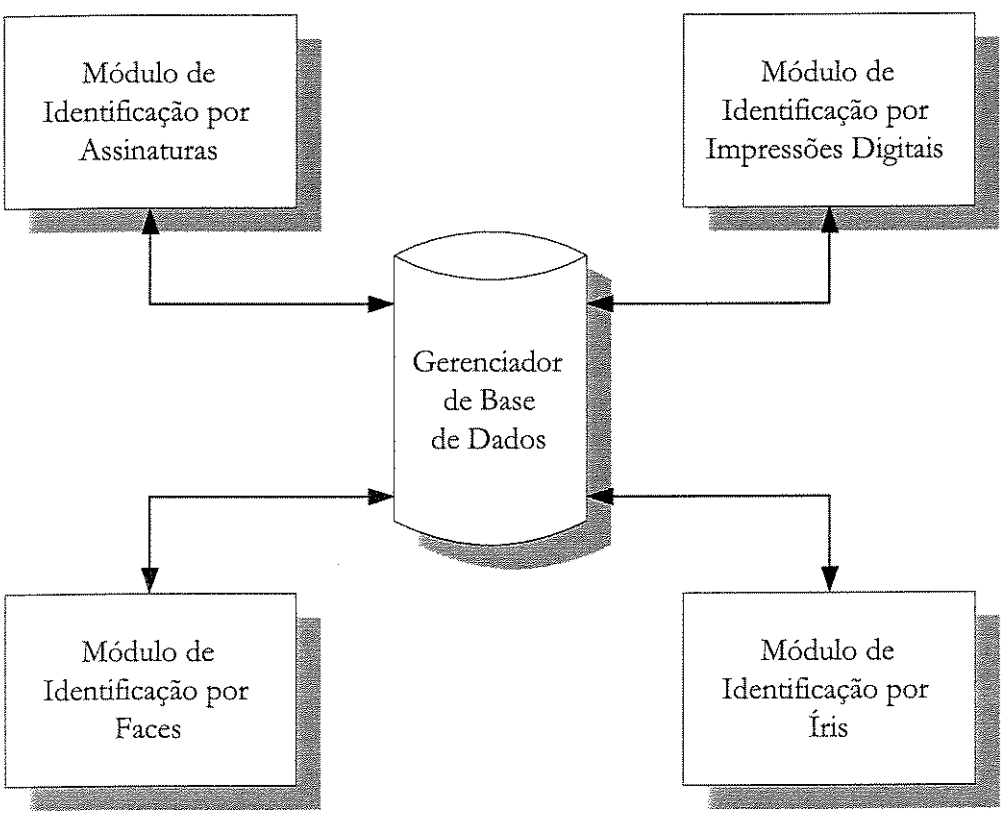


Figura 7.1: Relacionamentos entre módulos de identificação com o GBD.

Conforme apresentado no diagrama da figura 7.1, o relacionamento, do ponto de vista lógico, entre a base de dados e os módulos de identificação existe de forma exclusiva para cada um dos mesmos.

Por outro lado, ainda que os módulos sejam independentes entre si, existe a possibilidade da implementação de novos módulos ligados ao GBD que relacionem os dados adquiridos previamente pelos módulos de identificação.

Na atual implementação do sistema , cada um dos módulos de identificação pessoal, possui três sub-módulos.

1. Sub-módulo de cadastramento
2. Sub-módulo de visualização
3. Sub-módulo de verificação automática

A solicitação de informações ao GBD por parte dos módulos de identificação pessoal e consequentemente pelo sub-módulos a eles pertencentes é feita através de mensagens.

No caso do sub-módulo de cadastramento, as mensagens enviadas ao GBD se encarregam de criar o perfil de um novo cliente a ser cadastrado. Se o cliente ainda não existir, é criado na tabela de usuários, o registro de um novo cliente. Isso é feito enviando as informações do nome do cliente (*login*), número de identidade do cliente (ID), vetor de características médio referente à característica biométrica que desejamos cadastrar, o limiar de decisão e três arquivos de imagens. Por outro lado, se o cliente já existir, o GBD sinaliza que o cliente já foi cadastrado e pergunta se desejaríamos fazer uma atualização na base de dados.

No caso do sub-módulo de visualização, as mensagens enviadas ao GBD são o *login* e ID do cliente. A resposta do GBD a essas mensagens é o envio de uma imagem. Note que dependendo do sub-módulo que fez o pedido, a imagem que for retornada pelo GBD será diferente, por exemplo, se o sub-módulo que fez o pedido é o de visualização de assinaturas, a imagem será de uma assinatura, por outro lado se o sub-módulo que fez o pedido é o de visualização de impressões digitais, a imagem será de uma impressão digital e assim para cada módulo de visualização específico.

No caso do sub-módulo de verificação automática, as mensagens enviadas ao GBD são o *login* e ID. O GBD retornará um vetor de características médio, informações sobre o limiar de decisão e uma imagem. De modo semelhante ao caso do sub-módulo de visualização, as

informações que retornam do GBD estão relacionadas com o tipo de característica de identificação que se deseja utilizar. A figura 7.2 apresenta um diagrama do relacionamento entre o GBD e os módulos de identificação.

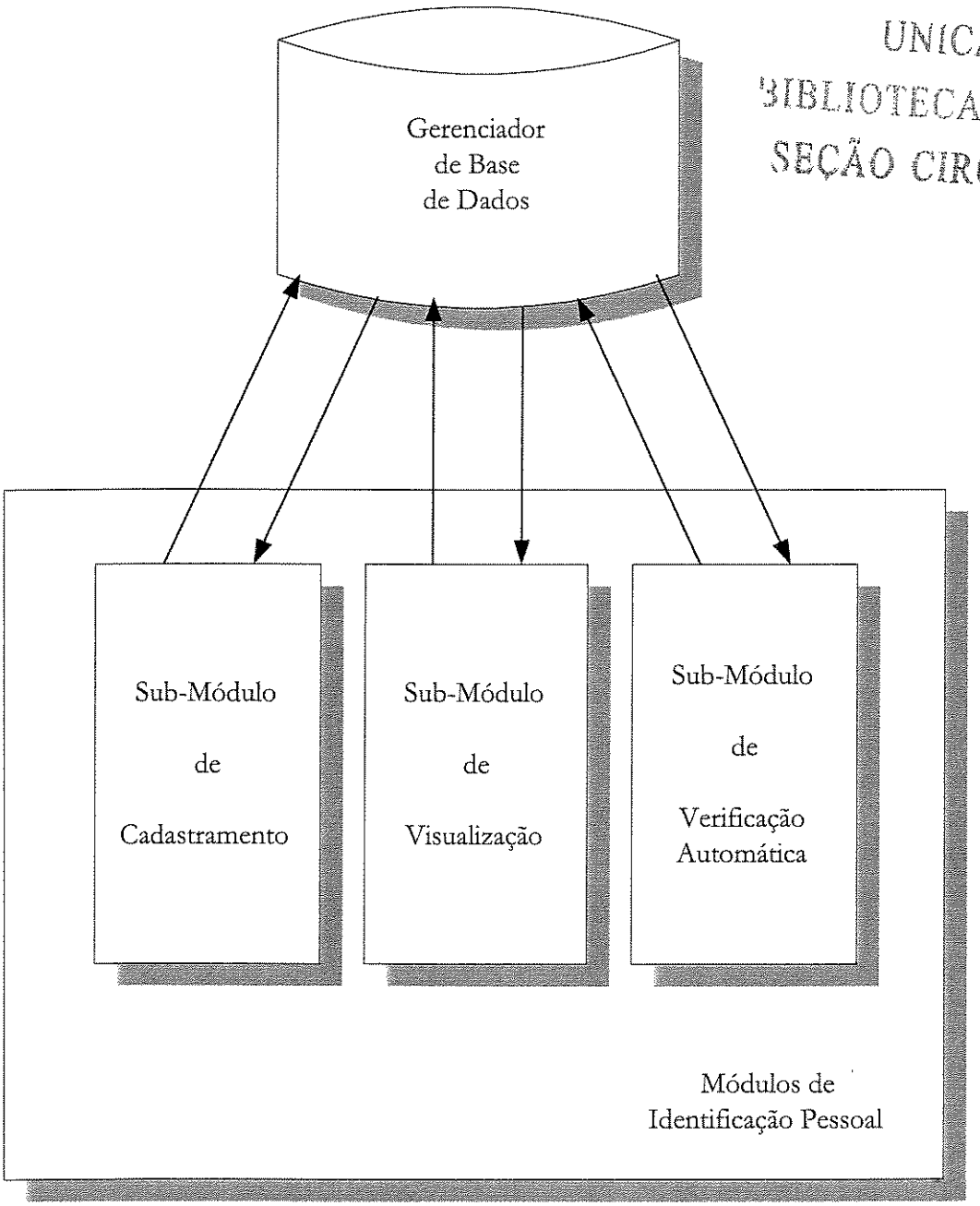


Figura 7.2: Diagrama do relacionamento entre o GBD e os módulos de identificação.

O gerenciador de base de dados que foi adotado para fazer parte do nosso sistema biométrico de identificação pessoal via internet foi o *Mini SQL* [90]. O Mini SQL ou mSQL é um gerenciador de base de dado que foi desenvolvido para prover acesso rápido a dados armazenados a baixo custo computacional. O mSQL oferece um sub-conjunto de instruções do SQL padrão [91]. Essas instruções são na prática as mensagens que são compartilhadas entre os módulos de identificação e o GBD.

7.3 Modelo de um Sistema de Identificação Pessoal via Internet

Uma das características mais importantes no sistema de identificação proposto é que pode ser utilizado por vários usuários ao mesmo tempo. Dispondo dessa característica, é possível utilizá-lo em atividades que necessitem de formas de identificação diferentes para os mesmos indivíduos. Outro ponto fundamental, é que as informações necessárias às várias formas de identificação, podem ser unicamente mantidas, ou seja, não ocorre duplicação de informações que podem comprometer a integridade dos dados.

Desenvolvido para operar em um ambiente de redes de computadores o sistema apresenta ao usuário, em qualquer ponto da rede, as mesmas funcionalidades escondendo detalhes operacionais que não sejam relevantes ao uso do sistema. Por exemplo, as informações referentes às características a serem verificadas podem ser centralizadas em um único ponto da rede ou podem ser divididas em vários locais de acordo com a maior utilização de um modo de identificação específico.

Além disso, informações referentes às características biométricas, podem ser compartilhadas por um número maior de aplicações. Entre essas aplicações podemos destacar o uso em transações comerciais que necessitem de comprovação de identidade, por exemplo, a utilização de cartões de créditos. Nesse caso, o comerciante poderia rapidamente fazer uma consulta via internet para verificar se a assinatura do cliente que está efetuando a compra é igual à assinatura do dono do cartão de crédito. Fica claro também, que qualquer sistema de segurança pode utilizar a base de informações via rede para habilitar o acesso de um usuário a algum local ou serviço. No entanto, deve-se ressaltar que as informações passadas via rede de computadores devem estar devidamente criptografadas para evitar possível interferência de terceiros no processo.

A execução de uma operação de cadastramento, visualização ou verificação automática via rede de computadores é feita através da utilização de páginas *Web*, preparadas para dar suporte às aplicações. Dentro desse contexto, apresentamos um modelo de sistema automatizado de cadastramento, consulta e verificação de características biométricas via a internet como mostrada na figura 7.3.

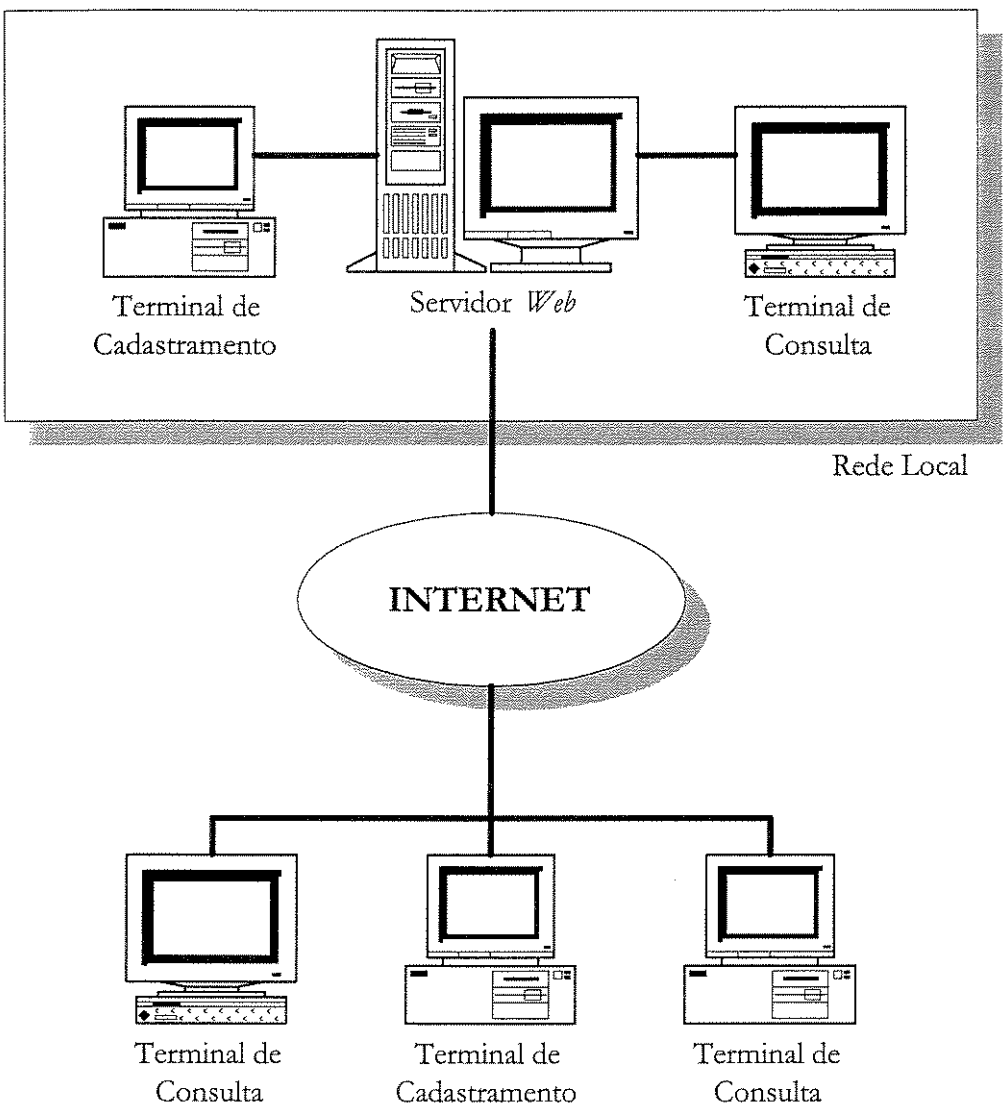


Figura 7.3: Sistema automatizado de cadastramento, consulta e verificação de característica biométricas.

A seguir faremos a descrição das funcionalidades dos terminais de computadores apresentados no modelo da figura 7.3:

- Servidor Web: responsável pelo gerenciamento da comunicação e tratamento das informações entre os terminais ligados à rede. Processa os pedidos de acesso a programas CGI que permitem o cadastramento, consulta e verificação de características biométricas. Na implementação atual do sistema, o programa servidor *Web* utilizado é o *Apache Web Server* [92]. Na mesma máquina em que reside o servidor *Web*, está instalado o programa mSQL que gerencia a base dados.

- Terminais de consulta: através deles são enviados os pedidos de consulta ao servidor *Web*, que por sua vez disponibiliza o acesso à base de dados para verificação e/ou visualização.

- Terminais de cadastramento: além de também serem terminais de consulta, possuem a capacidade de aquisição de sinais biométricos.

7.4 Implementação do Sistema de Identificação

Na implementação do sistema de identificação proposto, foi utilizado o modelo descrito na seção 7.3. O módulo de identificação implementado foi o módulo de assinaturas utilizando os vetores de características e algoritmos de reconhecimento de padrões descritos no capítulo 5. A seguir descreveremos detalhadamente o módulo de identificação por assinatura, composto pelos sub-módulos de cadastramento, visualização e verificação automática. Para cada um desses sub-módulos apresentaremos os programas CGI associados aos mesmos e suas interfaces com o usuário.

7.4.1 Cadastramento

O sub-módulo de cadastramento é composto por cinco programas CGI. Fisicamente esses programas se encontram na máquina 143.106.50.11 do LRPRC.

Os programas CGI do módulo de cadastramento são enroll1.cgi, enroll2.cgi, enroll3.cgi, enroll4.cgi e enroll5.cgi.

Os programas enroll1.cgi e enroll5.cgi foram feitos em linguagem C e compilados na plataforma Linux. Os programas enroll2, enroll3 e enroll4 são programas em PERL e utilizam o interpretador PERL instalado em 143.106.50.11.

7.4.1.1 Programa ENROLL1.CGI

Inicialmente aparece a tela mostrada na figura 7.4. Nessa tela é pedido para entrar com o nome e número de identificação do cliente a ser cadastrado.

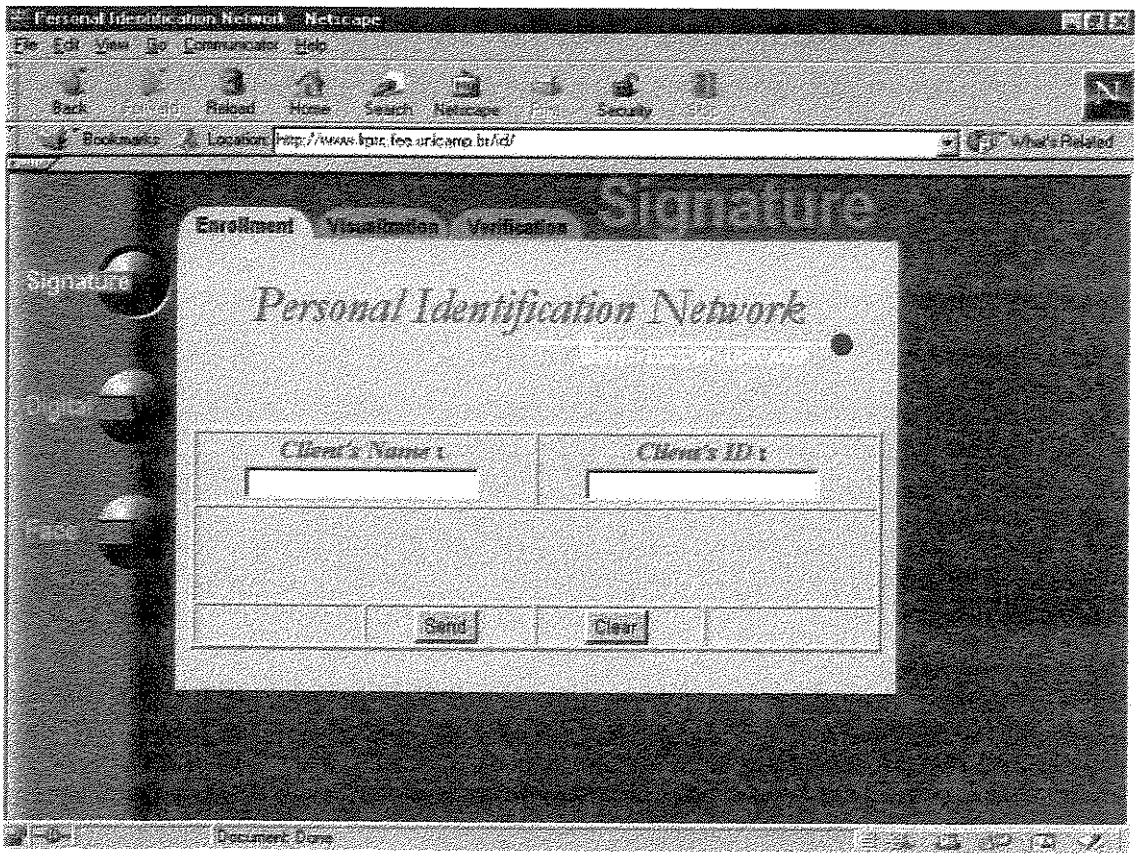


Figura 7.4: Tela inicial do sistema de identificação pessoal.

Após entrar com o nome do cliente e ID, temos a opção de enviar a informação clicando em ***Send***, ou reentrar com os dados clicando em ***Clear***.

Uma vez preenchido os campos indicados na interface, clicamos em ***Send*** e enviamos a informação. A seguir será mostrado uma tela como apresentada na figura 7.5.

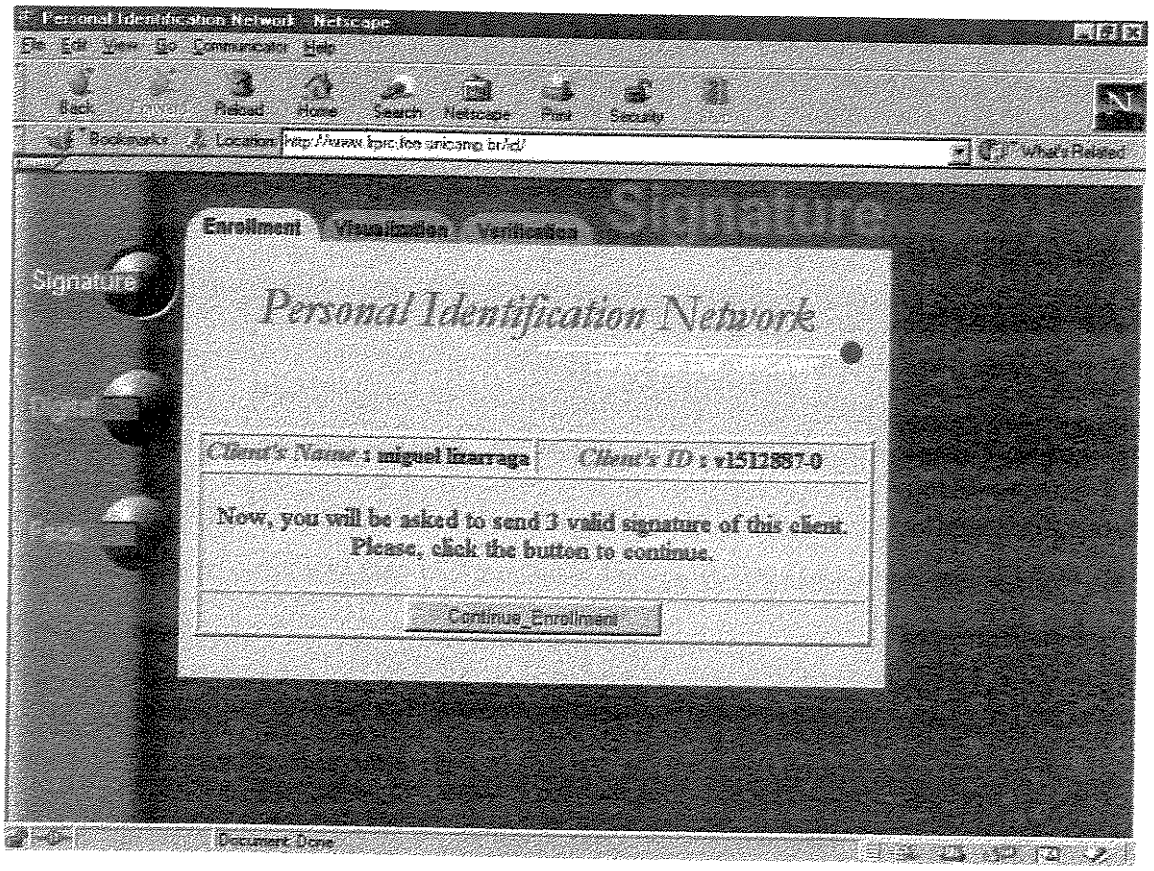


Figura 7.5: Dados do cliente recebidos pelo servidor *Web*.

A tela da figura 7.5 nos informa que o servidor *Web* recebeu os dados enviados a partir do *browser*. Internamente o programa enroll1.cgi, cria um arquivo chamado de **enroll_temp.txt**. Esse arquivo guarda a informação do nome do cliente e do seu ID temporariamente, isto é, até que o processo de cadastramento seja completado e as informações do clientes passem definitivamente para o servidor de base de dados. Essa tela ainda nos informa que serão pedidas 3 imagens de assinaturas válidas para o cadastramento do cliente. Para prosseguir é necessário clicar no botão **Continue_Enrollment**.

7.4.1.2 Programa ENROLL2.CGI

A continuação, a tela apresentada na figura 7.6 aparece. Essa tela é criada em tempo real pelo programa enroll2.cgi Nessa tela é pedido para se entrar com a primeira imagem da assinatura. Isso pode ser feito de duas maneiras. Digitando diretamente no campo ***File name*** o caminho onde está o arquivo, ou apertando o botão ***Browse***.

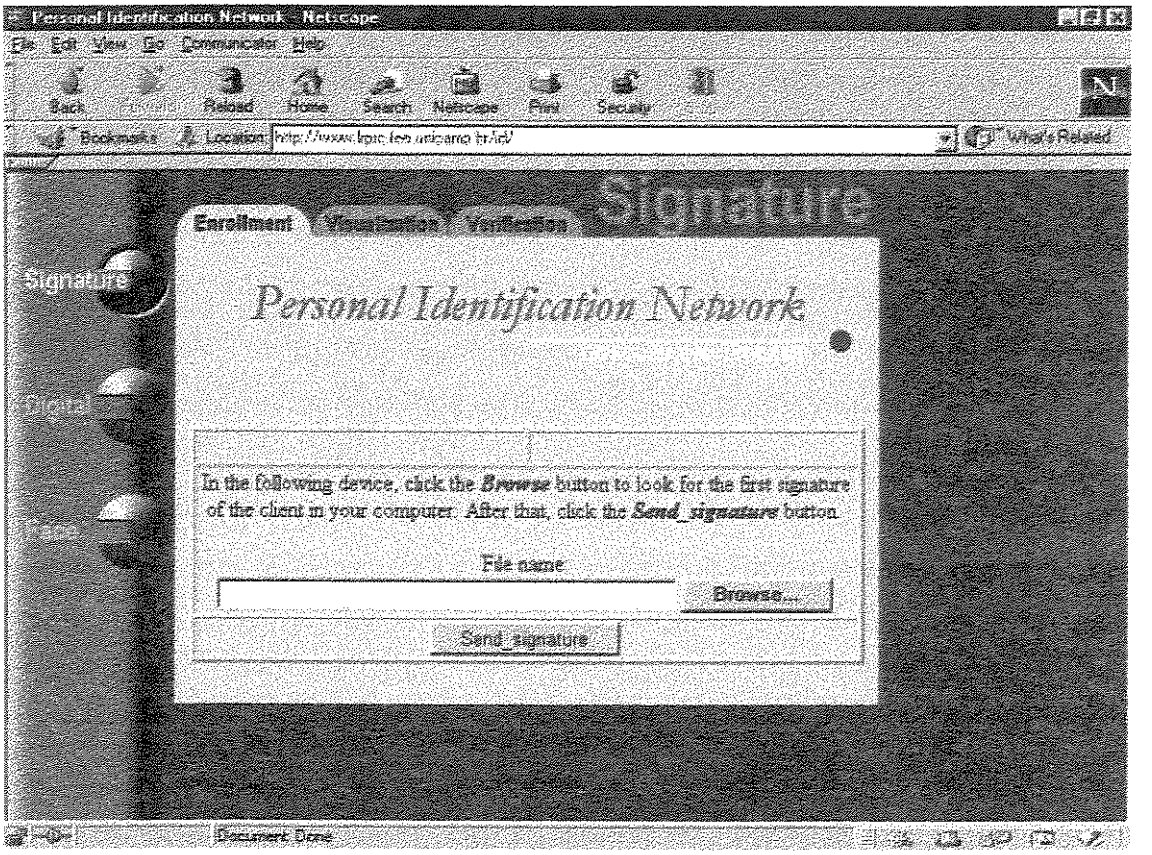


Figura 7.6: Pedido da primeira imagem de assinatura.

Quando o botão ***Browse*** é apertado aparece uma janela tipo *pop-up* como o da figura 7.7.

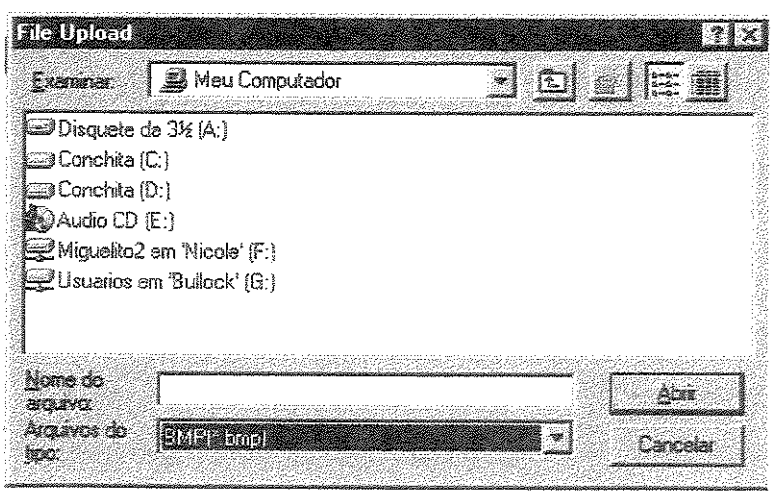


Figura 7.7: Janela *pop-up* para a escolha de uma assinatura.

Como o arquivo que devemos enviar é de algum tipo de imagem, é importante que se clique no campo "Arquivos do tipo" e mudemos a opção *default* do *browser* para visualizar arquivos do tipo, por exemplo, BMP. Dessa forma conseguiremos achar todos os arquivos que possuem essa extensão.

Uma vez encontrado o arquivo desejado, apertar "Abrir". Isso fará com que o campo ***File name*** fique preenchido pelo caminho do arquivo da imagem encolhido. Em seguida clique no botão ***Send_signature.***

Quando o servidor *Web* recebe o arquivo da imagem, é mostrada uma tela como vista na figura 7.8.

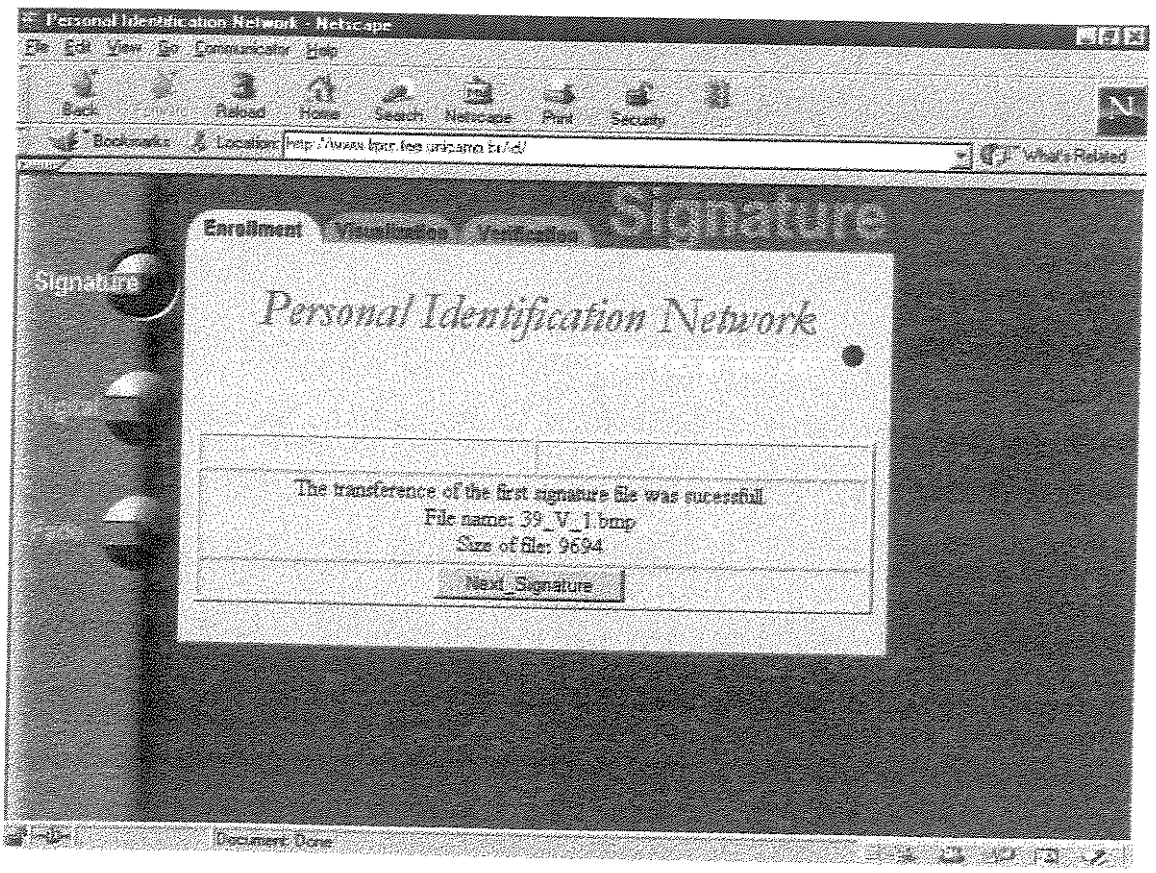


Figura 7.8: Transferência do arquivo com sucesso.

Essa tela informa que a transferência da assinatura foi feita com sucesso, indicando o nome do arquivo que foi recebido e o seu tamanho. Para prosseguir clique no botão **Next_Signature.**

7.4.1.3 Programa ENROLL3.CGI

O programa enroll3.cgi realiza as mesmas tarefas e apresenta a mesma interface que o programa enroll2.cgi.

7.4.1.4 Programa ENROLL4. CGI

O programa enroll4.cgi realiza as mesmas tarefas e a apresenta a mesma interface que o programa enroll2.cgi. Existe apenas uma única diferença na interface, é que após a tela sobre a informação do recebimento da assinatura, deve-se clicar o botão **Image_Validation**.

7.4.1.5 Programa ENROLL5.CGI

O programa enroll5.cgi executa as seguintes passos:

1. Verifica se os arquivos enviados foram arquivos de imagens binárias. Em caso negativo aparecerá uma mensagem de erro pedindo para repetir todo o processo.
2. Se o passo 1 for positivo será iniciado os seguinte processos:
   - 2.1 Realizar o corte dos traços estilísticos da imagem da assinatura.
   - 2.2 Normalizar as imagens nas escalas 64 e 256.
   - 2.3 Dividir a imagem de escala 256 em 5 quadros.
   - 2.4 Fazer a extração das características que compões os vetores de características de 1 a 7 e do vetor de correlação.
   - 2.5 Gerar os vetores de características médios dos vetores de características 1 a 7 e do vetor de correlação.
   - 2.6 Encontrar as distâncias dos vetores de correlação.
   - 2.7 Encontrar os valores dos limiares de decisão λ_1 e λ_2.
   - 2.8 Criar na tabela de usuários do gerenciador de base de dados um registro com o nome do cliente e o número de identificação do cliente.
   - 2.9 Enviar para o registro criado no item 2.8 uma das imagens de entrada, os vetores de características médios, os limiares de decisão.
   - 2.10 Apagar o arquivo temporário **enroll_temp.txt**.
   - 2.11 Exibir a tela que indica o final do cadastramento do cliente.

Uma amostra da tela que indica o final do cadastramento é mostrada na figura 7.9.

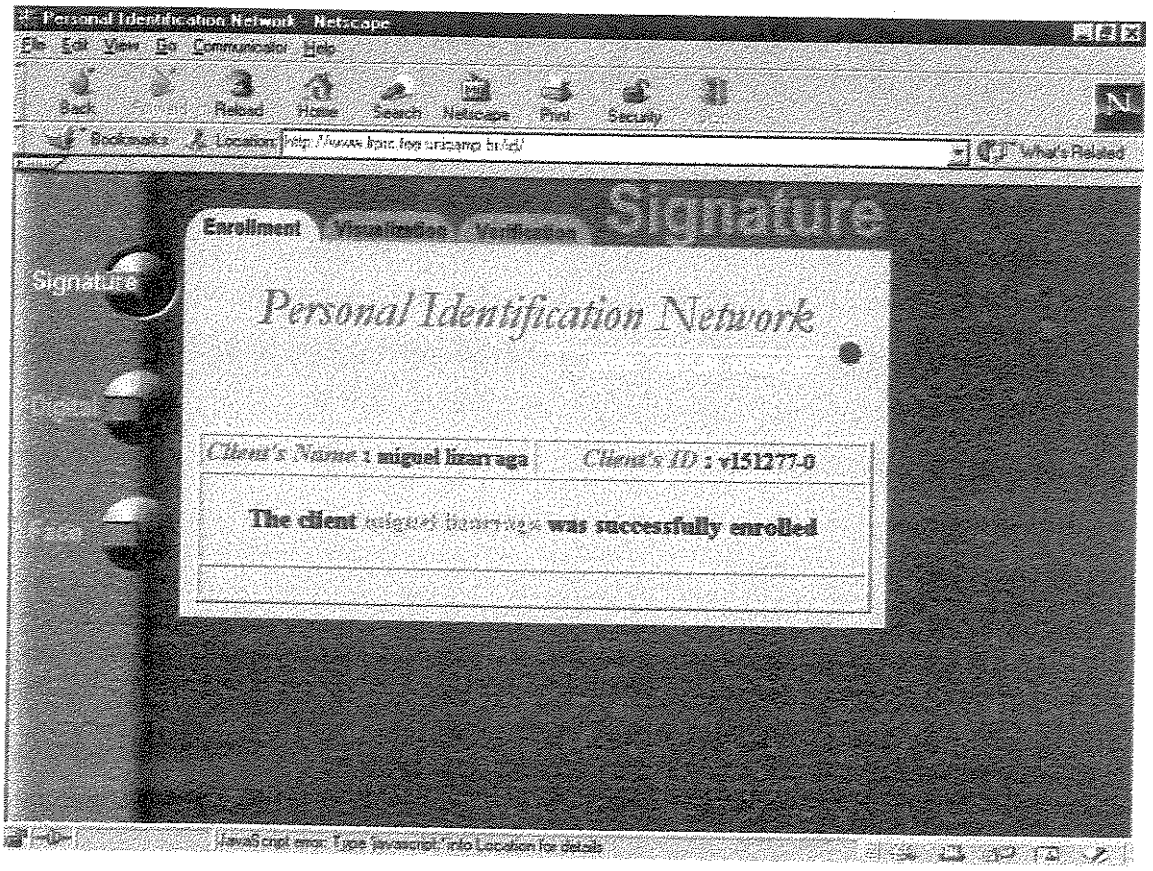


Figura 7.9: Cliente cadastrado com sucesso.

7.4.2 Visualização

O sub-módulo de visualização é composto por um programa CGI. Fisicamente esse programa se encontra na máquina 143.106.50.11 do LRPRC, foi feito em linguagem C e compilado na plataforma Linux.

7.4.2.1 Programa VISUAL1.CGI

A função de visualização foi implementada para permitir que no caso de um usuário desejar simplesmente fazer uma comparação visual entre uma assinatura que, por exemplo, esteja presente em um cheque, possa acessar a base de dados e ter uma amostra visual dessa assinatura (desde que previamente cadastrada).

Para iniciar o processo de visualização, clique no *tab* ***visualization*** na interface gráfica. A seguir aparecerá uma tela como a mostrada na figura 7.10. Nessa tela, é pedido para entrar com o

nome e número de identificação do cliente do qual desejamos visualizar a assinatura previamente cadastrada.

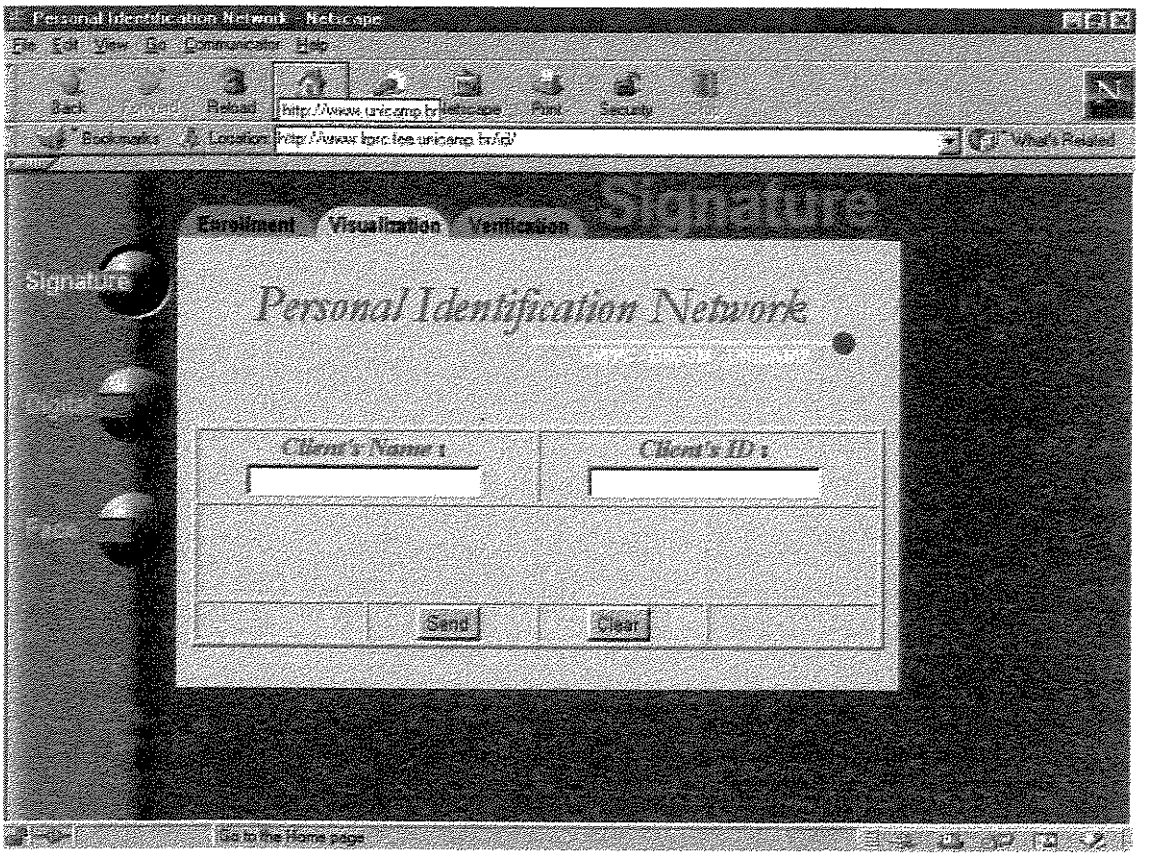


Figura 7.10: Entrada de dados para consulta de assinaturas.

Após entrar com o nome do cliente e ID, temos a opção de enviar a informação clicando no botão ***Send***, ou reentrar com os dados clicando no botão ***Clear***.

Clicando no botão ***Send*** enviamos a informação. Se não existir a pessoa cadastrada com o nome e ID enviados aparecerá uma mensagem como vista na figura 7.11:

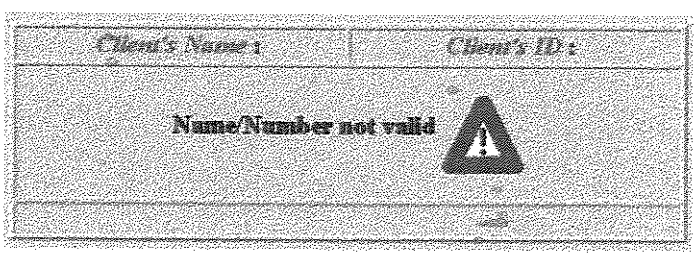


Figura 7.11: Nome ou número de identificação não válidos.

Em caso que o nome do cliente e o número identificação do cliente existirem, será apresentada uma tela como apresentada na figura 7.12.

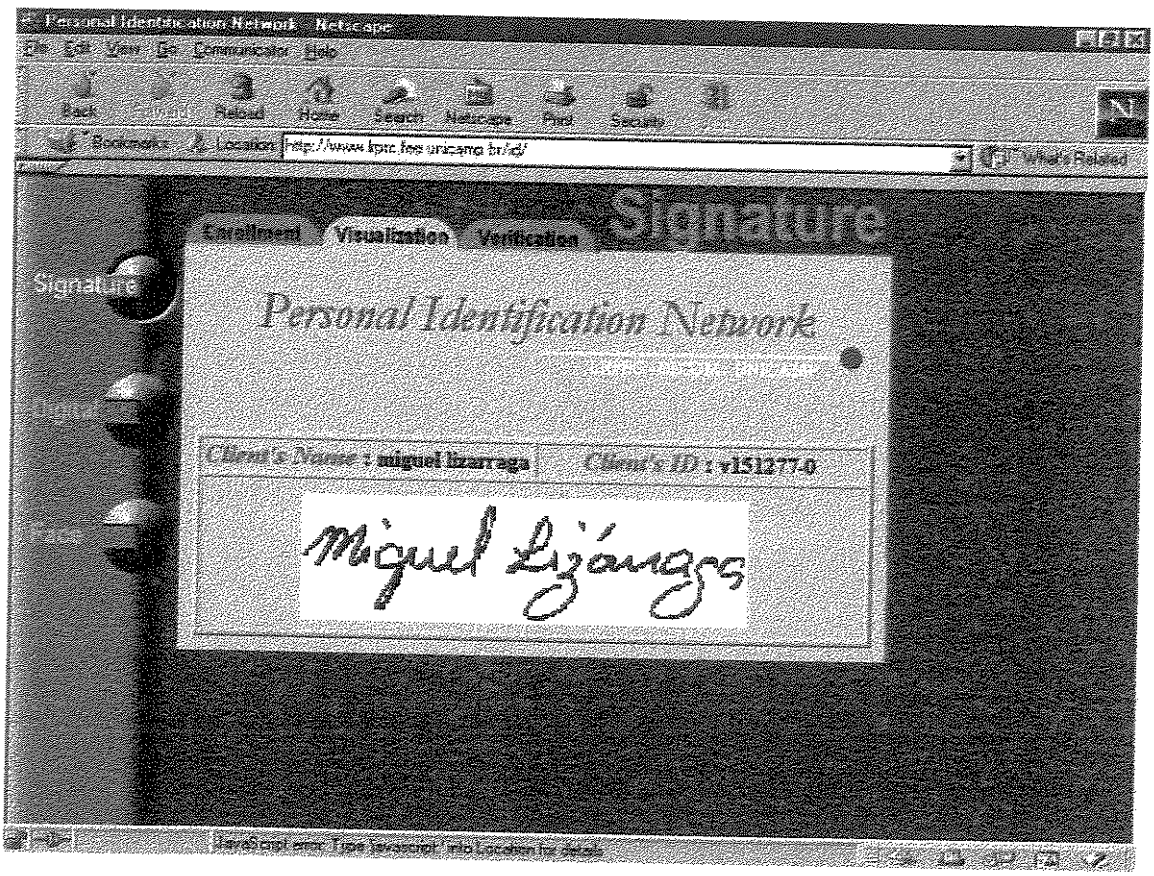


Figura 7.12: Visualização de uma imagem.

7.4.3 Verificação Automática

O sub-módulo de verificação automática de assinaturas é composto por três programas CGI. Fisicamente esses programas se encontram na máquina 143.106.50.11 no LRPRC. Os programas CGI do sub-módulo de verificação são verify1.cgi, verify2.cgi e verify3.cgi. Os programas verify1.cgi e verify3.cgi foram feitos em linguagem C e compilados em Linux. O programa verify2.cgi é um programa em PERL e utiliza o interpretador Perl instalado em 143.106.50.11.

7.4.3.1 Programa VERIFY1.CGI

Para iniciar o processo de verificação automática, clique no *tab* ***verification*** na interface gráfica. A seguir aparecerá uma tela como a mostrada na figura 7.13. Nessa tela, é pedido para entrar com o nome e número de identificação do cliente do qual desejamos verificar a assinatura automaticamente.

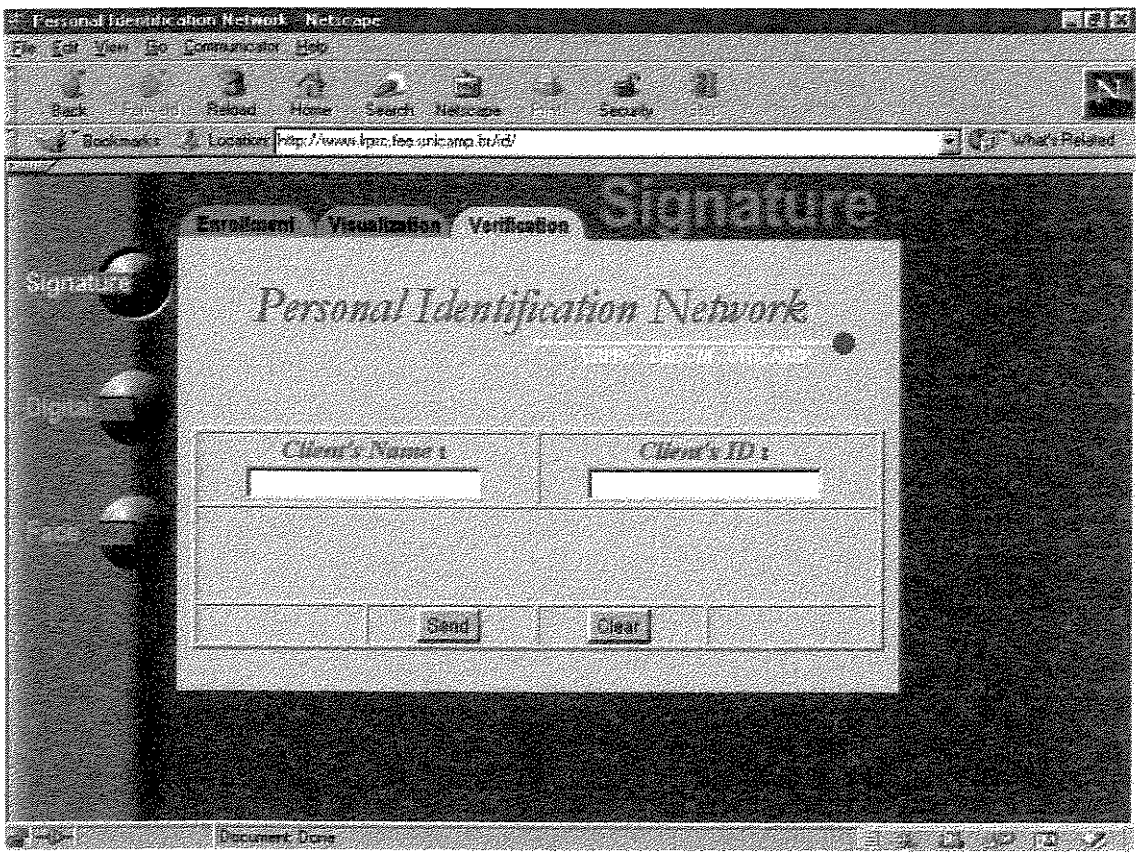


Figura 7.13: Verificação automática de assinaturas.

Após entrar com o nome do cliente e seu número de identificação, temos a opção de enviar a informação clicando no botão ***Send***, ou reentrar com os dados clicando no botão ***Clear***.

Clicando no botão ***Send*** enviamos a informação. Caso a informação enviada não pertencer a uma pessoa previamente cadastrada, aparecerá uma tela como apresentada na figura 7.14.

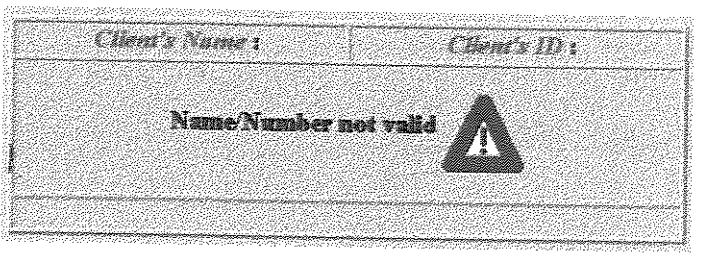


Figura 7.14: Nome ou número de identificação não válidos.

No caso do nome do cliente e número de identificação existirem, será apresentado uma tela como vista na figura 7.15.

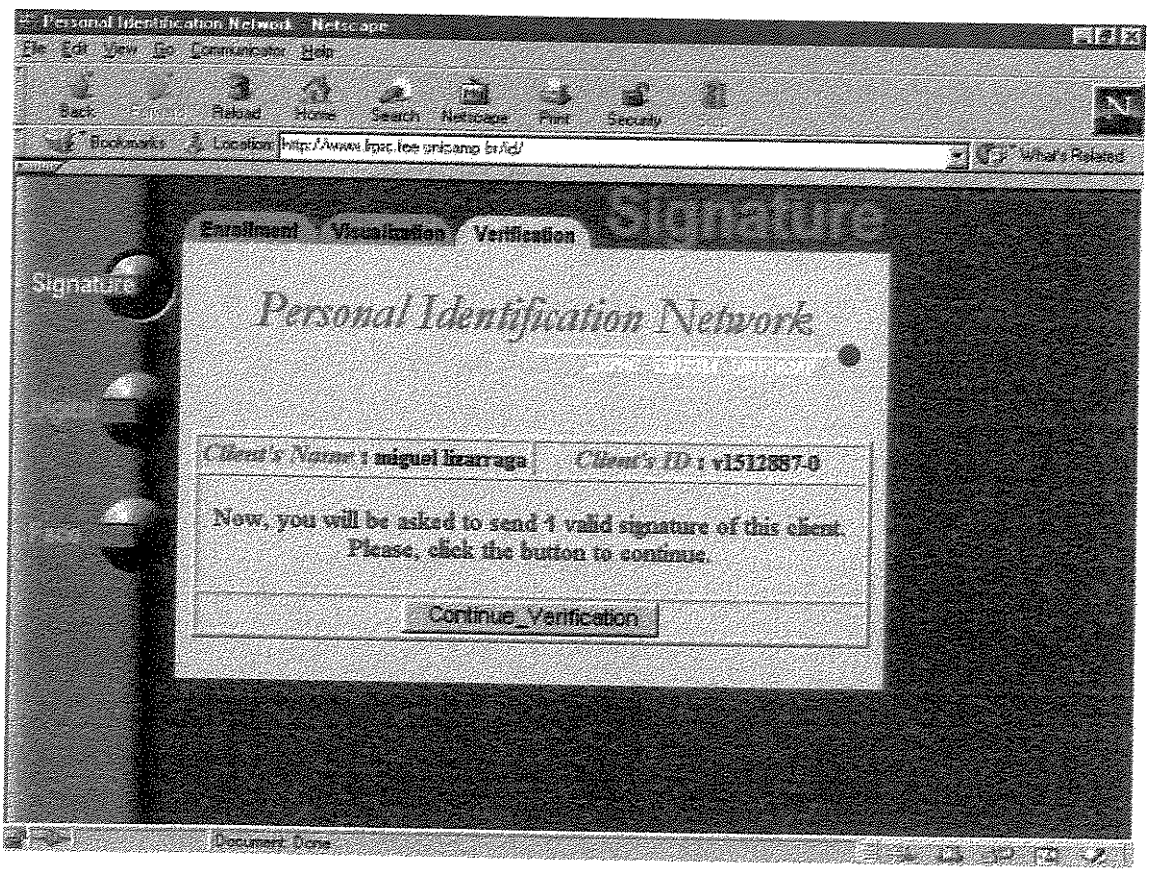


Figura 7.15: Dados do cliente recebidos pelo servidor *Web*.

A tela da figura 7.15 nos informa que o servidor *Web* recebeu os dados enviados a partir do *browser*. Essa tela ainda nos informa que será pedida 1 imagem de assinatura para ser utilizada

como entrada no processo de verificação automática. Para prosseguir é necessário clicar no botão **Continue_Verification**.

7.4.3.2 Programa VERIFY2.CGI

A continuação a tela apresentada na figura 7.16 aparece. Essa tela é criada em tempo real pelo programa verify2.cgi. Nessa tela é pedido para se entrar com a imagem de uma assinatura. Isso pode ser feito de duas maneiras. Digitando diretamente no campo ***File name*** o caminho onde está o arquivo, ou apertando o botão ***Browse***.

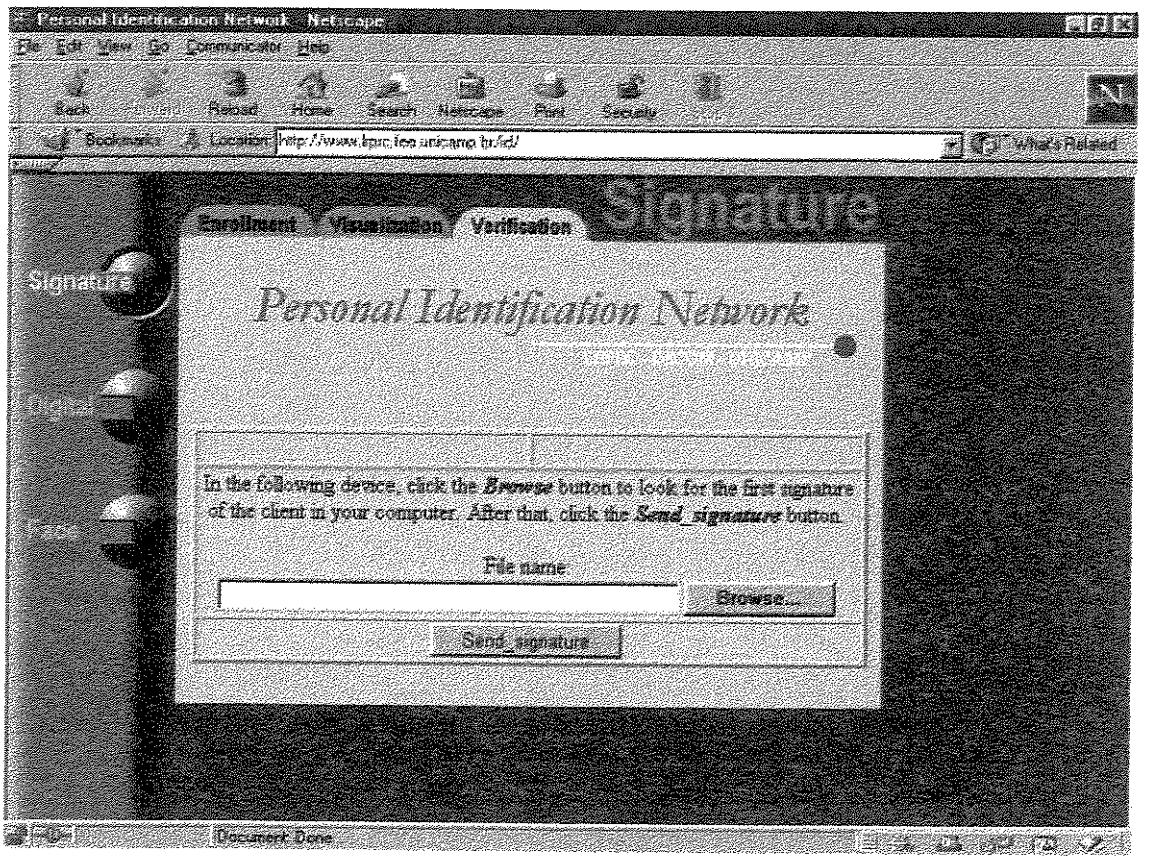


Figura 7.16: Pedido da imagem de uma assinatura.

Quando o botão ***Browse*** é apertado aparece uma janela tipo *pop-up* como a que foi previamente apresentada na figura 7.7.

Quando o servidor *Web* receber a imagem, será mostrada uma tela como vista na figura 7.17.

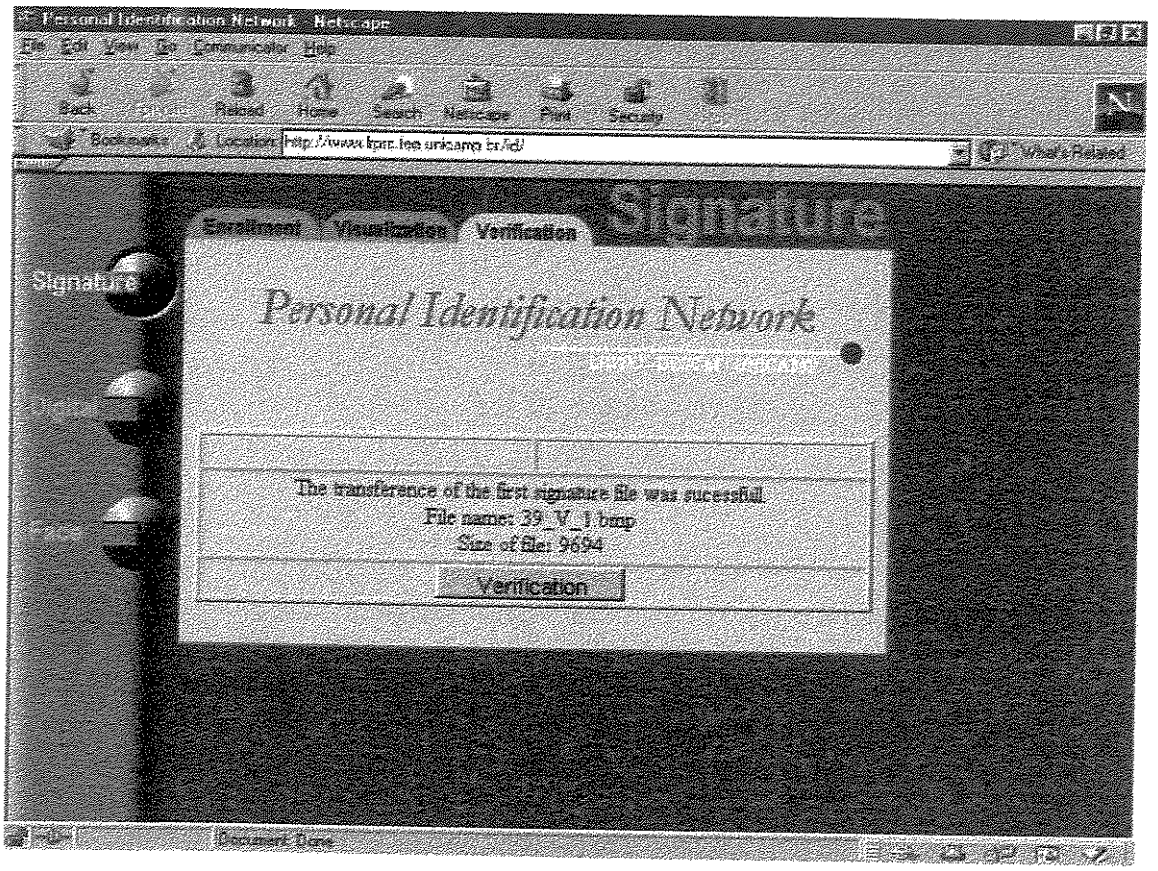


Figura 7.17: Transferência do arquivo com sucesso.

Essa tela informa que a transferência da assinatura foi feita com sucesso, indicando o nome do arquivo que foi recebido e seu tamanho. Para prosseguir clique no botão ***Verification.***

7.4.3.3 Programa VERIFY3.CGI

O programa verify3.cgi executa as seguintes passos:

1. Verifica se o arquivo enviado foi um arquivo de imagem binária. Em caso negativo aparecerá uma mensagem de erro pedindo para repetir todo o processo.
2. Se o passo 1 for positivo será iniciado os seguinte processos:
   2.1 Realizar o corte dos traços estilísticos da imagem da assinatura.
   2.2 Normalizar as imagens nas escalas 64 e 256.

2.3 Dividir a imagem de escala 256 em 5 quadros.

2.4 Fazer a extração das características que compõem os vetores de características de 1 a 7 e do vetor de correlação.

2.5 Encontrar a distância do vetor de correlação.

2.6 Encontrar as distâncias padrões dos vetores de características 1 a 7.

2.7 Mandar mensagens ao gerenciador de base de dados para enviar os vetores de características médios e limiares de decisão.

2.8 Executar o algoritmo multi-especialista de dois estágios como descrito no capítulo 5.

2.10 Exibir a tela apresentando o resultado da verificação automática.

Uma amostra da tela que apresenta o resultado da verificação automática pode ser vista na figura 7.18.

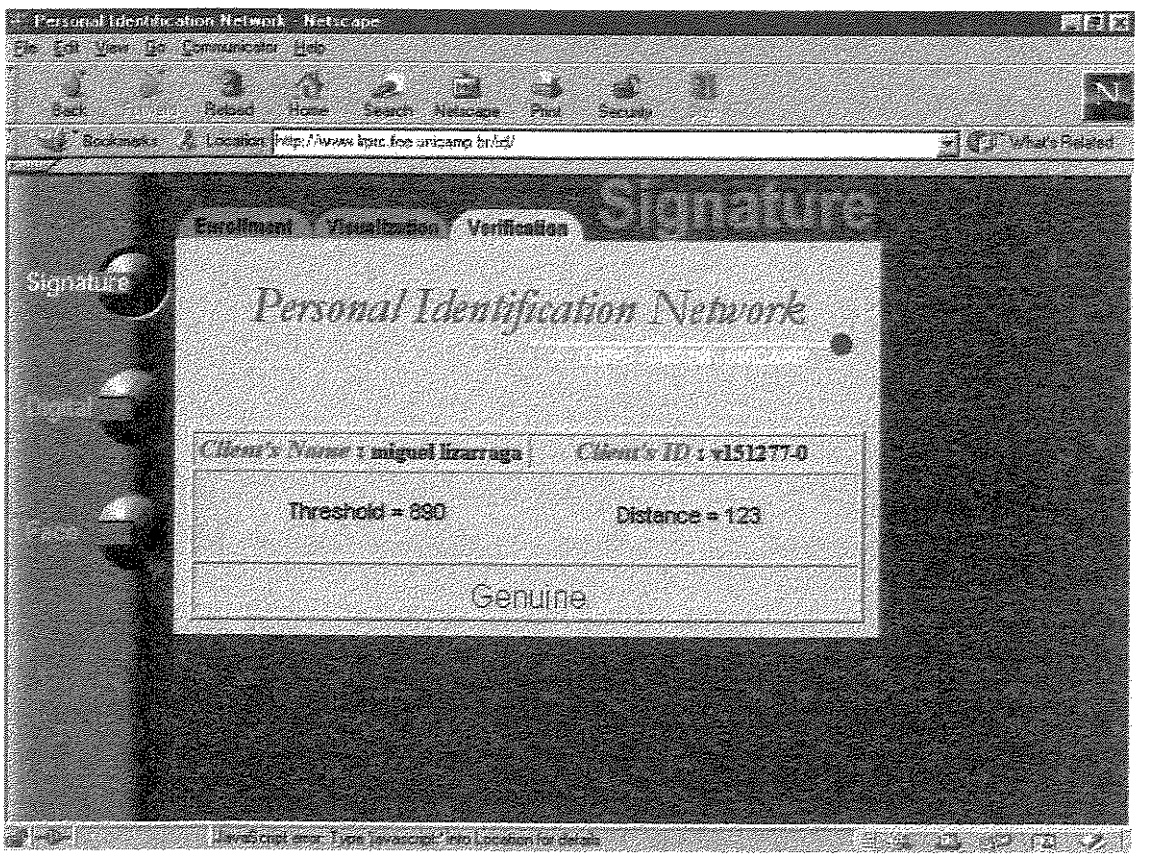


Figura 7.18: Resultado da verificação automática.

CAPÍTULO 8

CONCLUSÕES

Neste capítulo colocamos alguns comentários sobre o trabalho apresentado, enfatizando as contribuições oferecidas e indicados melhorias que podem ser feitas no sistema.

8.1 Contribuições

Neste trabalho apresentamos técnicas e métodos que utilizam medidas biométricas para realizar a tarefa automática de autenticação pessoal. Essas técnica e métodos de medidas biométricas foram estudadas e implementadas tendo como base imagens de assinaturas. A tarefa de autenticação pessoal, foi realizada através da verificação automática de assinaturas.

Foi disponibilizada uma plataforma que permite que diferentes métodos biométricos possam ser utilizados para identificação pessoal através do acoplamento de módulos de identificação. Esses módulos se referem a autenticação de identidade de indivíduos mediante algumas medidas biométricas que vem sendo desenvolvidas no Laboratório de Reconhecimento de Padrões e Redes de Comunicações (LRPRC) da Faculdade de Engenharia Elétrica e de Computação da UNICAMP, como por exemplo, imagens de impressões digitais, assinaturas estáticas e faces.

A principal característica da plataforma implementada é a utilização do modelo computacional cliente/servidor. Dessa forma é possível que tanto o cadastramento, consulta e autenticação de identidade sejam feitas se utilizando uma rede de computadores. Em nosso caso

específico, as tarefas anteriormente mencionadas podem ser realizadas de forma local dentro de uma intranet e de uma forma mais ampla através da internet.

8.2 Discussão sobre o Método de Verificação de Assinaturas

O método de verificação automático de assinaturas proposto se caracteriza por ser um sistema multi-especialista de dois estágios, onde o primeiro estágio trata das falsificações aleatórias e simples, e o segundo estágio de falsificações habilidosas.

Esse método se serve tanto de características globais como locais para fazer a descrição da assinatura. A técnica de divisão da imagem de assinaturas em quadros, introduz o conceito de que uma característica poder ser considerada global por pertencer ao um quadro, e ao mesmo tempo local, ao ser vista como integrante de apenas uma porção da imagem da assinatura.

As características utilizadas no primeiro estágio do sistema multi-especialista se baseiam na distribuição espacial dos pixels que compõe a assinatura. No segundo estágio, as características escolhidas se servem de técnicas de morfologia matemática para descrever as inclinações e contornos dos traços que compõe a assinatura.

Introduzimos o conceito da característica de correlação, a qual mede a similaridade entre o conjunto de assinaturas de referência e uma assinatura de teste.

O conjunto de referência utilizado consta de apenas três assinaturas e os classificadores que fazem parte do sistema são simples classificadores de distâncias.

Como parâmetros de desempenho de nosso sistema de verificação frente a falsificações aleatórias, obtivemos os valores de 0,47 % e 2,35 % de taxas médias de erros EFR_0 e EFA_0, respectivamente. No caso de falsificações habilidosas, as taxas médias de erros EFR_0 e EFA_0 foram de 12,75 % e 19,22 % respectivamente.

8.3 Discussão sobre a Plataforma do sistema de Identificação Pessoal

A plataforma do sistema de identificação é composta basicamente de um servidor *Web* e um gerenciador de base de dados. A essa plataforma podem ser acoplados módulos para executar diferentes tarefas. No sistema implementado, esses módulos são de identificação pessoal. Os módulos de identificação pessoal são na prática programas CGI que podem ser acessados através

de *browsers* via internet. Os *browsers* por sua vez, são a interface gráfica que permite ao usuário fazer o cadastramento, consulta e verificação automática de características biométricas.

8.4 Perspectivas para Novos Trabalhos

Com relação ao método de verificação é interessante estudar técnicas de lógica nebulosa tanto para a extração de características como para oferecer um melhor desempenho na tarefa de classificação.

No tocante à plataforma de identificação pessoal, é necessário a implementação dos módulos de autenticação pessoal por impressões digitais e faces. Além disso, podemos pensar em utilizar esses módulos em conjunto, isto é, associar características biométricas de assinaturas, impressões digitais e faces para melhor identificar um indivíduo [93].

É interessante também, desenvolver técnicas de criptografia de dados que levem em consideração características biométricas. Assim, permitiria que dados criptografados utilizando chaves baseadas em características biométricas, viagem com segurança por uma rede de computadores [94].

REFERÊNCIAS BIBLIOGRÁFICAS

[1] Mansfield, Tony & Roethenbaugh, Gary., 1998 Glossary of Biometric Terms. [*on-line*] Disponível na internet via *Web*. URL: http://www.afb.org.uk/public/glossuk1.html. Arquivo consultado em 15 de julho de 2000.

[2] Fairhurst M. C., "Signature verification revisited: promoting practical exploitation of biometric technology", *Electronics and Communication Engineering Journal*, pp. 273 - 280, dezember, 1997.

[3] Lee, Luan Ling., On-line systems for human signature verification. Ph.D. thesis, Cornell University, Cornell, 1992.

[4] Gomes, Herman; Machado, Patrícia; Carvalho, Edson., "Detecção de falsificações habilidosas na verificação estática de assinaturas via MLP-Backpropagation", II Simpósio Brasileiro de Redes Neurais, pp. 28 - 33. São Carlos, 1995.

[5] Boccignone, G.; Chianese, A.; Cordella, L.; Marcelli, A.; "Recovering dynamic information from static handwriting" *Pattern Recognition*, Vol. 26, N° 3, pp. 409 - 418, 1993.

[6] Holanda, Aurélio Buarque. Dicionário Aurélio Eletrônico, Versão 1.4, 1994.

[7] Ashbourn, Julian. The Biometric White Paper. [*on-line*] Disponível na internet via *Web*. URL: http://www.biometric.freeserve.co.uk/whitepaper.htm. Arquivo consultado em 15 de julho de 2000.

[8] Kapoor, T.; Kapoor, M.; Sharma, Gp., "Study of the form and extent of natural variation in genuine writings with age", Journal of the Forensic Science Society, Vol. 25, pp. 371 - 375, 1985.

[9] Chen, S.; Jain, A.; Ratha, N.. "Adaptative flow orientation-based feature extraction in Figerprint images", Pattern Recognition, Vol. 28, N° 11, pp. 1647 - 1672, 1995.

[10] Hrechak, A. & McHugh, J., "Automated fingerprint recognition using structural matching", *Pattern Recognition*, Vol. 23, N° 8, pp. 893 - 904, 1990.

[11] Kawagos, M. & Tojo, A., "Fingerprint pattern classification" *Pattern Recognition*, Vol. 17, pp. 295 - 303, 1984.

[12] Botha, E. & Coetzee, L., "Fingerprint recognition in low quality images", *Pattern Recognition*, Vol. 26, N° 10, pp. 1441 - 1460, 1993.

[13] Mardia, K.; Baczkowski, A.; Hainsworth, T., "Statistical methods for automatic interpretation of digitally scanned finger prints", *Pattern Recognition Letter*, Vol. 18, pp. 1197 - 1203, 1997.

[14] Daugman, J., "High confidence visual recognition of persons by a test of statistical independence", *Transactions on Pattern Analysis and Machine Intelligence*, Vol. 15, N° 11, pp. 1148 - 1161, 1993.

[15] Ferreira, Denilson. Identificação de pessoas por reconhecimento de íris utilizando decomposição em sub-bandas e uma rede neuro-fuzzy, Dissertação de Mestrado, Unicamp, dezembro, 1998.

[16] Wildes, P., "A machine vision system for iris recognition", *Mach. Vision applicat.* , Vol. 9, pp. 1 - 8, 1996.

[17] Berggren, L., "Iridology: A critical review", *Acta Ophthalmologica*, Vol. 64, pp. 1 - 8, 1985.

[18] Shu, W. & Zhang, D., "Automated personal identification by palmprint", *Optical Engeneering*, Vol. 37, N° 8, 1998.

[19] Jain, A.; Prabhakar, S.; Ross, A., "Biometrics-based web acces", Relatório Técnico MSU-CPS-98-33, Michigan State University, 1998.

[20] Pentland, A. & Choudhury T., "Face recognition for smart environments", *IEEE Computer Magazine*, Vol. 33, N° 2, pp. 46 - 49 , 2000.

[21] Harmon L.; Khan, K.; Lasch, R.; Ramig, P., "Machine identification of human faces", *Pattern Recognition*, Vol. 13. N° 2, pp. 97 - 110, 1981.

[22] Monrose, F. & Rubin, A., "Authentication via keystroke dynamics", *4th ACM Conference on Computer and Communications Security*, April, 1997.

[23] Joyce, R. & Gupta G. "Identity authorization based on keystroke latencies", *Communications of the ACM*, Vol 33. N° 2, pp 168 - 176, 1990.

[24] Pegoraro, Tarciano. Algoritmos robustos de reconhecimento de voz aplicados à verificação de locutor. Dissertação de Mestrado, Unicamp, Abril, 2000.

[25] Rosenberg, A.,"Automatic speaker verification: a review". *Proceedings of IEEE*, Vol. 64, N° 4, pp. 475 - 487, 1976.

[26] Wirtz, Brigitte, "Average Prototypes for stroke-based signature verification", *ICDAR 97*, Vol. 1, pp. 268 - 272, Germany, 1997.

[27] Lee L & Lizárraga, M., "Off-line methods for human signature verification", *Proceedings of IASTED International Conference on Signal and Image Processing - SIP-96*, USA, November, 1996.

[28] Jain, A.; Hong L.; Pankanti, S., "Biometrics: promising frontiers for emerging identification market", *Communication of ACM*, pp. 91 - 98, Febreary, 2000.

[29] Jain, A.; Duin, R.; Mao, J., "Statistical pattern recognition: a review", *IEEE Trans. on Pattern Analysis and Machine Intelligence*, Vol. 22, N° 1, pp. 4 - 37, 2000.

[30] Fu, K., "A step towards unification of syntatic an statistical pattern recognition ", *IEEE Trans. on Pattern Analysis and Machine Intelligence*, Vol. 5, N° 2, pp. 200 - 205, 1983.

[31] Duda, R. & Hart, P.. Pattern classification and scene analysis, New York, Wiley, 1973

[32] Mizukami, Y.; Yoshimura M.; Miike, Hidetoshi, M; Yoshimura, I. "An off-line signature verification system using an extracted displacement function", *ICDAR 99*, pp. 757 - 760, Bangalore, India, 1999.

[33] Ammar, M "A new effective approach for off-line verification of signatures by using pressure features", *Proc. 8th Int. Conf. On Pattern Recognition*, pp. 566 - 569, Paris, 1986.

[34] Evett, I.& Totty, R., "A study of the variation in dimensions of genuine signature", Journal of the Forensic Science Society, Vol. 25, pp. 207-215, 1985.

[35] Bruyne, P., "Signature verification using holistic measures", *Computers and Security*, Vol. 4, pp. 309 - 315, 1985.

[36] Mantas, J.,. "Methodologies in pattern recognition and image analysis - A brief survey", *Pattern Recognition*, Vol. 20, N° 1, pp. 1 - 6, 1987.

[37] Lee, L. & Lizárraga, M., "Classificação de Padrões e Extração de Parâmetros Discriminantes Utilizando Redes Neurais," *Anais do II Congresso Brasileiro de Redes Neurais*, Curitiba, novembro, 1995.

[38] Plamondon, R. & Lorette, G., "Automatic signature verification and writer identification - the state of the art", *Pattern Recognition*, Vol. 22, N° 2, pp. 107 - 131, 1989.

[39] Hilton, Ordway, "Signatures - Review and New View", *Journal of Forensic Sciences*, Vol. 37, N° 1, pp. 125 - 129, 1992.

[40] Lindgren, Nilo, "Machine recognition of human language - Part III - Cursive script recognition", *IEEE Spectrum*, may, 1965.

[41] Eden, Murray, "Handwritting and pattern recognition", *IRE trans. on Inf. Theory*, IT-8, February, 1962

[42] Foley, Robert G., "Characteristics of synchronous sequential signatures", *Journal of Forensic Sciences*, Vol. 32, N° 1, pp. 121-129, 1987.

[43] Chuang, Ping C., "Machine verification of handwritten signature image", *Proc Int. conference on Crime Countermeasure science and Engineering*, Lexington, pp. 105-109, 1977.

[44] Weszka, Joan & Rosenfeld, Azriel, "Histogram modification for threshold selection", *IEEE Trans. on System, Man. And Cybernatics*, Vol. SMC-9, N° 1, 1979.

[45] Yoshimura, I. & Yoshimura, M.. "Off-line verification of japanese signature after elimination of background patterns", *Int. Journal of Pattern Recognition and Art. Intelligence*, Vol. 8, N° 3, pp. 693 - 708, 1994.

[46] Lee, L.; Lizárraga, M.; Gomes, N.; Koerich, A., "A Prototype for Brazilian Bankcheck Recognition", *International Journal of Pattern Recognition and Artificial Intelligence*, Vol. 11. N°. 4, pp. 87 - 107, 1997.

[47] Banon, G. & Barrera, J. Bases da morfologia matemática, IX Escola de Computação, Recife, 1994

[48] Nemcek, W. & Lin, W., "Experimental investigation of automatic signature verification", *IEEE Trans. on Systems, Man, adn Cybernatics*, Vol. SMC-4, N° 1, 1974.

[49] Pender, Dorothy. Neural networks and handwritten signature verification. Ph.D. Thesis, Standford University, Standford, California, 1991.

[50] Lizárraga, Miguel. Um sistema automático de consulta e verificação de assinaturas estáticas. Dissertação de Mestrado, Unicamp, fevereiro, 1996.

[51] Qi, Y. & Hunt, B., "Signature verification using global and grid features", *Pattern Recogntion*, Vol. 27, N° 12, pp. 1621 - 1629, 1994.

[52] Ammar, Maan. "Structural description and classification of signature images", *Pattern Recognition*, Vol 23, N° 7, pp. 895 - 905, 1990.

[53] Powalka, R., "Feature extraction: on the importance of zoning information in cursive script recognition", *Progress in Image Analysis and Processing III*, pp 342 - 349, 1994.

[54] Nagel, R. & Rosenfeld, A.,"Computer detection of freehand forgeries", *IEEE Trans. on Computer*, Vol C-26, N° 9, pp. 895 - 905, 1977.

[55] Brocklehurst, Er, "Computer methods of signature verification", *Journal of the Forensic Science Society*, Vol. 25, pp. 445 - 457, 1985.

[56] Bajaj, R. & Chaudhury, S., "Signature verification using multiple neural classifiers", *Pattern Recognition*, Vol. 30, N° 1, pp. 1 - 7, 1997.

[57] Deng, P.; Liao, H.; Ho, C.; Tyan, H., "Wavelet-based off-line handwritten signature verification", *Computer Vision and Image Understanding*, Vol. 76, N° 3, pp. 173 - 190, 1999.

[58] Pavlidis, I.; Papanicolopoulos, N.; Mavuduru, R., "Signature identification through the use of deformable structures", *Signal Processing*, Vol. 71, pp. 187 - 201, 1998.

[59] Sabourin, R.; Cheriet, M.; Genest, G., "An extended shadow-code based approach for off-line signature verification", *ICDAR 1993*.

[60] Huang, K. & Yan H., "Off-line signature verification based on geometric feature extraction and neural network classification", *Pattern Recognition*, Vol. 3, N° 1, pp. 9 - 17, 1997.

[61] Murshed, Nabeel. Uma abordagem natural, baseada em redes neurais, para verificação de assinaturas manuscritas. Dissertação de mestrado. Centro Federal de Educação Tecnológica do Paraná. Março, 1995.

[62] Sabourin R.; Drouhard, J.; Wah, E., "Shape matrices as a mixed shape factor of off-line signature verification," *ICDAR 97*, pp. 661 - 665, 1997.

[63] Sabourin, R. & Genest, G.. "Off-line signature verification by locak granulometric size distributions", *IEEE Trans. on Pattern Analysis and Machine Intelligence*, Vol. 19, N° 9, pp. 976 - 988, 1997.

[64] Guo, J.; Doermann, D.; Rosenfeld A., "Local correspondence for detecting random forgeries", *ICDAR 97*, pp. 319 - 323, 1997.

[65] Cardot, H.; Revenu, M.; Victorri, B.; Revillet, M., "A static signature verification system based on a cooperative neural network architecture", *Int. Journal of Pattern Recognition and Art. Intelligence*, Vol 8, N° 3, pp. 679 - 692, 1994.

[66] Plamondon, R. & Srihri, S., "On-line and off-line handwriting recognition: A comprehensive survey", *IEEE Trans. on Pattern Analysis and Machine Intelligence*, Vol. 22, N° 1, pp. 63 - 84, 2000.

[67] Leclerc, F. & Plamondon, R.. "Automatic signature verification: the state of the art, 1989 - 1993", International Journal of Pattern Recognition and Artificial Intelligence, Vol. 8, N° 3, pp. 643-660. 1994.

[68] Oliveira, Francisco. Estatística e probabilidade, Editora Atlas, 2da Edição, 1999.

[69] Guyon, I.; Makhoul, J.; Schwartz, R.; Vapnik, V., "What size test set gives good error rate estimates?", *IEEE Trans. on Pattern Analysis and Machine Inteligence*, Vol. 20, N° 1, pp. 52 - 64, 1998.

[70] Qi, Y. & Hunt, B., "A multiresolution approach to computer verification of handwritten signatures", *IEEE Trans. on Pattern Analysis and Machine Inteligence*, Vol. 4, N° 6, pp. 870 - 874, 1995.

[71] Gonzales, R. & Woods, R. Digital Image Processing. Addison Wesley, 1992

[72] Hu, M., "Visual Pattern Recognition by Moments Invariants", *IRE Transaction on information theory*, IT-8, pp. 179 - 187, 1962.

[73] Lin, H. & Li, H., "Chinese signature verification with moments invariants", *Procedings of the Int. Conf. of System, Man and Cybernatics*, Vol. 4, pp. 2963 - 2968, 1995.

[74] Chim, Y.; Kassim A.; Ibrahim Y., "Character recognition using statistical moments", *Image and vision computing*, Vol. 17, pp. 299 - 307, 1999.

[75] Tsirikolias, K. & Mertzios, B., "Statistical pattern recognition using efficient two-dimensional moments with applications to character recognition", *Pattern Recognition*, Vol. 26, pp. 877 - 882, 1993.

[76] Heutte, L.; Paquet, T.; Moreau, J.; Lecourtier, Y.; Oliver, C., "A structural/statistical feature based vector for handwritten character recognition", *Pattern Recognition Letter*, Vol. 19, pp. 629 - 641, 1998.

[77] Al-Yousefi, H. & Udpa, S., "Recognition of Arabic Characters", *IEEE Trans. on Pattern Analysis and Machine Intelligence*, Vol. 14, N° 8, pp. 853 - 857, 1992.

[78] Cordella, L.; Foggia, P.; Sansone, C.; Vento, M., "Document validation by signature: a serial multi-expert approach", *ICDAR 99*, pp. 601 - 604, Bangalore, 1999.

[79] Dumas, Arthur. Programando Winsock, Axcel Books, 1995

[80] _____. International Organization for standardization homepage. [*on-line*] Disponível na internet via *Web*. URL: *http://www.iso.ch*. Arquivo consultado em 16 de julho de 2000.

[81] Quinn B. & Shute, D.. Windows sockets network programming, Addison-Wesley, 1996.

[82] .Stross, Charles, The Web Architect's Handbook, Addisson-Wesley, 1996.

[83] Pomykalski, J. Web Page Development: An Introduction. [*on-line*] Disponível na internet via *Web*. URL: *http://www.cs.jmu.edu/common/coursedocs/isat242/web*. Arquivo consultado em 16 de julho de 2000.

[84] Leong, K.; Srikanthan, T.; Hura, G., "An Internet Aplicaction for on-line Banking", *Computer Communication*, Vol. 20, pp. 1534 - 1540, 1998.

[85] Ureche, Ocravian & Plamondon, Réjean. "Document transport, transfer and exchange: security and comercial aspects", *ICDAR 99*, pp. 585 - 588, Bangalore, India, 1999.

[86] Ricarte, Ivan. "Uma introdução aos mecanismos de processamento web". Disponível na internet via *Web*. URL: *http://ww.dca.fee.unicamp.br/~ricarte*. Arquivo consultado em 16 de

julho de 2000.

[87] ____. "Hypertext Transfer Protocol -- HTTP/1.1". [*on-line*] Disponível na internet via *Web*. URL: *ftp://ftp.isi.edu/in-notes/rfc2616.txt*. Arquivo consultado em 16 de julho de 2000.

[88] Berners-Lee, Tim. Tim Berner-Lee home page. [*on-line*] Disponível na internet via *Web*. URL: *http://www.w3.org/People/Berners-Lee*. Arquivo consultado em 16 de julho de 2000.

[89] Rowe, Jeff. Building internet database servers with CGI, News Riders Publishing, 1996.

[90] Hughes, David. The Home of Mini SQL, [*on-line*] Disponível na internet via *Web*. URL: *http://www.hughes.com.au/*. Arquivo consultado em 16 de julho de 2000.

[91] Groff, J. & Weinberg, P. Using SQL, McGraw-Hill, 1994.

[92] _____. The Apache Software Fondation. [*on-line*] Disponível na internet via *Web*. URL: *http://www.apache.org*. Arquivo consultado em 16 de julho de 2000.

[93] Hong, Lin;. Jain, Anil; Pankanti, Sharath, "Can multibiometrics improve performance", Relatório Técnico MSU-CSE-99-39, Michigan State University, 1999.

[94] Maio, Dario & Maltoni, Davide, "A secure protocol for electronic commerce based on fingerprints and encryption", *ISAS'99*, Vol. 4, pp. 519-525, 1999.