UNIVERSIDADE ESTADUAL DE CAMPINAS

FACULDADE DE ENGENHARIA ELÉTRICA E DE COMPUTAÇÃO

DEPARTAMENTO DE COMUNICAÇÕES

Tese de Mestrado

Uma Metodologia para Avaliação de Pacotes de *Software* Biométricos

Luiz Humberto Rabelo Sucupira Júnior

Orientador: Prof. Dr. Lee Luan Ling

Co-orientador: Dr. Miguel Gustavo Lizárraga

Banca Examinadora:

Prof. Dr. Mario Jino (FEEC/UNICAMP)

Prof. Dr. João Baptista Tadanobu Yabu-uti (FEEC/UNICAMP)

Prof. Dr. Edson Costa de Barros Carvalho Filho (CIn/UFPE)

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

Campinas – SP – Brasil

Abril de 2004

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

Su19m

Sucupira Júnior, Luiz Humberto Rabelo
Uma metodologia para avaliação de software biométricos / Luiz Humberto Rabelo Sucupira Júnior. -- Campinas, SP: [s.n.], 2004.

Orientadores: Lee Luan Ling e Miguel Gustavo Lizárraga.
Dissertação (mestrado) - Universidade Estadual de Campinas, Faculdade de Engenharia Elétrica e de Computação.

1. Sistemas de reconhecimento de padrões. 2. Engenharia de software - Normas. 3. ISO 9000. 4. Software - Qualidade. 5. Biometria. I. Ling, Lee Luan. II. Lizárraga, Miguel Gustavo. III. Universidade Estadual de Campinas. Faculdade de Engenharia Elétrica e de Computação. IV. Título.

RESUMO

Nesse trabalho nós apresentamos uma metodologia para avaliação de pacotes de *software* biométricos. Nós propomos que o modelo hierárquico *top-down* utilizado pela ISO/IEC 9126 para avaliação de produtos de *software* seja adaptado para um novo modelo hierárquico que será utilizado na avaliação de pacotes de *software* biométricos baseado na divisão de um sistema biométrico em subsistemas. Pacotes de *software* biométricos são definidos como a junção do sistema biométrico mais as documentações que o acompanham, que é baseada na definição de pacotes de *software* estabelecida na norma ISO/IEC 12119.

Cinco passos básicos compõem a metodologia proposta: (1) realizar a coleta de informações sobre o pacote de *software* biométrico e sobre o fabricante, (2) estabelecer um nível de rigor em que se enquadra a avaliação do pacote de *software* biométrico, (3) selecionar um grupo de atributos para avaliar o pacote e aplicar os Questionários de Identificação do Perfil do Especialista (QIPEs) aos avaliadores, (4) aplicar os atributos selecionados na avaliação do pacote de *software* biométrico, e (5) apresentar um relatório sobre a avaliação e os resultados produzidos.

Baseada na metodologia mencionada, uma ferramenta computacional foi desenvolvida para aplicação de uma avaliação objetiva em algoritmos biométricos. Seu objetivo é verificar o desempenho e a eficiência dos algoritmos biométricos a partir de parâmetros de qualidade previamente estabelecidos. Esta ferramenta foi denominada BioEVA. O processo de submissão de algoritmos para análise pela ferramenta segue um protocolo baseado principalmente na FVC (*Fingerprint Verification Competition*). Na ferramenta foram implementados três módulos: cadastramento, autenticação e avaliação. Os dois primeiros módulos são utilizados para a realização de testes com o algoritmo biométrico submetido enquanto que o terceiro módulo é utilizado para a geração e exibição dos resultados da avaliação. Os parâmetros de qualidade que são utilizados para avaliar o desempenho e a eficiência do algoritmo biométrico são implementados no módulo de avaliação.

Avaliamos três algoritmos biométricos usando a ferramenta BioEVA: dois baseados em assinaturas estáticas (ASig1 e ASig2) e um baseado em dinâmica da digitação (AKey1). Com base nos resultados apresentados poderemos observar que mediante os parâmetros de qualidade avaliados nestes algoritmos, os algoritmos biométricos ASig2 e AKey1 apresentaram excelentes resultados, enquanto que o algoritmo biométrico Asig1 apresentou alguns problemas relacionados com as taxas de falsa aceitação e rejeição, que se apresentaram superior as taxas normalmente aceitas como ideais para este tipo de tecnologia biométrica.

A metodologia é demonstrada na prática através da avaliação de qualidade de um pacote de *software* biométrico submetido externamente, ou seja, uma empresa colaborou conosco para a avaliação do seu pacote. Os resultados da aplicação da metodologia mostram que esse pacote apresenta alguns problemas que na prática o tornaria um produto inadequado para o tipo de aplicação prática e público-alvo ao qual se destina. Além disso, o pacote foi classificado como um protótipo, pois ainda necessita que severas alterações sejam realizadas, para que atinja os objetivos ao qual se destina. Para tanto, fornecemos ao desenvolvedor um relatório com considerações e críticas para que ele possa efetuar melhorias no produto.

ABSTRACT

In this work, we present a methodology to evaluate biometric software packages. We propose that the ISO/IEC 9126 top-down hierarchical model, which is used to evaluate software products in general, need to be adjusted to a new model capable to support the definitions involving biometric software packages based on a division of biometric systems in subsystems. Biometric software package is composed of a biometric system and its documents based on the definition of software packages on ISO/IEC 12119 norm.

Five basic steps compounds the proposed methodology: (1) information is collected about the biometric software package and its developer, (2) a severity level is established according to the characteristics of the package, (3) a group of attributes is selected, and Specialist's Profile Identification Questionnaire (SPIQs) are applied to evaluators, (4) the selected attributes are applied to evaluate the package, and (5) a final report is presented with the produced results.

Based on the methodology, we developed a computational tool that we called BioEVA with the purpose of applying an objective evaluation without the subjective criteria. It is used to evaluate biometric algorithms, verifying their performance and efficiency according to quality parameters previously established. This tool was called BioEVA. The submission protocol for biometric algorithms is mainly based on FVC (Fingerprint Verification Competition). Three modules were implemented: enrollment, authentication and evaluation. The two first ones are used to perform tests with the biometric algorithm and the third one is used to generate and show the evaluation results. The quality parameters to evaluate the efficiency and the performance of the biometric algorithm are implemented in the evaluation module.

Three biometric algorithms were evaluated by BioEVA tool: two are related to static signature authentication (ASig1 and ASig2) and one to keystroke dynamics verification (AKey1). The evaluation results show that the ASig2 and AKey1 biometric algorithms presented excellent results, but the ASig1 biometric algorithm had some problems related to false acceptance and rejection rates whose values are not satisfactory to this kind of biometric technology.

The methodology was applied in a quality evaluation of a biometric software package. The evaluation results show that this package presents some problems that compromises its practical applications and will not cause consumers' satisfaction. Besides, the package was classified as a prototype because it need some modifications to attend its main purposes. The developer receives at the end of the evaluation process a report with considerations and the evaluation results with the purpose of improve packages quality.

Para minha amada

Lívia,

Pela coragem com que enfrenta os desafios

que a vida lhe impõe, dando-me coragem e forças

para enfrentar todos os meus desafios.

Uma grande e brilhante mulher a quem

dedico este trabalho.

"Não existe triunfo sem perda, nem vitória sem sofrimento, nem liberdade sem sacrifício."

The Lord of The Rings – The Return of the King

"A única coisa necessária para o triunfo do mal é que os homens bons não façam nada."

Edmund Burke, filósofo britânico

AGRADECIMENTOS

- A Deus, principalmente, por mais uma etapa cumprida da minha vida.
- A meus pais, Luiz Humberto e Maria Luiza, pelo carinho e dedicação, sempre acompanhando–me nas mais diversas etapas da minha vida.
- Ao Prof. Lee Luan Ling, pela oportunidade da realização deste trabalho.
- Ao Prof. Marcos Negreiros, pelo seu incentivo e apoio nos momentos mais difíceis, e mais importante, pela sua amizade e carinho.
- Ao Miguel Lizárraga, pelas contribuições no desenvolvimento deste trabalho e pela sua grande amizade e companheirismo.
- Ao Prof. Yabuuti, pela sua amizade, humanidade e compreensão, um ser humano ímpar.
- Ao irmão Paulo e aos eternos amigos Célio, Jorge, Hinelly, Lívio, Caroline, Ivna e Solange, que mesmo distantes sempre estiveram comigo em espírito apoiando-me nesta jornada.
- Ao casal Augusto e Érika, por todos os bons momentos que passamos juntos.
- Aos conterrâneos Lívio, Élder e Ponchet e aos amigos Glauco e Aline pela força de vontade e coragem inesquecíveis que demonstraram nos momentos pelo qual passamos juntos.
- Aos membros do LRPRC Fernando, Gilmar, Kesede, Júlio, Carlos, Juliano, Cleison, Flávio, Pepe, Magali, Stela e Gabriel pela amizade e apoio oferecidos nas suas mais diversas formas.
- A CAPES pelo apoio financeiro concedido a esta pesquisa.
- E a todos que de alguma forma contribuíram e ajudaram na conclusão deste trabalho.

ÍNDICE

LISTA DE TABELAS

LISTA DE FIGURAS

CAPÍTULO 1

INTRODUÇÃO

Neste capítulo apresentamos a motivação e as idéias envolvidas para o estudo de uma metodologia de avaliação de pacotes de software biométricos. Introduzimos os conceitos relacionados com o enquadramento do nosso projeto e os seus respectivos limitantes. Relacionamos também as áreas de concentração do conhecimento associadas. Apresentamos os objetivos desta dissertação e, finalmente, introduzimos a estrutura desta dissertação.

1.1 Qualidade de Produtos e Serviços

A cada dia, o mercado de produtos e serviços torna-se mais competitivo, e os consumidores mais exigentes em suas necessidades com relação à qualidade destes produtos e serviços a eles oferecidos. Isto ocasiona a necessidade das empresas desenvolverem produtos e oferecerem serviços cada vez melhores. Neste contexto insere-se a questão da qualidade para que as empresas possam sobreviver e assegurar seu lugar neste cenário competitivo.

A globalização da economia, a evolução da tecnologia da informação e o movimento irreversível da qualidade (mercado cada vez mais competitivo e consumidores mais exigentes) estão alavancando o processo de reestruturação de conceitos, princípios e crenças, onde as organizações bem sucedidas fundamentam suas estratégias e seus planejamentos de produção e oferta de produtos e serviços para assegurar a vantagem competitiva no mercado. Esta situação é chamada "era das organizações baseadas em conhecimento" ou "era do capitalismo intelectual"

[1]. Neste contexto, o engenheiro de *software* é solicitado a atuar como um agente para promover a implantação de um processo de qualidade em produtos e serviços.

Qualidade é um tema muito discutido e estudado. Existem diversos conceitos de qualidade, que podem ser resumidos em três definições distintas [2]:

- Qualidade é estar em conformidade com os requisitos do cliente;
- Qualidade é antecipar e satisfazer os desejos do cliente;
- Qualidade é escrever tudo o que se deve fazer e fazer tudo o que foi escrito.

Estas definições apresentam um conceito simplificado e de fácil entendimento para dar uma idéia sobre o quê é qualidade. Uma definição formal de qualidade pode ser encontrada na norma internacional ISO/IEC 9126, onde qualidade é "a totalidade das características de uma entidade que lhe confere a capacidade de satisfazer as necessidades implícitas e explícitas dos seus usuários" [3]. Esta definição formal exige alguns complementos. A entidade é o produto que estamos referenciando, podendo ser um bem, serviço ou processo. As necessidades implícitas dos usuários envolvem diversos critérios subjetivos, como as diferenças étnico-culturais dos usuários, a evolução no tempo, a variabilidade intra e interpessoal, e as questões de segurança. As necessidades explícitas dos usuários são as próprias condições e objetivos propostos pelo fabricante ou prestador de serviço.

Não podemos pensar em qualidade como sinônimo de perfeição. Trata-se de algo factível, relativo, substancialmente dinâmico e evolutivo, amoldado a granularidade dos objetivos a serem atingidos [4]. Considerá-la como algo absoluto e definitivo seria transportar-se para o inatingível e, com base neste sofisma, propiciar entraves a qualquer esforço de produzi-la. Qualidade, portanto, não significa somente excelência ou um atributo de um certo produto ou serviço. A qualidade deve ser perseguida dentro da organização que está propondo o produto ou serviço, pois, certamente, o que se propõe por qualidade é o que os usuários esperam de um produto.

Dentro desse contexto, propomos uma avaliação de qualidade de produtos biométricos que foram desenvolvidos com o intuito de autenticar a identidade de indivíduos a partir de suas

características comportamentais e/ou físicas. Baseando-se nas características particulares destes produtos, desenvolvemos uma metodologia capaz de avaliar o grau de qualidade destes produtos e identificar deficiências que possam gerar recomendações para melhoria em sua qualidade.

1.2 Identificação Pessoal

Com a evolução e o aumento da sofisticação da sociedade, as pessoas passam cada vez mais por situações em que são obrigadas a ter que provar sua identidade. Podemos citar, como exemplos, os cartões magnéticos para retirar dinheiro em bancos, as assinaturas para autenticar cheques bancários, ou ainda a apresentação de documentos com nossa foto, como em passaportes e em 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.

Existem basicamente quatro categorias de autenticação pessoal. A primeira categoria envolve a posse de um dispositivo, como, por exemplo, um cartão ou um crachá. A segunda categoria envolve o conhecimento individual de chaves secretas, como, por exemplo, senhas e contra-senhas. A terceira categoria envolve a validação da identidade através de um padrão ou atividade específica do indivíduo, como por exemplo sua assinatura ou fala. A quarta categoria envolve a análise das possíveis características físicas que a pessoa possui, dentre as quais podemos mencionar as impressões digitais, geometria da mão, íris, DNA, etc.

Na maioria das vezes, a maneira de autenticar a identidade de um indivíduo recai sobre as duas primeiras categorias [5]. 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. Além disso, ainda temos que carregar conosco vários documentos de identificação, como por exemplo, carteira de identidade, carimbos, selos, cartões e chaves. Porém, nenhum destes métodos é 100% confiável, visto que podem ser esquecidos, roubados, emprestados, perdidos, copiados e/ou falsificados.

Por essas razões, tem aumentado o interesse em desenvolver métodos de autenticação de identidade pessoal que levem em consideração estratégias que se fundamentem na terceira e quarta categorias. Estes métodos baseiam-se em medidas biométricas, onde "medida biométrica" é definida pela *Association for Biometrics* [6] como: "A medida de atributos/características físicas ou

de comportamento de uma pessoa com o objetivo de distinguí-la dentre as demais". Pesquisas recentes mostram que a inclusão de medidas biométricas em sistemas de identificação pessoal aumentam o grau de confiança na autenticação da identidade de um indivíduo [6]. Na terceira categoria de autenticação pessoal enquadram-se as medidas biométricas do tipo comportamentais como o tipo de escrita do indivíduo, a maneira como assina seu nome, a forma como se pronunciam determinadas palavras, etc. Na quarta categoria de autenticação pessoal enquadram-se as medidas biométricas do tipo fisiológicas tais como o padrão da íris, as impressões digitais, a forma do contorno da mão, e face.

Apesar desse aumento na adoção de sistemas biométricos para reconhecimento pessoal que atualmente vem ocorrendo, o emprego de procedimentos que garantam a qualidade destes sistemas ainda são pouco utilizados, pois, somente há alguns anos, órgãos de padronização e laboratórios de pesquisa têm interessado-se por este tema [5]. Um sistema é construído de acordo com uma especificação, que determina o seu aspecto operacional e satisfaz as necessidades dos seus usuários. Uma especificação do sistema inadequada ou incorreta pode ocasionar prejuízos e insatisfação para os seus usuários, além de comprometer o desempenho do sistema. Mesmo que a especificação esteja correta, existe a possibilidade de seus usuários utilizarem o sistema de forma inadequada. Sendo assim, a questão é quando tornar o sistema operacional, como salvaguardar seus usuários de erros e respeitar suas necessidades, e, além disso, garantir que ele está de acordo com sua especificação.

Dentro desse contexto, neste trabalho, propomos a implementação de uma metodologia que seja capaz de avaliar a qualidade de um sistema biométrico como um produto comercial, sem considerar as etapas do seu desenvolvimento. Assim, procuraremos garantir que o produto está de acordo com os objetivos aos quais se propõe e pelos quais foi desenvolvido, ou seja, suas especificações originais. Propomos também adaptar um modelo hierárquico para suportar os componentes resultantes da divisão de um sistema biométrico, assim como mostrar as dependências diretas existentes entre eles em cada nível hierárquico.

1.3 Áreas de Concentração

Esse trabalho aborda basicamente duas áreas de conhecimento. A primeira área é a de Engenharia de *Software*, que disponibiliza métodos, técnicas e ferramentas com o objetivo de

elevar a qualidade do *software* produzido, melhorando assim sua relação custo/benefício. A segunda é Reconhecimento de Padrões, a qual lida com a aquisição, a extração e a classificação de informações. As duas áreas de conhecimento foram combinadas com o intuito de utilizar os conceitos existentes em Qualidade de *Software* (Engenharia de *Software*) e em Biometria (Reconhecimento de Padrões) para produzir uma metodologia capaz de avaliar pacotes de *software* biométricos com simplicidade, robustez e expressividade.

1.3.1 Engenharia de Software

Esta área do conhecimento será explorada neste trabalho objetivando a criação de uma metodologia para a avaliação de qualidade em pacotes de *software* biométricos. Algumas possíveis definições são [2]:

- "é a disciplina que integra métodos, ferramentas e procedimentos para o desenvolvimento de *software* para computadores";

- "é um termo usado para se referir a modelos de ciclos de vida, metodologias de rotina, técnicas de estimativa de custo, estruturas de documentação, ferramentas de gerenciamento de configuração, técnicas de garantia de qualidade e outras técnicas de padronização da atividade de produção de *software*."

A Engenharia de *Software* surgiu em meados dos anos 70 numa tentativa de contornar a "crise do *software*" e dar um tratamento de "engenharia" (mais sistemático e controlado) ao desenvolvimento de sistemas de *software* complexos. Um sistema de *software* complexo se caracteriza por um conjunto de componentes abstratos de *software* (estruturas de dados e algoritmos) encapsulados na forma de procedimentos, funções, módulos, objetos ou agentes, interconectados entre si, compondo a arquitetura do *software*, que deverão ser executados em sistemas computacionais. Os fundamentos científicos para a engenharia de *software* envolvem o uso de modelos abstratos e precisos que permitem ao engenheiro especificar, projetar, implementar e manter sistemas de *software*, avaliando e garantindo suas qualidades. Além disto, a

engenharia de *software* oferece também mecanismos para o planejamento e o gerenciamento do processo de desenvolvimento de sistemas de *software*.

Os Paradigmas da Engenharia de Software são um conjunto de etapas que são definidas no processo de desenvolvimento de um *software*. Destacam-se 4 paradigmas principais: o ciclo de vida clássico, a prototipação, o modelo espiral e as técnicas de quarta geração (4GT). A prototipação traz bons resultados principalmente quando o cliente não tem precisão na declaração do problema [7]. O modelo espiral é baseado no princípio do desenvolvimento incremental, onde novas funções são adicionadas a cada ciclo. Análise, especificação, projeto, implementação e validação são repetidos a cada ciclo, gerando uma nova versão do *software* e permitindo um *feedback* mais imediato do usuário [7]. As técnicas de quarta geração utilizam poderosas ferramentas para o desenvolvimento do *software*, que permitem um nível de especificação mais elevado, próximo à linguagem natural, sendo capazes, a partir destas definições, de gerar o código-fonte do sistema [7].

Os paradigmas podem ser combinados visando a obtenção de um melhor resultado. Independentemente do paradigma a ser utilizado, 3 fases genéricas dividem o processo de desenvolvimento [7]:

- Definição: esta fase focaliza o "*o quê*" (análise do sistema, planejamento do projeto de *software* e análise de requisitos);

- Desenvolvimento: focaliza-se o "*como*" (projeto de *software*, codificação e realização de testes no *software*);

- Manutenção: Concentra-se nas "*mudanças*" (correção, adaptação e melhoramento funcional).

A aplicação dos paradigmas e das fases genérica regulamenta todo o processo de desenvolvimento e manutenção do *software*. Porém, eles não garantem que o *software* resultante do processo de desenvolvimento possui qualidade e que vai atender as necessidades dos seus usuários. Neste contexto, para preencher esta lacuna, uma sub-área do conhecimento em

Engenharia de *Software* foi criada, chamada Qualidade de *Software*, a qual exploraremos nesta dissertação para avaliação de qualidade de um sistema biométrico como um produto comercial. Os principais conceitos e aplicações práticas neste trabalho envolvendo Qualidade de *Software* serão abordados no próximo capítulo.

1.3.2 Reconhecimento de Padrões

O termo Reconhecimento de Padrões aplica-se aos métodos para extração e 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, têm-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. Este 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 e a aprendizagem a partir de exemplos, o reconhecimento por redes neurais acaba sendo tratado como uma área distinta.

Nós iremos envolver uma área específica de Reconhecimento de Padrões denominada Biometria, que trata da identificação pessoal baseada em características comportamentais e fisiológicas de um indivíduo. Neste sentido, iremos avaliar a qualidade de sistemas biométricos desenvolvidos com o intuito de identificação pessoal.

1.4 Objetivos do Trabalho

O primeiro objetivo deste trabalho é desenvolver uma metodologia para avaliação de qualidade de pacotes de *software* biométricos com o intuito de garantir que estes pacotes estão de acordo com normas e padrões de qualidade para produtos de *software* biométricos e determinar quais são os seus pontos fortes e fracos, promovendo recomendações para melhoria da qualidade destes produtos. Para tanto, procuramos adaptar um modelo comumente utilizado para avaliação de qualidade de produtos de software em geral, o modelo hierárquico *top-down* da ISO/IEC 9126 para abrigar os conceitos inerentes a pacotes de *software* biométricos. Para visualizar um pacote de *software* biométrico como um produto comercial, fizemos uso da Norma ISO/IEC 12119, que descreve os conceitos envolvendo pacotes de *software* e as documentações que devem acompanhá-lo.

O segundo objetivo é disponibilizar uma ferramenta que permite a implementação de uma avaliação objetiva de qualidade de algoritmos biométricos, determinando o grau de eficiência e de desempenho de um algoritmo biométrico de acordo com parâmetros de qualidade implementados na ferramenta. Os módulos que compõem esta ferramenta implementam interfaces gráficas de interação homem-máquina nas quais realizam-se o cadastramento e autenticação de indivíduos, e a avaliação de algoritmos biométricos que foram submetidos para avaliação pela ferramenta e que apresentaremos *a posteriore*. Amostras de dinâmica da digitação e assinaturas foram coletadas no Laboratório de Reconhecimento de Padrões e Redes de Comunicações (LRPRC) da Faculdade de Engenharia Elétrica e de Computação (FEEC) da Universidade Estadual de Campinas (UNICAMP). A BioEVA foi desenvolvida utilizando a linguagem de programação java, na plataforma Java 2 Standard Edition desenvolvida pela Sun Microsystems.

1.5 Estrutura da Dissertação

Esta dissertação está dividida em sete capítulos e três anexos:

1. Introdução
2. Qualidade de Software
3. Biometria
4. A Metodologia para Avaliação de Pacotes de Software Biométricos
5. A Ferramenta BioEVA
6. Resultados das Avaliações
7. Conclusões

I. Passos Práticos para Aplicação da Metodologia na Avaliação de Pacotes de *Software* Biométricos

II. Esquema Completo de Definição de um Atributo

III. Publicações e Submissões

No capítulo 2, faremos uma introdução sobre a área da engenharia de *software* que envolve qualidade de *software*, mostrando as principais formas de avaliação de produtos e processos de *software*, assim como sobre o modelo ISO reconhecido mundialmente em avaliação de qualidade de produtos e serviços. No capítulo 3, faremos uma apresentação geral sobre a biometria e os principais métodos biométricos de autenticação pessoal. No capítulo 4, descreveremos a metodologia proposta nesta dissertação para avaliar pacotes de *software* biométricos. Ainda neste capítulo, mostraremos como adaptamos o modelo hierárquico *top-down* ISO/IEC 9126 para avaliações de pacotes de *software* biométricos. A ferramenta BioEVA será apresentada no capítulo 5, no qual detalharemos os módulos implementados para suportar uma avaliação objetiva, assim como as regras básicas para submissão de um algoritmo para avaliação por esta ferramenta. No capítulo 6, apresentaremos os resultados obtidos pela aplicação da ferramenta BioEVA na avaliação de três algoritmos biométricos e da aplicação da metodologia na avaliação de um pacote de *software* biométrico. No capítulo 7, apresentaremos um sumário geral da dissertação, descrevendo o método de elaboração deste trabalho, os objetivos e as contribuições alcançadas, e as perspectivas para novos trabalhos. No anexo I, apresentamos os passos práticos para aplicação

da metodologia. No anexo II apresentamos um exemplo completo de definição de um atributo segundo a documentação que será apresentada no capítulo 4 para definição de um atributo. Finalmente, no anexo III mencionamos as referências das publicações alcançadas pela metodologia e pela ferramenta BioEVA e as respectivas submissões para um pedido de patente e registro de *software*.

CAPÍTULO 2

QUALIDADE DE SOFTWARE

Neste capítulo apresentamos os conceitos básicos que regem a qualidade de software. Apresentamos também uma visão geral das diversas categorias de análise de qualidade de software, assim como dos principais modelos para análise de qualidade envolvidos. Apresentamos o padrão ISO, o qual é uma referência mundial em avaliação de qualidade de produtos e serviços, e que se tornou base para a elaboração de um modelo hierárquico que atendesse aos interesses envolvidos nesta dissertação.

2.1 Introdução

O desenvolvimento de produtos de *software* evidencia-se como uma atividade complexa, devido à necessidade de serem construídos projetos que combinem múltiplos requisitos entre si, envolvam várias equipes de trabalho e produtos não materiais, associados a seus programas e documentações [4].

Um *software* perfeito (sem erros e 100% seguro) para um sistema complexo não pode ser garantido na prática porque as incorretudes presentes nas especificações serão transportadas para o *software* [4]. Além disso, mesmo que as especificações estejam corretas, seus usuários podem utilizá-lo de forma inadequada. Um *software* deve ser suficientemente robusto para salvaguardar seus usuários de erros e atender suas necessidades, além de ser fiel às especificações. Neste contexto, o *software* difere de outros produtos, em vários aspectos críticos [4]:

- Erros graves podem permanecer em um produto de *software*, mesmo depois de ter sido submetido a testes rigorosos, em virtude de sua complexidade lógica;

- Não é trivial estabelecer um padrão uniforme de *software*, que possa fazer parte de regulamentações e inspeções;

- O *software* afeta um grande e crescente número de indivíduos, devido a sua fácil reprodução e maleabilidade em computadores;

- A formação de pequenas equipes sem o conhecimento necessário e/ou o preparo adequado pode produzir *software* de qualidade inferior.

2.2 Certificação de Qualidade

Um aspecto interessante sobre qualidade é que não basta que ela exista: ela deve ser reconhecida pelo cliente. Por causa disso, é necessário que exista algum tipo de certificação oficial, emitida com base em um padrão. Um padrão de qualidade é utilizado para avaliar e julgar um processo, produto e/ou serviço com base em normas ou padrões previamente estabelecidos.

Certificação é um processo que envolve normas ou padrões que identificam características importantes de um produto, processo ou serviço e que resulta na emissão de um documento oficial indicando a conformidade destas características com requerimentos e especificações [3][8]. A aplicação de uma certificação pode ser realizada de três formas:

- Auto-Certificação: ocorre quando o fabricante autodeclara que o seu produto está em conformidade com determinados padrões por ele pré-estabelecidos;

- Consumidor: um potencial consumidor em particular pode requerer que um produto seja submetido para certificação por um corpo de avaliadores por ele selecionado;

- Certificação de Terceiros: ocorre quando um corpo de avaliadores, independentemente de consumidor ou fabricante, aplica um processo de certificação.

A Certificação de Terceiros é a forma de certificação mais empregada atualmente [9], e é onde o contexto dessa dissertação se enquadra.

Aplicada a *software*, a percepção comum obtida é de que uma certificação fornece alguma forma de confiança, geralmente de qualidade do *software*. Contudo, em particular, certificação de *software* pode ser vista de forma diferente por diferentes grupos de pessoas, de acordo com o seu envolvimento com *software* e processos de desenvolvimento de *software*. Portanto, existe uma ambigüidade sobre a expressão "certificação de *software*". Empresas em todos os setores da economia estão aumentando a cada dia sua dependência com relação a soluções de *software* baseadas em sistemas de tecnologia da informação (TI), responsáveis por disseminar conhecimentos e informações nos mais diversos setores de uma empresa, agilizando a comunicação entre eles, e entre eles e seus parceiros e clientes. Conseqüentemente, a produção de um *software* eficiente, eficaz, e de alta qualidade tem tornado-se um fator determinante de competitividade entre as indústrias desenvolvedoras de *software*.

No mercado de *software*, existe um claro interesse dos consumidores de que o *software* possua algum tipo de certificação para que eles possam ter certeza de que ele tenha a qualidade esperada. Existem muitas evidências de que adicionar uma certificação a um *software* fornece-lhe um valor de confiabilidade muito alto. Porém, o conceito e importância de uma certificação não estão completamente disseminados: a indústria desenvolvedora de *software* é muito jovem quando comparada com as outras áreas da indústria, como a automobilística ou construção civil.

A garantia de uma certificação constitui o estágio final em um processo de teste, avaliação e confirmação de que um produto está em conformidade com padrões especificados. Uma certificação de qualidade envolve as três etapas seguintes [9]:

- Avaliação da Qualidade do *Software*: este processo envolve técnicas de Verificação e Validação (V&V), testes, análise estática e dinâmica, medidas para determinar a qualidade do *software* (processo / produto);

- Julgamento da Qualidade do *Software*: este processo envolve a comparação dos testes atuais e resultados das medidas das características com as suas especificações;

- Certificação da Qualidade do *Software*: este processo envolve um corpo certificador de terceiros que produz um documento garantindo que um processo ou produto de *software* está em conformidade com características previamente especificadas.

Nosso trabalho envolve as duas primeiras etapas de um processo de certificação conjuntamente com a produção de um documento (relatório) como resultado do processo avaliativo.

2.3 Qualidade de Processo x Qualidade de Produto

A busca de qualidade e produtividade no desenvolvimento de *software* tem sido intensa. No entanto, ainda não está bem definido como desenvolver um *software* de qualidade. A avaliação de qualidade e a tentativa de corrigir erros em *software*, por si só, mostrou-se insuficiente e limitada para garantir qualidade em *software*. Atualmente, tem-se evidenciado que a qualidade de produto depende fortemente da qualidade e adequação de seu processo de desenvolvimento. Porém, um processo de desenvolvimento de qualidade não garante que o produto final será o esperado, pois as especificações podem estar incorretas e o produto final pode não satisfazer o seu usuário em potencial [10]. Portanto, para se aplicar um processo de qualidade de *software* completo devemos aplicar uma avaliação de qualidade no processo de desenvolvimento (qualidade de processo) e uma avaliação de qualidade no produto final (qualidade de produto).

2.3.1 Qualidade de Processos de *Software*

O processo de *software* é uma seqüência de estágios para o desenvolvimento ou manutenção do *software*, composto por um conjunto de estruturas técnicas e de gerenciamento para o uso de métodos e ferramentas, e de pessoas para desenvolver, testar e manter as tarefas do sistema [11].

A avaliação de processos de *software* compreende [12]:

- A compreensão do estado dos processos de uma organização (empresa), para a melhoria dos mesmos;

- Estabelecer a conformidade dos processos de uma organização (empresa) para com um requisito em particular ou uma classe de requisitos;

- Determinar a adequação dos processos de uma outra organização (empresa) com um contrato ou uma classe de contratos, para o caso de processos de desenvolvimento terceirizados ou compartilhados.

Um ciclo de vida de um *software* é definido como um conjunto de etapas que devem ser cumpridas para o desenvolvimento e manutenção do *software*. A ISO/IEC 12207 define as etapas do ciclo de vida de um *software* como sendo constituídos por um conjunto de atividades, formadas também por um conjunto de tarefas. As atividades que devem ser realizadas durante o ciclo de vida do *software* estão divididas em três classes [13]:

- Processos Fundamentais: consistem de atividades de início e execução do desenvolvimento, operação ou manutenção do *software* durante o seu ciclo de vida. São constituídos por cinco processos: aquisição, fornecimento, desenvolvimento, operação e manutenção;

- Processos de Apoio: compostos por atividades que auxiliam um outro processo fundamental ou organizacional. São constituídos por oito processos: documentação, gerência de configuração, garantia de qualidade, verificação, validação, revisão conjunta, auditoria e resolução do problema;

- Processos Organizacionais: composto por atividades que implementam uma estrutura constituída de processos de ciclo de vida e pessoal associado (recurso humano), melhorando continuamente a estrutura dos processos. São constituídos por quatro processos: gerenciamento, infra-estrutura, melhoria e treinamento.

A tabela 2.1 mostra todos os processos envolvidos e suas respectivas definições [13].

Tabela 2.1: Processos do Ciclo de Vida de um Software (ISO/IEC 12207)

Processos Fundamentais	Início e execução do desenvolvimento, operação ou manutenção do s*oftware* durante o seu ciclo de vida.
Aquisição	Atividades do consumidor que incluem: a definição da necessidade de adquirir um *software*, o pedido, a seleção do fornecedor, a gerência da aquisição e a aceitação do *software*.
Fornecimento	Atividades dos fornecedores do *software*, que incluem: a preparação da proposta, contrato, a determinação dos recursos necessários, os planos de projeto e a entrega do *software*.
Desenvolvimento	Atividades dos desenvolvedores do *software*, que incluem: a análise de requisitos, o projeto, a codificação, a integração, os testes, a instalação e a aceitação do *software*.
Operação	Atividades dos operadores do *software*, que incluem: a operação do *software* e o seu suporte operacional.
Manutenção	Atividades de quem faz a manutenção no *software*.
PROCESSOS DE APOIO	Auxiliam outros processos.
Documentação	Registro de informações produzidas por um processo ou atividade de produção do *software*.
Gerência de Configuração	Identificação e controle dos itens do *software*.
Garantia de Qualidade	Garante os processos e produtos de *software* em conformidade com os requisitos e os planos pré-estabelecidos.
Verificação	Determina se os produtos de *software* de uma atividade atendem completamente aos requisitos ou condições impostas a eles.
Validação	Determina se os requisitos e o produto final (sistema ou *software*) atendem ao uso específico proposto.
Revisão Conjunta	Define as atividades para avaliar a situação e produtos de uma atividade de um projeto.
Auditoria	Determina adequação aos requisitos, planos e contratos.
Resolução de Problemas	Análise e resolução de problemas de qualquer natureza ou fonte, descobertos durante a execução do desenvolvimento, operação, manutenção ou outros processos.
Processos Organizacionais	Implementam uma estrutura constituída de processos de ciclos de vida e pessoal associado, melhorando continuamente a estrutura e os processos.
Gerência	Gerenciamento de Processos.
Infra-estrutura	Fornecimento de recursos para outros processos, incluindo: de hardware, software, ferramentas, técnicas, padrões de desenvolvimento, operação ou manutenção.
Melhoria	Atividades para estabelecer, avaliar, medir, controlar e melhorar um processo de ciclo de vida de software.
Treinamento	Atividades para prover e manter pessoal treinado.

Os padrões ISO 9000-3 enunciam os procedimentos para a garantia da qualidade de *software* em relação a seu processo de desenvolvimento, presumindo que o produto de *software* é o resultado de um acordo contratual entre um cliente e um fornecedor, sendo este último uma empresa com um sistema de qualidade suportado pela ISO 9000. A aceitação do padrão internacional de qualidade ISO 9000 tem despertado um grande interesse das organizações, pois, através dele, elas podem conquistar uma certificação de qualidade, o que significa alcançar um padrão internacional em seus processos. Da mesma forma, os clientes vêem nesta certificação um indicador que assegura a qualidade dos produtos e serviços oferecidos por elas.

Muitas organizações buscam novos paradigmas que conduzam a uma melhoria contínua e progressiva da qualidade de seus processos de desenvolvimento. Assim surgiram alguns modelos de qualidade para processos de desenvolvimento de *software* como:

- Modelo de Maturidade e Capacidade de *Software* (*Capability Maturity Model* - CMM) [14]: este modelo está sendo implantado em muitas organizações, objetivando a padronização e a melhora de processos de desenvolvimento de *software*. O princípio fundamental deste modelo é que a qualidade do produto de *software* pode ser alcançada através da melhoria da qualidade de seus processos [15]. O CMM é estruturado em cinco níveis em ordem crescente de maturidade. Quando a organização se encontra em um determinado nível, deve seguir atividades determinadas pelo modelo para alcançar o nível seguinte [16]. Conforme estudos da SEI/CMU (*Software Engineering Institute/Carnegie Mellon University*) uma empresa de *software* que alcance certificação ISO 9001 atende a todos os requisitos para ser classificada no nível 2 do CMM, mesmo que tenha alcançado alguns requisitos além dos requisitos de níveis superiores [17]. O modelo CMM tem sido muito criticado por alguns pesquisadores por não ter base teórica formal, sendo fundamentada na experiência de um grupo de pessoas [4]. Em [18], por exemplo, o autor argumenta que o CMM é uma mistificação do processo evolutivo e não uma representação legítima do processo de *software*, podendo levar a organização a um colapso em seu potencial competitivo.

- *Bootstrap* [19]: derivado do modelo CMM, é um projeto que faz parte do Projeto Esprit, desenvolvido na Comunidade Européia, para avaliação de organizações. O *Bootstrap* desenvolve um método de avaliação, medição quantitativa e melhoria do processo de *software*. Avalia, também, as unidades produtoras de *software* e seus projetos. Além disso, determina o nível de maturidade da organização, identificando seus méritos e deficiências e fornecendo guias para o seu aperfeiçoamento.

- *Trillium* [20]: desenvolvido no Canadá, é derivado também do modelo CMM e de outros métodos para avaliação de organizações. O objetivo do *Trillium* é prover um método para o início e a condução de um programa de melhoramento contínuo da qualidade de processos. Este modelo é orientado às telecomunicações, fornecendo uma perspectiva do produto segundo os padrões ISO, sendo desenvolvido sob a perspectiva do cliente.

- O Projeto *Software Process Improvement and Capability dEtermination* (SPICE) [12]: objetiva a criação de normas para avaliação de processos e suas melhorias contínua, baseando-se nas melhores características de modelos como o CMM, *Trillium* e *Bootstrap*. A melhoria de processos é realizada através de avaliações que descrevem práticas usuais da organização, de uma unidade organizacional ou de um projeto. A análise dos resultados é feita em relação às necessidades do negócio da organização, levando em consideração seus aspectos positivos e negativos, assim como os riscos envolvidos no processo. O projeto SPICE pode ser usado por organizações com atividades de planejamento, gerenciamento, monitoração, controle, fornecimento, desenvolvimento, operação e suporte de *software*. Esse projeto é interessante por seu direcionamento e sua flexibilidade, para que as organizações que o utilizem determinem a capacitação de cada um dos seus processos, com o intuito de promover melhorias contínuas nos mesmos. Desta forma, obtém-se uma avaliação mais detalhada do estado de organização [21]. A estratégia de melhoria de processos deve ser dinâmica, pois para assegurar a qualidade de produtos de *software* é necessário que as habilidades se multipliquem, a tecnologia seja modificada, e que se crie novos ambientes de trabalho [11]. Atualmente, o projeto SPICE tornou-se uma norma ISO – ISO/IEC 15504.

2.3.2 Qualidade de Produtos de *Software*

Para avaliação de qualidade de produtos de *software*, as organizações internacionais de normalização ISO/IEC definiram as seguintes normas [22]:

- Norma de Avaliação das Características de Qualidade e Métricas: compreendendo a definição e seleção das (*i*) características e subcaracterísticas de qualidade, (*ii*) métricas externas e (*iii*) métricas internas.

- Normas de Avaliação dos Produtos de *Software*: envolvendo (*i*) a visão geral do produto, (*ii*) o planejamento e o gerenciamento, (*iii*) o processo de avaliação da equipe de desenvolvimento, (*iv*) o processo de seleção dos adquirentes, (*v*) o processo de avaliação aplicado pelos avaliadores, e (*vi*) os módulos de avaliação.

- Requisitos de qualidade e teste de pacotes de *software*.

Uma avaliação de qualidade de produto de *software* é direcionada para um único produto de *software* de forma a julgar seu nível de qualidade [9]. A análise é feita utilizando um conjunto de características por meio de técnicas apropriadas aplicadas a várias partes do produto: especificações, documentos técnicos, código-fonte, manuais do usuário, etc.

Uma avaliação de qualidade de produto de *software* está relacionada com a identificação de características importantes e que elas estão em conformidade com requerimentos e especificações pré-estabelecidos [9]. O principal propósito desta avaliação está em fornecer notas quantitativas e recomendações referente ao produto de *software* que sejam compreensíveis, aceitáveis e confiáveis por qualquer uma das partes interessadas.

Modelos de avaliação de qualidade de *software* devem mapear a realidade e/ou os requisitos pretendidos pelos usuários, enfocando as questões referentes à construção do produto e à monitoração dos possíveis desvios. Neste contexto, os modelos de avaliação de qualidade estão diretamente associados com o processo de medição, determinando como as medidas serão executadas e planejadas [21]. Apenas um bom método de desenvolvimento não é suficiente para garantir um produto de qualidade. Deve-se considerar também os fatores de suporte à decisão,

como a qualidade da equipe de desenvolvimento, e o tempo estipulado sob o qual os elementos desta equipe devem trabalhar [23].

Vários modelos de avaliação de qualidade de *software* têm surgido. O Padrão ISO é aceito mundialmente como uma referência e será apresentado na próxima seção. Outros modelos que podemos citar como exemplos são:

- O Paradigma *Goal/Question/Metric* (GQM) [24]: é uma estrutura para o desenvolvimento de um programa de métricas: definição, planejamento, construção, análise e *feedback*. Foi desenvolvida para várias áreas de estudo, especialmente aquela concernente a questões de melhoramento, e consiste em três etapas [25]:

  1. Gerar um conjunto de alvos: baseando-se nas necessidades da organização, determina-se o que se quer melhorar e definem-se os alvos em termos de propósitos, perspectivas e ambientes, usando-se modelos genéricos.

  2. Derivar um conjunto de questões: as questões quantificam os alvos como sendo possíveis, requerendo a interpretação de termos nebulosos, dentro do contexto do ambiente de desenvolvimento. As questões são classificadas como sendo relacionadas a produtos ou processos e fornecem *feedback* da perspectiva de qualidade.

  3. Desenvolver um conjunto de métricas: essas métricas fornecem as informações necessárias para responder a cada questão. As métricas podem ser objetivas e subjetivas e possuem guias de interpretação, isto é, um valor que indique se o produto é de alta qualidade. Geralmente, uma questão não é respondida simplesmente por uma métrica, mas por uma combinação delas. Uma vez definidos os alvos, derivadas as questões, e desenvolvidas as métricas, são criadas matrizes para relacionar alvos/questões/métricas.

- O Projeto SCOPE [26]: Na estrutura e desenvolvimento do projeto Esprit, o projeto que trata das questões de certificação de qualidade de produtos de *software* é chamado *Software Certification Programme in Europe* (SCOPE). Um dos resultados mais importantes deste

projeto é a definição de uma estrutura de avaliação, que tem sido experimentada em muitos estudos de caso. A avaliação é realizada para vários ciclos de vida, através do uso de diversas classes de métricas, como o tamanho, a estrutura do fluxo de controle, a modularidade e o fluxo de informação, a estrutura de dados, a eficiência e a complexidade de algoritmos, e as medidas gerais de complexidade. Seus principais objetivos são [27]:

- Elucidar o relacionamento entre fornecedores e clientes, através de procedimentos de definição, permitindo concessões de um selo de qualidade, quando um produto possui um determinado conjunto de atributos de qualidade;

- Desenvolver tecnologias de avaliação eficientes e efetivas, para a concessão do selo de certificação;

- Promover a divulgação de modernas tecnologias de engenharia de *software*, para que sejam usadas durante o desenvolvimento de produtos de *software*.

- O Modelo Rocha [28]: define a qualidade de produtos de *software* a partir dos seguintes conceitos:

  - Objetivos de qualidade: são as propriedades gerais que o produto deve possuir;

  - Fatores de Qualidade: determinam a qualidade na visão dos diferentes usuários do produto. Podem ser compostos por subfatores, quando estes não definem completamente, por si só, um único objetivo;

  - Critérios: são atributos primitivos, possíveis de serem avaliados;

  - Processos de Avaliação: determinam o processo e os instrumentos a serem utilizados, de forma a se medir o grau de presença, no produto, de um determinado critério;

- Medidas: são os resultados da avaliação do produto, segundo os critérios;

- Medidas Agregadas: são os resultados da agregação das medidas obtidas ao se avaliar de acordo com os critérios, além de quantificarem os fatores.

Os objetivos de qualidade são atingidos através dos fatores de qualidade, que podem ser compostos por subfatores. Objetivos, fatores e subfatores não são diretamente mensuráveis e só podem ser avaliados através de critérios. Um critério é um atributo primitivo. Um único critério não descreve completamente um determinado fator ou subfator. Da mesma maneira, nenhum fator define completamente um objetivo.

Neste trabalho iremos empregar a avaliação da qualidade de produtos de *software* que autenticam usuários a partir de características físicas e/ou comportamentais (biométricas). O modelo que usaremos será baseado no padrão ISO, conforme apresentaremos na próxima seção.

2.4. O Padrão ISO

A *International Organization for Standardization* (ISO) é uma organização não-governamental estabelecida em 1947. Sua missão é promover o desenvolvimento de atividades de normatização a nível mundial. O seu trabalho resulta em acordos entre países que são publicados como Normas Internacionais. Qualquer país pode participar dos trabalhos da ISO em Comitês Técnicos ou Subcomitês. A participação pode ser do tipo P, quando há atuação ativa nos trabalhos com obrigação de voto, ou do tipo O, quando o país participa como observador, recebendo cópias dos documentos, participando das reuniões e apresentando comentários, mas sem o direito de voto [3].

A *International Electrotechnical Commission* (IEC), fundada em 1906, é a organização mundial que publica normas internacionais relacionadas com eletricidade, eletrônica e áreas relacionadas, e atualmente conta com a participação de mais de 50 países.

A ISO e a IEC são as duas organizações internacionais mais importantes para o setor de *software*. O padrão ISO apresentado nesta seção está relacionado com a avaliação de qualidade de *software*, a partir de uma abordagem nas normas ISO/IEC 14598 [29] e 9126 [30]. Estas normas são produzidas por um comitê conjunto, o *Joint Technical Committees* (JTC) na área de Tecnologia

da Informação (TI). Além disto, apresentaremos também a norma ISO/IEC 12119 responsável pelo controle de qualidade em pacotes de *software*. As normas ISO/IEC 14598-1, 9126 e 12119 foram base para o desenvolvimento de um modelo hierárquico para a avaliação de pacotes de *software* biométricos. Cada uma das normas mencionadas e sua respectiva composição são mostradas na figura 2.1. Nos tópicos a seguir, cada uma delas será explicada com mais detalhes.

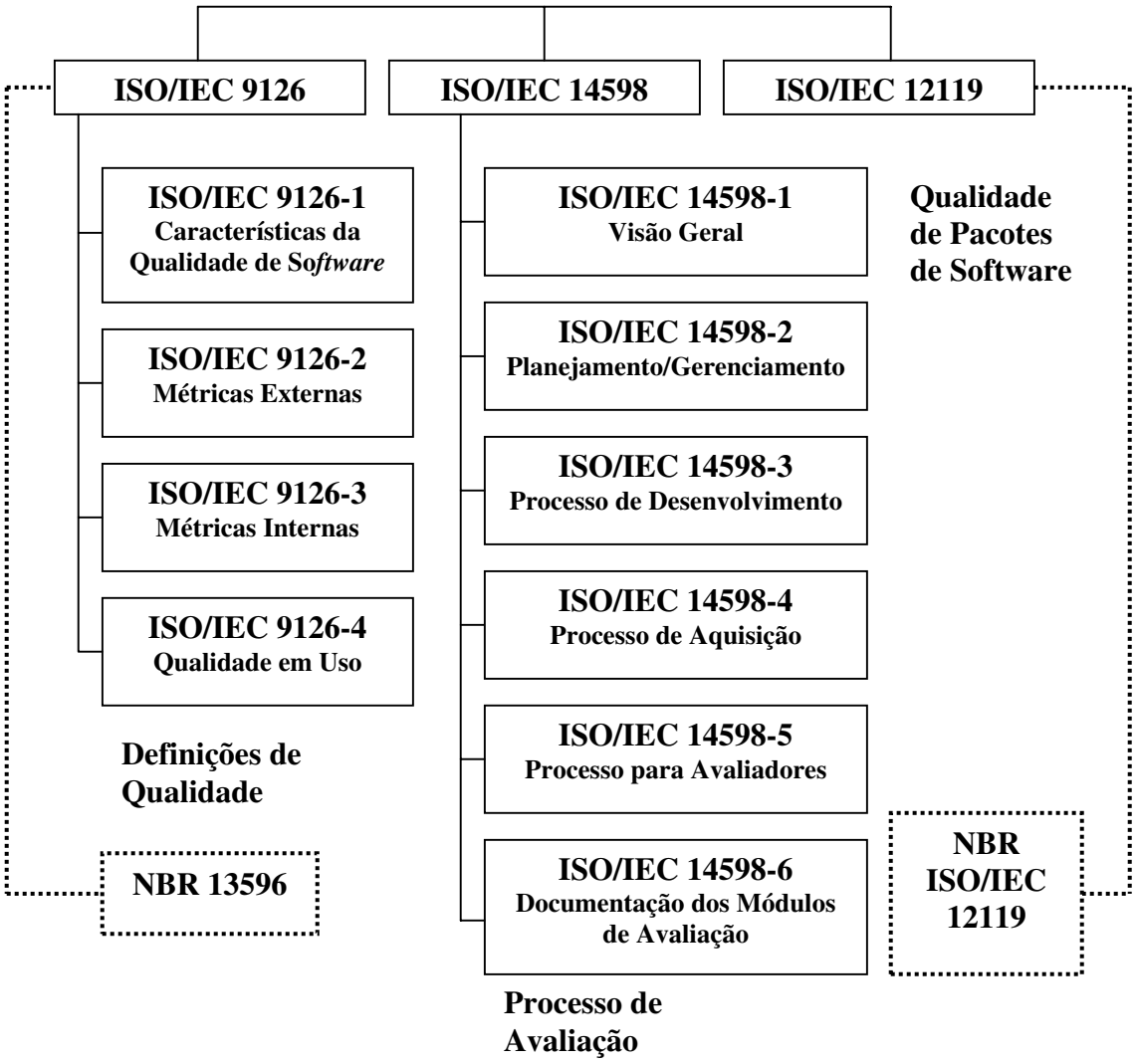


Figura 2.1: Normas ISO e suas normas componentes para avaliação de qualidade de s*oftware*.

2.4.1 Norma ISO/IEC 14598

Esta norma determina como proceder em um processo de avaliação de qualidade. O processo de avaliação é dividido em 6 normas que padronizam as etapas deste processo. Faremos uma abordagem mais completa na norma 14598-1, pois esta norma está orientada para a avaliação de qualidade de produtos de *software*, enquanto as demais estão relacionadas com a avaliação de qualidade de processos de *software* e elementos componentes da avaliação, como, por exemplo, os avaliadores, o que está fora do escopo deste trabalho.

O processo de avaliação de qualidade de produtos de *software* descrito na norma 14598-1 é representado na figura 2.2. Os blocos quadrados à esquerda são as tarefas a serem cumpridas em cada etapa, que são ainda subdivididas em tarefas menores com seus objetivos específicos. Os blocos quadrados à direita contêm as normas adicionais que apóiam o processo avaliativo, cujas características veremos na seção posterior.

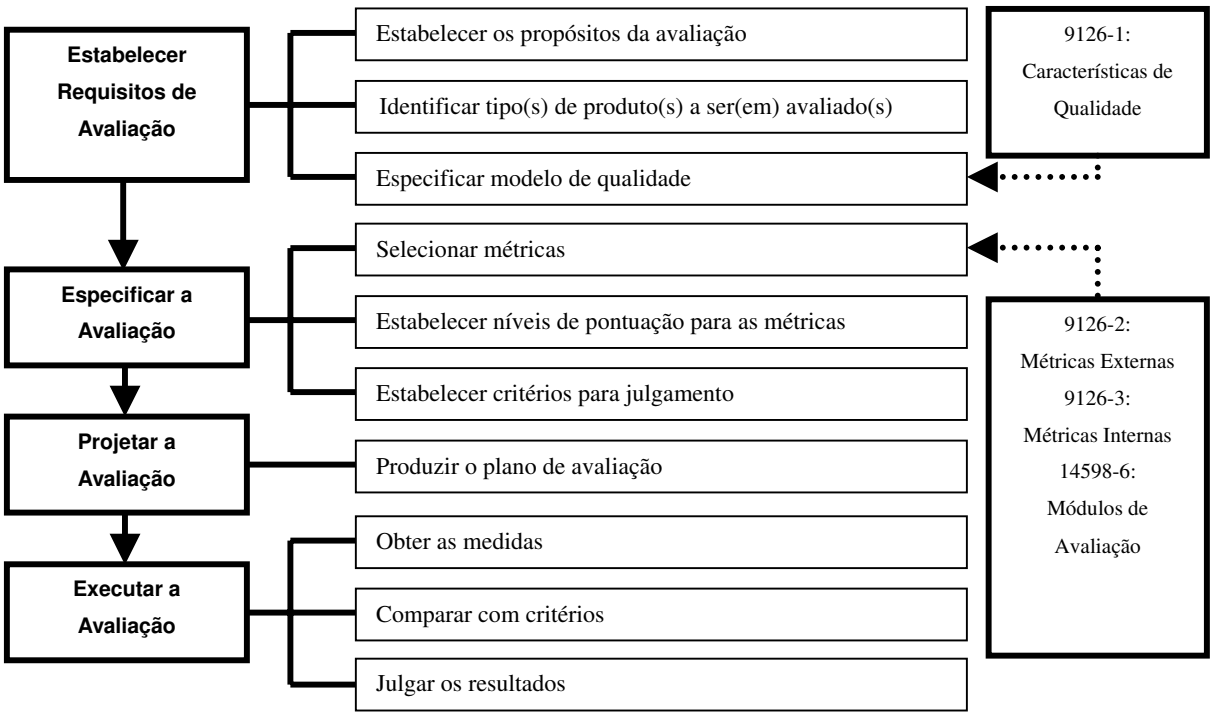


Figura 2.2: Processo de Avaliação de Qualidade de *Software*.

Cada tarefa descrita na figura 2.2 é sucintamente descrita abaixo [3]:

- Estabelecer o propósito da avaliação – o propósito da avaliação é apoiar diretamente o desenvolvimento e a aquisição de *software* que atenda às necessidades do usuário e do cliente. O objetivo final é assegurar que o produto forneça a qualidade requerida e que ele atenda as necessidades implícitas e explícitas do usuário.

- Identificar tipo(s) de produto(s) a ser(em) avaliado(s) – o tipo de produto de *software*, quer seja um produto em desenvolvimento ou final a ser avaliado, dependerá do estágio no seu ciclo-de-vida e do propósito da avaliação. O objetivo é que o produto, ao ser utilizado pelo usuário, atenda suas necessidades implícitas e explícitas.

- Especificar o modelo de qualidade – A primeira etapa na avaliação de *software* é selecionar as características de qualidade relevantes utilizando um modelo de qualidade. Os modelos de qualidade geralmente representam a totalidade dos atributos de qualidade de *software* classificados em uma estrutura de árvore hierárquica. O nível mais alto é constituído por características de qualidade ou elementos resultantes de uma classificação do produto, enquanto o nível mais baixo é composto pelos atributos primitivos de qualidade de *software*. Neste contexto, a ISO/IEC 9126-1 fornece um modelo de propósito geral, definindo seis amplas características: funcionalidade, confiabilidade, usabilidade, eficiência, manutenibilidade e portabilidade. Este modelo será explicado na próxima seção com mais detalhes.

- Selecionar métricas – a forma pela qual características ou componentes do produto de *software* têm sido definidas não permite sua medição direta. Portanto, é necessário estabelecer métricas que se correlacionem às características. Todo atributo quantificável que se correlacione com uma característica ou componente do produto e interaja com o seu ambiente pode ser definido como uma métrica. É importante que as medições de um produto possam ser economicamente viáveis e fáceis de aplicar e utilizar. As normas ISO/IEC 9126-2 e 9126-3 definem métricas de qualidade, enquanto a norma 14598-6 define módulos de avaliação, cujo objetivo é a utilização das métricas definidas nas

normas 9126-2 e 9126-3 de forma eficiente e que permita a troca de informações sobre avaliações anteriores, garantindo assim que uma avaliação seja reproduzível e imparcial.

- Estabelecer níveis de pontuação para as métricas – as particularidades quantificáveis de um produto podem ser medidas qualitativamente usando-se métricas de qualidade. O resultado, isto é, o valor medido é mapeado numa escala. Este valor, por si só, não mostra o nível de qualidade do produto e nem de satisfação dos requisitos. Para isto, a escala precisa ser dividida em faixas correspondentes aos diversos graus de satisfação dos requisitos. Assim, o valor medido é traduzido em um grau de satisfação que determina o nível de qualidade do requisito avaliado.

- Estabelecer critérios para o julgamento – para julgar a qualidade de um produto, o resultado da avaliação de cada característica precisa ser sintetizado. Convém que o avaliador prepare um procedimento para tanto, com critérios diferentes para características de qualidade diferentes, onde cada característica ou componente do produto poderá ser representado em termos mensuráveis ou ser uma combinação ponderada de suas subcaracterísticas ou subcomponentes. O procedimento normalmente incluirá outros aspectos como tempo e custo, os quais contribuem para o julgamento da qualidade de um produto de *software* em um ambiente particular.

- Produzir o plano de avaliação – o plano de avaliação descreve os métodos de avaliação e o cronograma das ações do avaliador, que podem ser encontradas nas normas ISO/IEC 14598-3, 14598-4 e 14598-5.

- Obter as medidas – para medição, as métricas selecionadas são aplicadas ao produto de *software*. Como resultado, obtém-se os valores nas escalas das métricas.

- Comparar com critérios – os valores medidos e obtidos na etapa anterior são comparados com critérios de qualidade pré-determinados.

- Julgar os resultados – o julgamento é a etapa final do processo de avaliação do *software*, onde um conjunto de níveis pontuado é resumido. O resultado é uma declaração de quanto o produto de *software* atende aos requisitos de qualidade. Então, a qualidade resumida é comparada com outros aspectos como tempo e custo. Finalmente, uma decisão será tomada baseada nos critérios de qualidade. O resultado é uma decisão quanto à aceitação ou rejeição, ou quanto à liberação ou não do produto.

Esta norma foi utilizada para que pudéssemos estabelecer uma base para definirmos os passos de um processo avaliativo de um produto de *software* biométrico. Estes passos foram adequados aos propósitos e objetivos desta dissertação e particularizados à realidade desses tipos de produto.

2.4.2 Norma ISO/IEC 9126

A estrutura da ISO/IEC 9126 possui também um conjunto de documentos técnicos que definem características de qualidade de *software* e seus indicadores, orientando o planejamento e a execução da avaliação [22]:

- ISO/IEC 9126-1: fornece características e subcaracterísticas de qualidade, sendo uma norma essencialmente de definições. As características e subcaracterísticas presentes nessa norma são mostradas e definidas na tabela 2.2.

- ISO/IEC 9126-2: define métricas externas para a medição de características e subcaracterísticas de qualidade da norma ISO/IEC 9126-1. Estas métricas referem-se a medições indiretas de um produto de *software*, a partir da medição do comportamento do sistema computacional do qual o produto faz parte.

- ISO/IEC 9126-3: define métricas internas para a medição de um produto de *software*. Estas métricas referem-se a medições diretas de um produto, a partir de suas características internas, sem que seja necessária a execução do programa.

Tabela 2.2: Características e Subcaracterísticas de *software* – ISO/IEC 9126

Qualidade de Produtos de *Software* – ISO/IEC 9126	
Características	**Subcaracterísticas**
Funcionalidade: as funções e propriedades específicas de um produto, que satisfazem as necessidades do usuário.	**Adequação:** existência de um conjunto de funções apropriadas para as tarefas requeridas.
	Acurácia: produção de resultados ou efeitos corretos.
	Interoperabilidade: habilidade de interação do produto de *software* com outros produtos.
	Conformidade: o produto está de acordo com as convenções, as normas e os regulamentos estabelecidos.
	Segurança: aptidão para evitar acessos não-autorizados a programas e dados.
Confiabilidade: o produto de *software* é capaz de manter seu nível de desempenho, ao longo do tempo, nas condições estabelecidas.	**Maturidade:** estado de maturação do *software*, detectado por sua baixa freqüência de falhas.
	Tolerância a Falhas: o nível de desempenho é mantido, quando ocorrem falhas.
	Recuperabilidade: existem mecanismos que restabelecem e restauram os dados após a ocorrência de falhas.
Usabilidade: esforço necessário para a utilização do sistema, baseado em um conjunto de implicações e de condições do usuário.	**Inteligibilidade:** facilidade de entendimento dos conceitos utilizados no produto de *software*.
	Apreensibilidade: facilidade de aprendizado do *software*.
	Operacionalidade: faculdade de operar e controlar operações pertinentes ao *software*.
Eficiência: os recursos e os tempos envolvidos são compatíveis com o nível de desempenho requerido pelo *software*.	**Comportamento no tempo:** refere-se ao tempo de resposta de processamento.
	Comportamento dos recursos: relaciona-se com a quantidade dos recursos empregados.
Manutenibilidade: refere-se ao esforço necessário para a realização de alterações específicas no produto de *software*.	**Analisabilidade:** característica de ser possível diagnosticar deficiências e causas de falhas.
	Modificabilidade: característica que o produto deve ter de forma a facilitar modificações e remoções de defeitos.
	Estabilidade: ausência de riscos ou ocorrências de defeitos inesperados no *software*.
	Testabilidade: facilidade de o produto ser testado.
Portabilidade: facilidade de o *software* poder ser transferido de um ambiente operacional para outro.	**Adaptabilidade:** facilidade de o produto poder ser adaptado a novos ambientes.
	Instalabilidade: facilidade de instalação do produto de *software*.
	Conformidade com padrões de portabilidade: o produto está em conformidade com padrões ou convenções de portabilidade.
	Substituibilidade: o produto de *software* pode ser substituído por outro, sem grandes esforços.

A ISO/IEC 9126 define um modelo hierárquico *top-down* contendo referências necessárias para a realização de comparações ou medições. Em um modelo hierárquico *top-down* a ordem de

importância hierárquica dar-se-á de cima para baixo, enquanto a avaliação dos elementos e de suas respectivas medições dar-se-á de baixo para cima, conforme ilustrado na figura 2.3. No nível mais alto encontram-se as características previamente definidas na tabela 2.2. As definições apresentadas na tabela 2.2 mostram que elas evitam a possibilidade de combinar ou utilizar inadequadamente as características [31]. Cada característica é subdividida em subcaracterísticas, de forma a detalhar o ponto de vista quando analisando um produto de *software*, e localiza-se um nível abaixo na hierarquia. Porém, as subcaracterísticas não podem realmente ser mensuradas, porque não possuem acurácia, e, portanto, elas devem ser subdivididas em atributos. Para cada tipo diferente de produto de *software* e subcaracterísticas, os atributos devem ser identificados de acordo com o propósito da avaliação.

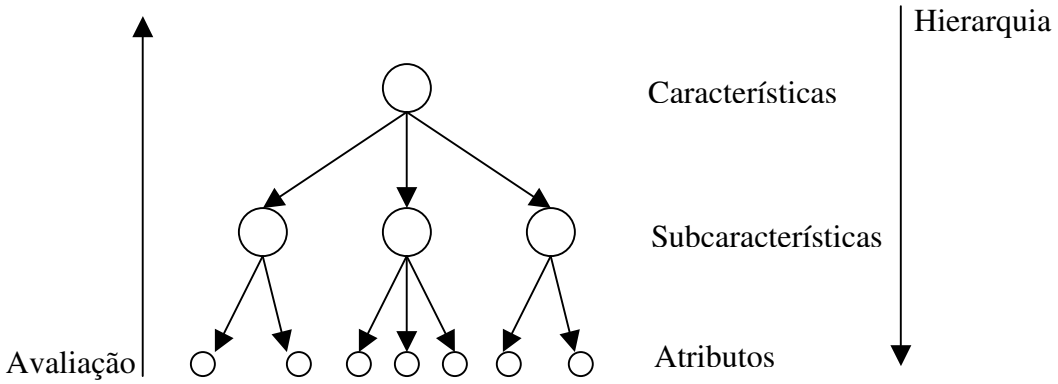


Figura 2.3. O modelo hierárquico *top-down* ISO/IEC 9126

Apesar da grande relevância da ISO/IEC 9126, há dificuldades em adequar sua aplicabilidade na avaliação prática de produtos de *software* [32], pois as características de qualidade, por ela determinadas, não são diretamente mensuráveis [33]. Portanto, para que se obtenha a qualidade desejada de produtos de *software*, fazem-se necessários modelos que viabilizem a avaliação de qualidade destes produtos: não é mais tolerado o uso de modelos artesanais na elaboração de programas, pois é necessário assegurar um nível mais elevado de qualidade nos produtos de *software*. Para atender as necessidades de avaliação de um produto de *software* biométrico, tornou-se necessário, a partir do modelo hierárquico ISO/IEC 9126, montar um novo modelo que suportasse os conceitos envolvidos nestes produtos e mensurá-los, identificando seus pontos fortes e fracos.

2.4.3 Norma ISO/IEC 12119

Esta norma internacional é aplicada a pacotes de *software*. Um pacote de *software* é um conjunto completo e documentado de programas fornecido a vários usuários para uma aplicação ou função genérica [34], ou seja, é um *software* ou sistema em conjunto com suas documentações. Esta norma estabelece:

- Requisitos para pacotes de *software* (requisitos de qualidade);

- Instruções de como testar um pacote de *software* de acordo com estes requisitos (instruções para testes, em particular, para testes executados por terceiros).

Esta norma trata somente de como os pacotes de *software* são ofertados e entregues. Ela não abrange seus processos de produção, nem atividades ou produtos intermediários. Esta norma tem como um de seus possíveis alvos entidades que desejam estabelecer um esquema de certificação de terceiros, que é o desejado nesta dissertação.

Os requisitos de qualidade apresentados nessa norma são, em resumo [34]:

- O requisito de que cada pacote de *software* tenha uma descrição do produto e uma documentação do usuário. A descrição do produto define o produto em si e faz parte de sua documentação, além de prover informações sobre a documentação do usuário, sobre o programa e, se houver, sobre os dados. Esta documentação deve estar disponível para qualquer pessoa nela interessada. Os principais objetivos da descrição do produto são ajudar o usuário ou comprador em potencial na avaliação da adequação do produto à sua realidade e necessidades, e servir como base para testes. A documentação do usuário deve conter as informações necessárias para o uso do produto, incluindo as funções a serem chamadas pelo usuário no programa e sua manipulação, as limitações do produto, e os processos de instalação e manutenção, caso possam ser realizados pelo usuário. Todas as informações na documentação do usuário devem ser corretas (livre de ambigüidade e erros), consistentes (livre de contradições internas e em relação à descrição do produto), inteligíveis (compreensível, clara e objetiva) e com facilidade de visão geral;

- Os requisitos para a descrição do produto. Em particular, esta descrição deve conter informações específicas do produto e todas as suas declarações, que devem ser testáveis e corretas.

- Requisitos para a documentação do usuário;

- Requisitos para os programas e dados, se existirem, inclusos no pacote de *software*.

Utilizando esta norma, possibilitamos suprir uma necessidade de visualizar um produto de *software* biométrico como um produto comercial. Adaptamos os conceitos desta norma aos nossos objetivos e aos conceitos envolvidos nesse tipo de produto. Dessa forma, o produto de *software* biométrico não é somente um produto final de um processo de desenvolvimento de um *software*, mas, além disso, um produto pronto para ser comercializado, um pacote completo (produto mais suas documentações), para avaliá-lo no âmbito de seus objetivos e do seu potencial mercado consumidor.

CAPÍTULO 3

BIOMETRIA

Neste capítulo apresentamos os conceitos básicos que regem a biometria e sistemas biométricos de identificação pessoal. Mostramos alguns órgãos de padronização voltados para biometria e a necessidade de suas existências. Apresentamos as subdivisões de um sistema biométrico e definiremos cada uma delas. 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 para realizar a tarefa de autenticação pessoal.

3.1 O que é Biometria?

A Biometria é o ramo da ciência que estuda a mensuração dos seres vivos [35]. Tecnologias biométricas são definidas como "métodos automáticos de verificação ou identificação da identidade de uma pessoa viva baseados em características fisiológicas ou comportamentais" [6]. Vamos examinar algumas das palavras-chave encontradas nesta definição:

Métodos Automáticos: Dentro do contexto de um sistema automatizado, os componentes que servem de fundamento para a implementação de um sistema biométrico são três: O primeiro componente é o mecanismo de captura de um sinal digital ou analógico das 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 a realização da tarefa de verificação/identificação automática. O termo "automática" demanda que uma vez feita a captura da amostra biométrica, os processos que envolvem o processamento, classificação e o resultado da autenticação sejam feitos sem a 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. Neste 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. Neste caso, o sistema decide se existe um casamento (*matching*) entre a informação de entrada e a armazenada na base de dados. Este 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. Este tipo de sistema é chamado também de sistema de identificação.

Pessoa viva: define que um dispositivo de captura seja capaz de identificar se na amostra biométrica coletada existe alguma característica "viva". Inicialmente, a interpretação deste 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. Exemplos de dispositivos que possam identificar características "vivas" já pode ser encontrado em alguns sistemas de reconhecimento de faces. Neste caso, o sensor que faz a captura da imagem não é uma câmera de vídeo comum, mas 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 à intensidade de luz casem com as da base de dados, aquelas referentes à distribuição de temperatura serão diferentes e, portanto, o resultado do pedido de autenticação de identidade falhará.

Características Fisiológicas e Comportamentais: 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 comportamental é mais um reflexo de atitudes psicológicas do indivíduo. A assinatura é a característica comportamental mais utilizada para autenticação. Outros comportamentos que podem ser utilizados são a maneira como se digita nos teclados e a maneira de falar.

As características comportamentais tendem a variar com o tempo. Por este motivo, muitos sistemas biométricos permitem que sejam feitas atualizações de seus dados biométricos de referência à medida que estes vão sendo utilizados [36]. 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 fisiológicos e comportamentais são importantes por vários motivos. Primeiro, o grau de variação intrapessoal numa característica fisiológica é menor do que em uma característica comportamental. 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 têm um grande trabalho em ajustar as variações intrapessoais. As técnicas comportamentais e as fisiológicas provêem níveis significativamente maiores de autenticação e segurança do que aquelas baseadas em senhas e cartões isoladamente.

3.2 Visão Geral envolvendo Tecnologias Biométricas

Em geral, a construção de sistemas de autenticação pessoal edifica-se sobre três pilares [37]:

1. Prova por Posse: possuir um objeto que seja em si a autenticação (um cartão),

2. Prova por Conhecimento: informações baseadas no seu conhecimento (senhas),

3. Prova por Propriedade: características biométricas (uma característica biométrica).

A mais comum delas é a prova por conhecimento pela sua simplicidade e facilidade de implementação. Senhas são tradicionalmente utilizadas em diversos sistemas e existem muitas razões pelas quais elas não são seguras, sendo que a principal delas é que os usuários de um sistema geralmente escolhem senhas "fracas", ou seja, que podem ser facilmente descobertas ou adivinhadas [38].

A partir desses três pilares é possível criar diferentes esquemas de autenticação. Estes esquemas podem ser mais ou menos complexos dependendo do grau das 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 autenticação, o custo do sistema, entre outros.

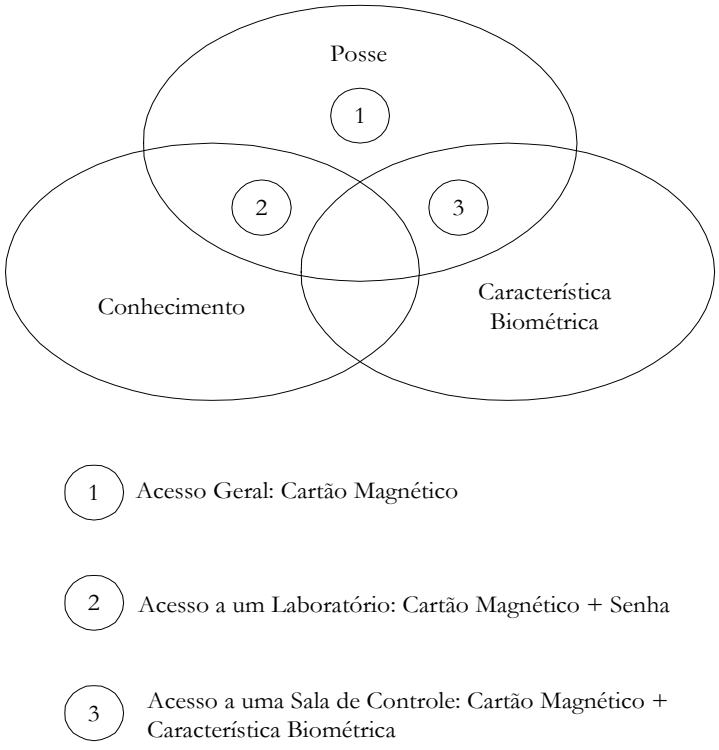


Figura 3.1: Esquemas de acesso para autenticação de autenticação.

A figura 3.1 apresenta uma representação desses três pilares exemplificando três esquemas de acesso a diferentes locais. No primeiro esquema, o acesso a um determinado lugar é permitido

simplesmente apresentando-se um cartão magnético. No segundo esquema, o acesso é permitido através do conhecimento de uma senha e da posse de um cartão magnético. O terceiro caso é semelhante ao anterior, com a diferença de que o acesso só é permitido se for apresentada também 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 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 e à segurança do serviço de autenticação.

Um típico processo de autenticação utilizando tecnologias biométricas consiste nos seguintes passos básicos [39]:

1. Capturar a(s) amostra(s) biométrica(s);

2. Avaliar a qualidade da amostra biométrica capturada e, se necessário, recapturá-la;

3. Processar a amostra biométrica capturada para comparação*;*

4. Comparar a amostra biométrica processada com o *template* previamente armazenado na base de dados (ou *templates*) para determinar se a amostra biométrica processada pertence ao usuário do *template* armazenado. Esta comparação pode ser feita fazendo uso do processo de autenticação por verificação ou identificação.

Um *template* é associado com um identificador do usuário. Eles podem ser armazenados em cartões de memória, em uma base de dados central ou em cartões magnéticos. O tipo de armazenamento dar-se-á pela aplicabilidade prática a que se destina o sistema biométrico e pelo tamanho dos *templates* gerados [40].

3.2.1. Medidas de Desempenho em Sistemas Biométricos

A captura de amostras biométricas por um dispositivo ou sensor biométrico não é um processo que leve, após sucessivas tentativas, à extração de características perfeitamente precisas, repetitíveis e idênticas destas amostras. Muitas são as variáveis que influenciam para esta variabilidade nas características: estado físico, emocional e/ou psicológico, a idade, as condições de temperatura e umidade são alguns exemplos que afetam o indivíduo que fornece a amostra biométrica, e o dispositivo ou sensor que a captura. Estas variações nas características ocasionam erros de autenticação dos usuários no sistema biométrico, rejeitando usuários legítimos e aceitando usuários impostores.

Os erros de autenticação em sistemas biométricos são medidos através de duas estimativas: erro Tipo I e erro Tipo II. O erro Tipo I, também chamado de Erro de Falsa Aceitação (EFA) é uma estimativa da probabilidade do sistema incorretamente indicar que uma amostra biométrica é verdadeira, quando de fato é falsa. O erro Tipo II, também chamado de Erro de Falsa Rejeição (EFR) é uma estimativa da probabilidade do sistema incorretamente indicar que uma amostra biométrica é falsa, quando de fato é verdadeira. As taxas destes erros são fator crítico para tomarmos conhecimento do desempenho do sistema. A taxa do EFA é chamada de *False Acceptance Rate* (FAR) ou *False Match Rate* (FMR). A taxa do EFR é chamada de *False Rejection Rate* (FRR) ou *False Non-Match Rate* (FNMR). Ambas podem ser representadas através de curvas em gráfico de acordo com as equações (3.1) e (3.2).

Dados *imp* como sendo o conjunto de amostras biométricas provindas de usuários impostores, *leg* como sendo o conjunto de amostras biométricas provindas de usuários legítimos, *ims(imp)* como sendo o conjunto de valores obtidos pelos resultados das comparações entre os *templates* da base de dados e *imp*, e *gms(leg)* como sendo os valores obtidos pelos resultados das comparações entre os *template* da base de dados e *leg* , então para um dado valor de limiar *t*,

$$FAR(t) = \frac{card\{ims(imp) \mid ims(imp) \geq t\}}{card\{ims(imp)\}} \tag{3.1}$$

$$FRR(t) = \frac{card\{gms(leg) \mid gms(leg) < t\}}{card\{gms(leg)\}} \tag{3.2}$$

Variando o valor de limiar *t* nas equações (3.1) e (3.2), obtemos as curvas de FAR e FRR exibidas na figura 3.2. Nas curvas de FAR e FRR da figura 3.2, podemos notar três pontos, rotulados como ZeroFRR, ZeroFAR e EER. Cada um deles é definido como se segue:

- ZeroFRR – é o menor valor de FAR(*t*) quando FRR(*t*) é igual a zero. O valor de *t* é representado na figura 3.2 por t_a . Indica a probabilidade de incorretamente o sistema biométrico aceitar amostras biométricas impostoras como sendo genuínas, quando todas as quando todas as amostras biométricas genuínas são detectadas.

- ZeroFAR – é o menor valor de FRR(*t*) quando FAR(*t*) é igual a zero. O valor de *t* é representado na figura 3.2 por t_b . Indica a probabilidade de incorretamente o sistema biométrico aceitar amostras biométricas legítimas como sendo impostoras, quando todas as amostras biométricas impostoras são detectadas.

- EER – é o ponto no qual os valores de FAR(*t*) e FRR(*t*) são iguais. O valor de *t* é representado na figura 3.2 por t_c . Este ponto especifica a separabilidade que o sistema biométrico oferece entre amostras biométricas impostoras e genuínas.

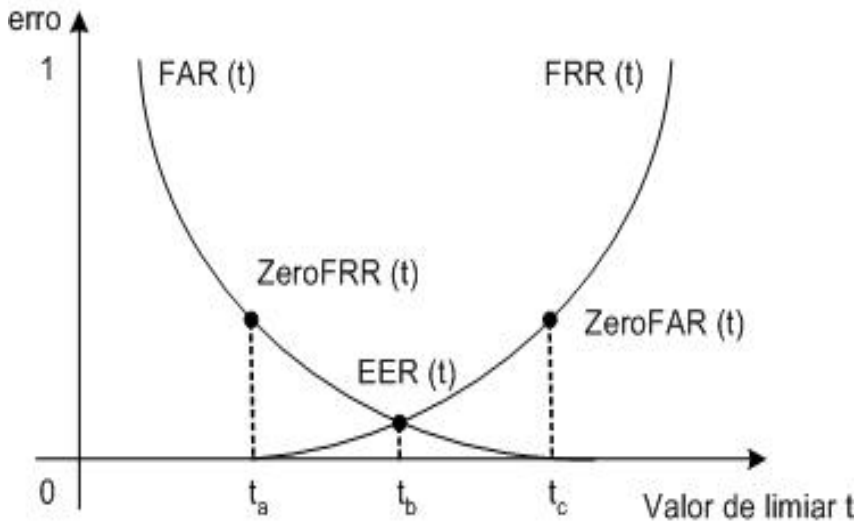


Figura 3.2: Um exemplo de curva de FAR X FRR.

Na prática, um sistema biométrico apresenta um gráfico semelhante ao da figura 3.2, no qual as curvas de FAR e FRR se cruzam no ponto de EER. Por outro lado, numa situação ideal o valor de EER é igual a zero, o que significa que as curvas de FAR e FRR estão completamente separadas, ou seja, FAR(t) = FRR(t) = 0. Se um sistema biométrico é configurado para operar num valor de limiar nesta situação (EER = 0), como conseqüência não haverá nenhum caso de rejeição de usuários legítimos ou de aceitação de usuários impostores. Este é um objetivo que todos os pesquisadores e desenvolvedores que trabalham com sistemas biométricos almejam alcançar.

3.3 Padronizações Biométricas

A existência de padronizações biométricas atinge uma importância fundamental na medida em que existe uma necessidade de uma uniformização relacionada, por exemplo, com os seguintes aspectos [39]:

- Manutenção da integridade e autenticidade dos dados biométricos circulantes, processados e armazenados;

- Gerenciamento dos dados biométricos durante o ciclo de vida do sistema biométrico;

- A aplicação prática do sistema biométrico;

- Controle de acesso às informações armazenadas pelo sistema biométrico;

- Encapsulamento dos dados biométricos;

- Implementação de técnicas de segurança para o armazenamento e transmissão dos dados biométricos;

- Implantação de políticas de segurança que considerem a privacidade e a propriedade das informações (biométricas ou não) de cada indivíduo cadastrado no sistema biométrico.

Como as tecnologias biométricas são novas, as padronizações não são unificadas e cada um dos centros de padronização em tecnologias biométricas possui sua visão e estudos particulares. Alguns destes centros de padronização mais importantes são [40][41]:

- *The National Bureau of Standards:* publicou um guia, "*Guidelines on Evaluation of Techniques for Automated Personal Identification*", que fornece critérios de como escolher um sistema de identificação pessoal;

- União Européia: A União Européia procura nesses últimos anos abordar questões legais envolvendo biometria, como por exemplo, certificações de produtos biométricos, segurança nos dados transacionados ou armazenados, padronizações apropriadas a cada tipo de aplicação biométrica. A *European Commission* financia projetos para o incentivo de desenvolver tecnologias biométricas, como os projetos CASCADE e BIOTEST. Uma padronização européia para controle de acesso (-EM 50133-1) está em desenvolvimento, e um de seus principais apontamentos diz que tecnologias biométricas para controle de acesso devem ter uma FAR de 0.001% e uma FRR de 1%;

- *The Association for Biometrics* (AFB): fundada na Inglaterra em 1993, vem desenvolvendo um glossário de termos envolvendo tecnologias biométricas, que foi plenamente aceito pelo *British Standards Institute*. Seu principal objetivo é a educação popular em tecnologias e produtos biométricos.

- *The Biometry Industry Standards Association*: localizado nos Estados Unidos, tem por objetivo estabelecer um ambiente de testes para tecnologias biométricas independente.

- *The Biometric Consortium*: criado em 1992 pelo Departamento de Defesa dos Estados Unidos, tem por objetivo a criação de padrões de teste para tecnologias biométricas em benefício de todas as agências do governo norte-americano. Além disso, estuda as tecnologias biométricas com o objetivo de melhorar seus desempenhos, promove troca de informações entre o governo, indústria e universidades, sugere aspectos éticos, legais,

de desempenho e segurança de tecnologias biométricas e auxilia agências governamentais na seleção, compra e operação de dispositivos biométricos.

- *Federal Bureau of Investigation* (FBI): desenvolve padrões para a troca de informações entre sistemas biométricos. Um algoritmo chamado *Wavelet Scalar Quantization* (WSQ) desenvolvido pelo FBI, NIST e *Los Alamos Laboratory* tornou-se um padrão para a compressão de imagens de impressão digital.

- Outras Centros são: *The Security Industry Association*, *U.S. Army's Facial Recognition Technology Program*, *The Asr Group*, *The International Civil Aviation Organization, Swiss Association for Artificial Intelligence* (SGAICO), e *International Association for Pattern Recognition* (IAPR).

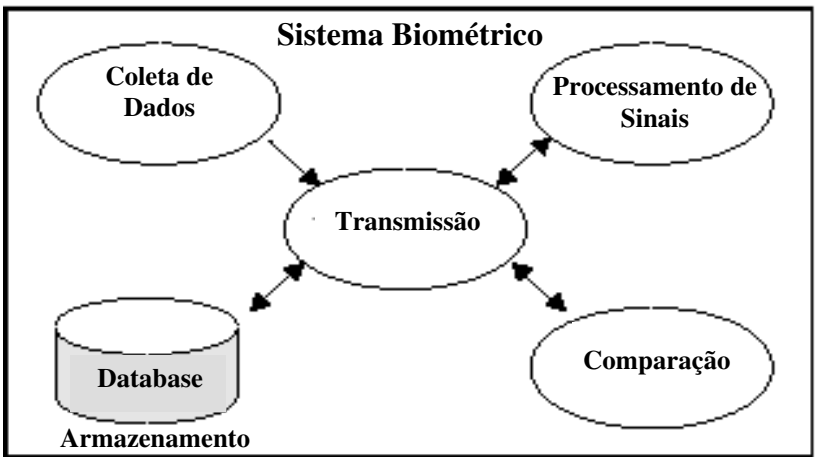


Figura 3.3: Composição de um Sistema Biométrico

3.4 Composição de Sistemas Biométricos

A figura 3.3 mostra o modelo geral de um sistema biométrico dividido em subsistemas. Cada um dos subsistemas apresentados na figura 3.3 é definido a seguir [39]:

- Subsistema de Coleta de Dados – contém o dispositivo ou sensor que capta como entrada para o sistema biométrico a amostra biométrica de um usuário e converte-a em uma forma adequada (sinal eletrônico) para a utilização pelo restante do sistema. O

desempenho de um dispositivo ou sensor de coleta de dados é afetado pela qualidade da amostra fornecida e pelo desempenho do próprio sensor ou dispositivo de coleta.

- Subsistema de Transmissão – é responsável pela comunicação entre os demais subsistemas. A conectividade pode ser ponto-a-ponto ou difusão, e não necessariamente ele é monolítico (composto de um único tipo de meio de transmissão). É responsabilidade deste subsistema manter a autenticidade e integridade dos dados transmitidos;

- Subsistema de Processamento de Sinais / Extração de Características – é responsável por receber a amostra biométrica fornecida pelo subsistema de coleta de dados e de convertê-la em uma forma adequada para o processamento pelo subsistema de comparação. Este subsistema pode aplicar uma análise da qualidade da amostra fornecida para determinar se ela pode ser passada adiante, ou aplicar uma filtragem para remover ruídos ou outras informações que podem afetar o julgamento do subsistema de comparação, ou ainda normalizar o sinal. Estes são alguns dos tipos de processamento aplicados por este subsistema, cujos métodos variam de desenvolvedor para desenvolvedor. Uma vez que a amostra tenha sido processada, este subsistema extrai características da amostra para o processamento pelo subsistema de comparação, mas este passo não é obrigatório;

- Subsistema de Comparação – este sistema faz a comparação da amostra biométrica apresentada com um *template* da base de dados. Ele verifica o quanto ambas são similares e após isto toma uma decisão, que identifica se a amostra apresentada pertence ou não ao proprietário do *template* selecionado da base de dados. Para tomar esta decisão, um valor de limiar deve ser estabelecido neste subsistema.

- Subsistema de Armazenamento – este subsistema mantém os *templates* dos usuários cadastrados no sistema biométrico. Ele disponibiliza a adição, deleção ou atualização dos *templates* cadastrados. Ele pode conter para um único usuário um único *template* ou vários deles, dependendo da forma como o sistema foi desenvolvido. Os dados armazenados

neste subsistema sempre devem incluir o *template*, mas outras informações também podem ser incluídas.

Em alguns sistemas biométricos, o subsistema de processamento de sinais / extração de características é uma passagem, não havendo qualquer tipo de processamento da amostra coletada ou extração de características, mas todos os outros subsistemas são necessários [39]. Nestes casos, a própria amostra coletada pelo Subsistema de Coleta será utilizada para comparação no Subsistema de Comparação.

Este modelo de divisão de sistema biométrico em subsistemas será utilizado para adaptar o modelo hierárquico ISO/IEC 9126 para os conceitos envolvendo produtos de *software* biométricos.

3.5 Métodos Biométricos de Autenticação Pessoal

A figura 3.4 apresenta um diagrama de blocos com a tipologia de métodos de autenticação associados a sistemas baseados em características biométricas. Nas próximas subseções, descreveremos estes métodos de forma mais detalhada, assim como mostraremos, em uma tabela, um quadro comparativo entre as tecnologias biométricas de acordo com a figura 3.4.

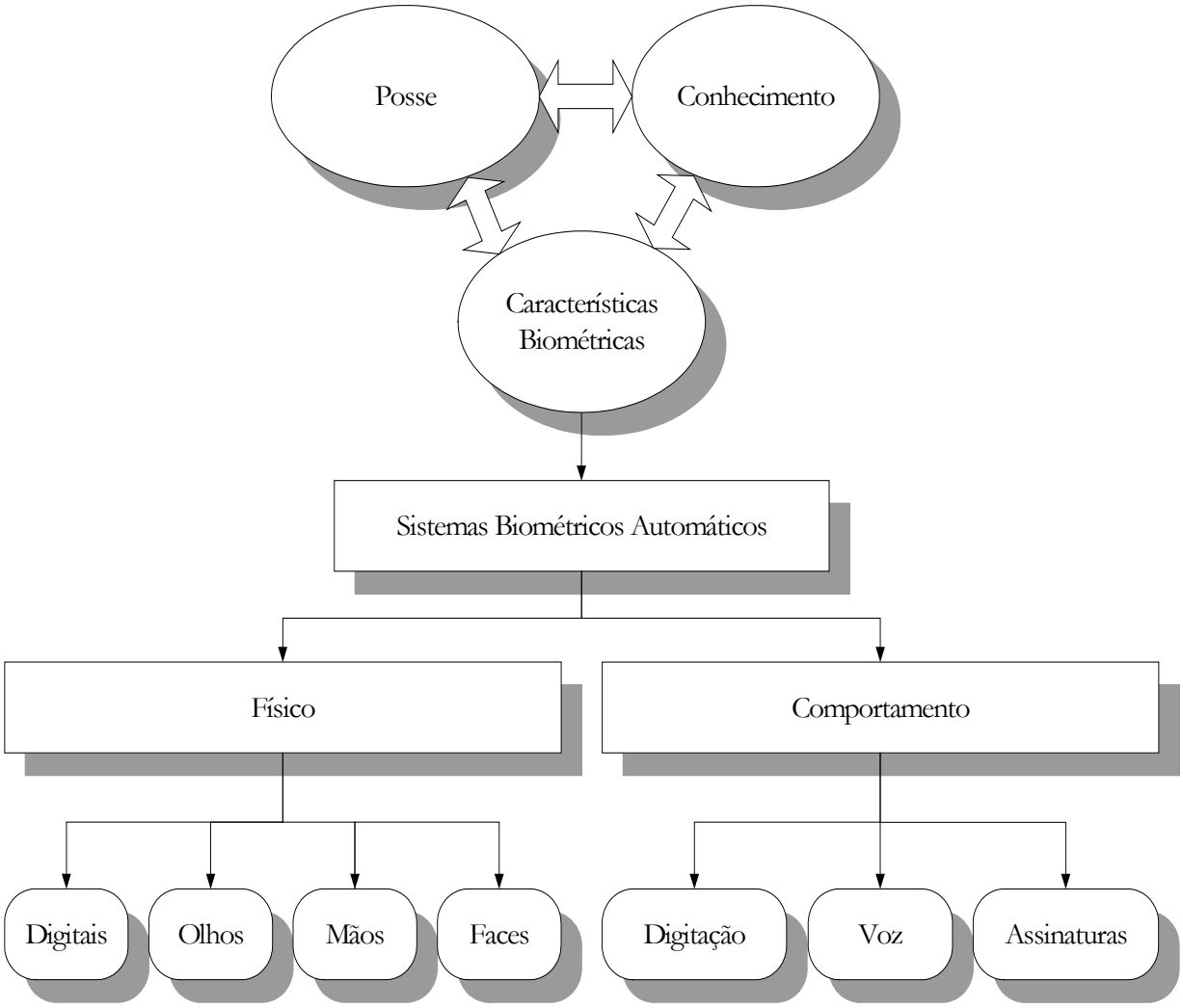


Figura 3.4: Tipologia de métodos de autenticação associados a sistemas baseados em características biométricas.

3.5.1 Impressões Digitais

A estabilidade e unicidade das impressões digitais já estão mais que comprovadas, pois, após muitos estudos [42][43][44], estima-se que a chance de duas pessoas, incluindo gêmeos, tenham a mesma impressão digital é menor do que uma em um bilhão. Além disso, uma impressão digital não muda com o passar do tempo e com as modificações corporais que surgem com o crescimento de uma pessoa [38]. A extração de características sobre impressões digitais baseia-se 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 [45]. Outras

pesquisas contam o número de vales e sulcos que existem entre estes pontos [46]. Dependendo do esquema de autenticação escolhido e do grau de segurança do sistema, o tamanho da base de dados que contém as informações sobre a impressão digital varia de algumas centenas até milhares de bytes.

Sistemas baseados em impressão digital podem ser utilizados em favor da justiça e em outras aplicações. O *Federal Bureau of Investigation* (FBI) desenvolve uma rede de comunicação de dados nacional de forma a realizar autenticação pessoal utilizando impressões digitais. Esta rede irá fornecer acesso rápido para um sistema integrado chamado *Automated Fingerprint Identification System* (AFIS) [47] e aumentará a velocidade de identificação de criminosos.

Uma pesquisa concluiu que os clientes de bancos britânicos apoiavam o uso de impressões digitais em conjunto com cartões para evitar fraudes, e que tecnologias baseadas em impressões digitais são seguras, rápidas, confiáveis e fáceis de utilizar [38]. Porém, pessoas que não possuem dedos não podem utilizar este tipo de tecnologia. Pessoas com dedos seriamente feridos ou machucados por acidentes podem ter problema ao tentarem autenticar-se nesses sistemas. Em ambientes em que é necessário o uso de luvas, esse método de autenticação não seria apropriado [38].

Alguns dispositivos ou sensores biométricos que coletam amostras de digitais apresentam problemas quanto a fraudes. Em [48] é mostrado que um sensor pode ser fraudado bastando bafejar sobre ele. Após utilizá-lo uma quantidade de vezes, rastros da digital ficam impregnados no sensor. Ao bafejar sobre o sensor, estes rastros são reativados e o sensor autentica erroneamente o indivíduo. Esta fraude também pode ser reproduzida utilizando-se um saco plástico transparente cheio de água, posicionando-o sobre o sensor, ou utilizando grafite em pó em conjunto com uma película adesiva fixada sobre o sensor. De uma forma mais sofisticada, utilizando um kit utilizado por departamentos de investigações criminais, por exemplo, é possível extrair impressões digitais latentes de indivíduos os quais deseja-se fraudar.

Além disso, outro tipo de fraude envolve a utilização de digitais "artificiais". Em [49] é mostrado que é possível fabricar uma digital "artificial" fazendo uso de um procedimento simples e de baixo custo. Inicialmente, derrete-se a cera de uma vela e depois se pressiona o dedo que contêm as impressões digitais as quais deseja-se fraudar sobre o material derretido. Por fim, basta preencher a cavidade formada na cera derretida com silicone para obter a digital "artificial". Uma solução para evitar este tipo de fraude é que os sensores e dispositivos de captura de amostras

biométricas sejam capazes de identificar se a amostra da impressão digital fornecida pertence a uma pessoa viva [49].

3.5.2 Olhos

Oftalmologistas originalmente propuseram que a íris pode ser utilizada como uma espécie de digital ótica para autenticação pessoal [50]. A principal vantagem da captura de padrão da íris sobre a captura do padrão dos vasos sangüíneos do fundo do olho (retina) é que não é necessário que o olho do indivíduo esteja focalizado e imóvel em uma determinada posição. Ainda mais, segundo [51], a imagem da íris pode ser obtida pelo dispositivo de captura até a um metro de distância. No caso da varredura de retina, ela é realizada direcionando-se uma luz infravermelha de baixa intensidade na pupila e na parte posterior do olho. O padrão da retina é refletido de volta para a câmera que está capturando o padrão. O método de autenticação via retina é um dos melhores métodos biométricos existentes, com taxas de erros muito baixas (FAR menor que 0.0001% e FRR entre 2% e 3%), base de dados de referências pequenas e processos rápidos de confirmação de identidade [52].

Atualmente, o que mais dificulta a difusão desse tipo de tecnologia continua sendo a resistência dos usuários, isto é, convencer a pessoa que vai fazer uso dessa técnica para a autenticação da sua identidade de que a luz infravermelha que incidirá sobre seu olho não lhe irá fazer mal [52]. Uma pesquisa entre a população britânica mostrou que o dispositivo que capta amostras biométricas de íris é considerado o de menor aceitabilidade pública, e entre a população italiana ele é inaceitável. Além disso, pessoas cegas ou com danos severos na superfície do olho não podem fazer uso deste tipo de tecnologia [38]. Médicos também estão mudando sua opinião quanto à estabilidade desse tipo de tecnologia: variações críticas foram apresentadas em caso de disfunções orgânicas e doenças [53].

Fraudes nesses sistemas envolvem tentativas de utilizar imagens impressas ou fotografias de um usuário do sistema, onde os olhos estejam em evidência. Outra tentativa envolve a utilização dessas mesmas imagens impressas ou fotografias, mas com um corte ao redor da pupila: neste ponto o fraudador põe o buraco do corte em frente à sua pupila. Desta forma, ele contorna a tentativa do dispositivo ou sensor de reconhecer uma imagem artificial: o dispositivo ou sensor emite feixes de luz que causam variações de abertura/fechamento da pupila. Outra forma de fraudar o sistema envolve a utilização de olhos "artificiais". Olhos "artificiais" são próteses de

biocerâmica ou polietileno criadas a partir do conhecimento do padrão do olho de um indivíduo [48].

3.5.3 Mãos

Um sistema de autenticação via geometria da mão baseia-se em medidas das dimensões de partes das mãos, tais como o comprimento do dedo, sua largura e área, contorno externo, linhas internas e veias. A classificação utilizando estes parâmetros leva em conta a forte correlação que existe entre estas diferentes medidas. Os primeiros sistemas baseados nestas características datam de 1960, sendo que as medidas utilizadas eram apenas o comprimento de quatro dedos [54][55]. Esse tipo de tecnologia biométrica é muito utilizada para o controle de acesso a áreas restritas.

Sistemas baseados nesse tipo de tecnologia são rápidos nos procedimentos de autenticação e o tamanho dos *templates* requerem pouco espaço de armazenamento na base de dados. Estes sistemas apresentam problemas de autenticação quando um usuário rotaciona a mão sobre o mecanismo de captação da amostra. Também apresentarão problemas de autenticação com relação a pessoas que usam anéis nos dedos, apresentam cicatrizes deformatórias ou inchaços nos dedos. Sujeira também pode ocasionar problemas de autenticação pessoal [38].

Sistemas baseados nesse tipo de tecnologia são encontrados em ambientes fechados e de temperatura controlada. A influência da luz solar incidindo diretamente sobre o dispositivo ou sensor pode influenciar no desenho do contorno da mão.

Em [38], o *Sandia National Laboratories* realizou uma pesquisa que identificou esta tecnologia biométrica como a favorita entre os usuários quando comparada com outras tecnologias biométricas. Apesar de ser bem aceita publicamente em muitos países, esta tecnologia biométrica não é aceita no Japão: devido a aspectos culturais, os japoneses não gostam de colocar suas mãos onde outras pessoas colocaram anteriormente. Pessoas com paralisia ou com Mal de Parkinson não são recomendadas a utilizar este tipo de tecnologia biométrica.

Fraudes em tecnologias biométricas baseadas em mãos são muito semelhantes a utilizadas para fraudar digitais.

3.5.4 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 [56]. Muitos

dos trabalhos nesta área empregam tanto métodos de redes neurais como correlações estatísticas do formato geométrico da face. Nestes métodos tenta-se imitar como os seres humanos reconhecem uma pessoa. As imagens das faces são adquiridas de forma direta pelos equipamentos de vídeo que, hoje em dia, estão financeiramente viáveis. O usuário deve permanecer em frente à câmera com o mínimo de movimento e esperar até o momento que o sistema o autentique. Os atuais sistemas têm dificuldade de conseguir altos níveis de desempenho quando a base de dados aumenta para alguns milhares de indivíduos [57].

Os sistemas atuais não são capazes de identificar um indivíduo quando algumas características faciais são modificadas. O uso de barba, mudança no corte de cabelo, ou mesmo expressões faciais podem causar erros de autenticação. Porém, apesar destes problemas, sistemas baseados em reconhecimento facial têm alta aceitabilidade pública, uma vez que reconhecer uma face é uma das formas naturais aos seres humanos de se reconhecerem [38].

Fraudes nesses sistemas ocorrem com a apresentação de imagens ou fotografias com uma boa qualidade da face. Para burlar mecanismos de captação de amostras artificiais de um usuário, vídeos dos rostos do usuário são utilizados, com pequenas movimentações da sua cabeça [48].

3.5.5 Digitação

A dinâmica da digitação, também chamada de ritmo de digitação, é um método biométrico que está diretamente ligado à área de segurança de computadores. Como o nome indica, este método analisa a maneira como os usuários digitam no teclado. Neste caso, as características extraídas são as seqüências de valores alfanuméricos que o usuário está digitando, assim como o intervalo de tempo entre apertar uma tecla e outra na digitação de uma palavra [58][89].

Nos sistemas que fazem uso 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 deste método, cada vez que um usuário tenta se autenticar no sistema biométrico, é necessário que ele seja capaz de reproduzir com pouca variabilidade os intervalos de tempo do conjunto de teclas que compõem a seqüência alfanumérica da senha dele previamente cadastrada [59][60].

Sistemas baseados nesse tipo de tecnologia biométrica são influenciados negativamente com relação a ferimentos e machucados nas mãos ou fadiga. Pessoas com doenças neurológicas que afetem o ritmo de suas digitações podem ficar incapacitadas de utilizar esse tipo de sistema [38].

Fraudes nesses sistemas abordam o conhecimento sobre o tipo de *string* que um usuário está digitando e/ou o seu ritmo de digitação para esta *string* [59].

3.5.6 Voz

A voz é utilizada em sistemas automáticos de verificação e 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" [61], tais como sotaque, estilo do locutor, entoação, estado emocional, etc., para reconhecer uma pessoa através de sua voz. Como este 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 para o processo de autenticação pessoal [62]. Apesar dos seres humanos utilizarem naturalmente o reconhecimento através da voz para reconhecer outro ser humano, ele é computacionalmente pesado, com baixo desempenho com relação ao tempo de reconhecimento pessoal [38].

Sistemas computacionais baseados em voz não conseguem realizar o reconhecimento quando ocorrem alterações na voz, devido a problemas de rouquidão ou ao estado emocional do usuário, por exemplo. A voz também muda com a idade: mecanismos de adaptação devem ser implementados ou ficará difícil reconhecer um indivíduo pela voz com o passar do tempo. Além disso, é difícil filtrar barulhos provindos do ambiente, que se tornam ruídos junto com a voz coletada. Pessoas que não podem falar (mudos) ou com séria rouquidão não podem utilizar estes sistemas [38].

Fraudes nesses sistemas ocorrem por meio de dublagem ou por gravação da voz de um usuário do sistema. Dublagens, em geral, falham pois as principais características da fala encontram-se em regiões de freqüência da voz que distinguem completamente o usuário legítimo do fraudador. A gravação da voz é a ameaça mais freqüente de fraude sofrida por esses tipos de sistemas.

3.5.7 Assinaturas

Os sistemas de reconhecimento de assinaturas dividem-se em sistemas dinâmicos e sistemas estáticos. Os sistemas de reconhecimento de assinaturas dinâmicos 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), extraem características como a inclinação dos traços da escrita, o número de palavras, a razão entre a altura e o comprimento da assinatura [63].

A chave do sucesso de um sistema de verificação e identificação de assinaturas é encontrar características da assinatura que sejam mais constantes, isto é, que variem pouco durante o processo de cadastramento e autenticação dos seus usuários [64].

Quando o processo de cadastramento em um sistema de autenticação pessoal baseado em assinaturas apresenta uma quantidade excessiva de amostras de assinaturas, ocasiona um descontentamento por parte dos usuários, que para se cadastrar tem de assinar várias vezes [38]. Esses sistemas não podem ser utilizados por pessoas com mal de Parkinson ou nem serão bem aceitos em países em que o índice de analfabetismo é muito alto. Esses sistemas também apresentam dificuldades de autenticação quando existem usuários que modificam sua assinatura radicalmente com o passar do tempo, ou quando eles estão alcoolizados ou drogados [38].

Fraudes nesses sistemas incluem a falsificação aleatória, simples e a habilidosa [65]. A falsificação aleatória caracteriza-se por ter suas formas gráficas e componentes semânticos completamente diferentes da assinatura original. A falsificação simples caracteriza-se por uma fraude do nome da pessoa, mas sem conseguir a imitação da forma gráfica. A falsificação habilidosa ocorre quando o falsificador tem acesso à assinatura original e tenta reproduzir uma cópia fiel. Mais de 90% das falsificações em assinaturas são do tipo simples e aleatória. As mais difíceis de detectar em sistemas baseados nessa tecnologia biométrica são, logicamente, as falsificações habilidosas.

3.5.8 Quadro Comparativo entre Tecnologias Biométricas

A tabela 3.1 apresenta uma comparação entre as tecnologias biométricas apresentadas anteriormente, levando em consideração quatro fatores [66]:

- Robustez: o padrão biométrico deve permanecer estável através de um período de tempo.

- Distinção: identifica o quão único é um padrão biométrico dentre uma população de usuários.

- Evidência: identifica o grau pelo qual uma amostra biométrica identifica e está relacionada a um usuário, com base nos dois fatores anteriores.

- Potencial Biométrico: indica a avaliação qualitativa do potencial de reconhecimento da identidade de um indivíduo baseado nas três características anteriores: robustez, distinção e evidência.

Tabela 3.1: Comparação entre tecnologias biométricas

Característica Biométrica	Robustez	Distinção	Evidência	Potencial Biométrico
Impressões Digitais	Médio-Alto	Alta	Muito Alta	Alto
Olhos	Alto	Muito Alta	Alta	Muito Alta
Mãos	Médio-Alto	Alto	Médio	Médio-Alto
Face	Médio	Alto	Baixo	Médio
Digitação	Desconhecido	Desconhecido	Baixo	Desconhecido
Voz	Médio	Médio-Alto	Médio-Alto	Médio-Alto
Assinaturas	Baixo	Médio	Baixo	Médio-Baixo

As tecnologias biométricas apresentadas na tabela 3.1 são as mais conhecidas e mencionadas na literatura envolvendo reconhecimento pessoal baseado em tecnologias biométricas. A pesquisa bibliográfica teve por objetivo a extração de informações a respeito das características inerentes a cada uma delas. Estas informações foram utilizadas para criar atributos (para o caso da metodologia – capítulo 4) ou parâmetros de qualidade (para o caso da ferramenta BioEVA – capítulo 5), com a finalidade de determinar o grau de qualidade presente em um pacote de *software* biométrico ou em um algoritmo biométrico, respectivamente.

Além disso, das tecnologias biométricas mencionadas neste capítulo, também utilizamos as informações inerentes àquelas baseadas em assinaturas (estáticas) e em dinâmica da digitação para configurar os atributos (metodologia) e os parâmetros de qualidade (ferramenta BioEVA) selecionados em uma avaliação de qualidade. Dessa forma, procuramos aplicar uma avaliação de acordo com as características particulares a cada tipo de tecnologia biométrica. No capítulo 6 veremos, por exemplo, como foram configurados os parâmetros de qualidade da ferramenta BioEVA de acordo com o tipo de tecnologia biométrica do algoritmo que estava sendo avaliado.

CAPÍTULO 4

A METODOLOGIA PARA AVALIAÇÃO DE PACOTES DE SOFTWARE BIOMÉTRICOS

Neste capítulo apresentamos os conceitos envolvidos na metodologia para avaliação de pacotes de software biométricos. Definimos o documento Acordo Comum que torna explícito o processo avaliativo do pacote de software biométrico para avaliadores e avaliados. Apresentamos os Níveis de Rigor utilizados para classificar um pacote de software biométrico e definir o rigor da avaliação. Definimos os atributos, assim como o documento padrão elaborado para abrigar seus conceitos e detalhamentos formais. Apresentamos os QIPEs (Questionários de Identificação de Perfil de Especialista) empregados para avaliar o conhecimento e experiência do avaliador em um atributo, e os PAAs (Processos de Avaliação do Atributo) que são utilizados para especificar o processo de avaliação de um atributo. Mostramos o modelo hierárquico top-down biométrico criado para abrigar e tornar compreensíveis os resultados da avaliação para o desenvolvedor do pacote de software biométrico. Por fim, apresentamos um modelo de relatório que conterá os resultados da avaliação.

4.1 Esquema Completo de Aplicação da Metodologia

A figura 4.1 apresenta o esquema completo de aplicação da metodologia em um pacote de *software* biométrico. O esquema apresentado envolve todos os passos básicos necessários para a avaliação em um pacote de *software* biométrico.

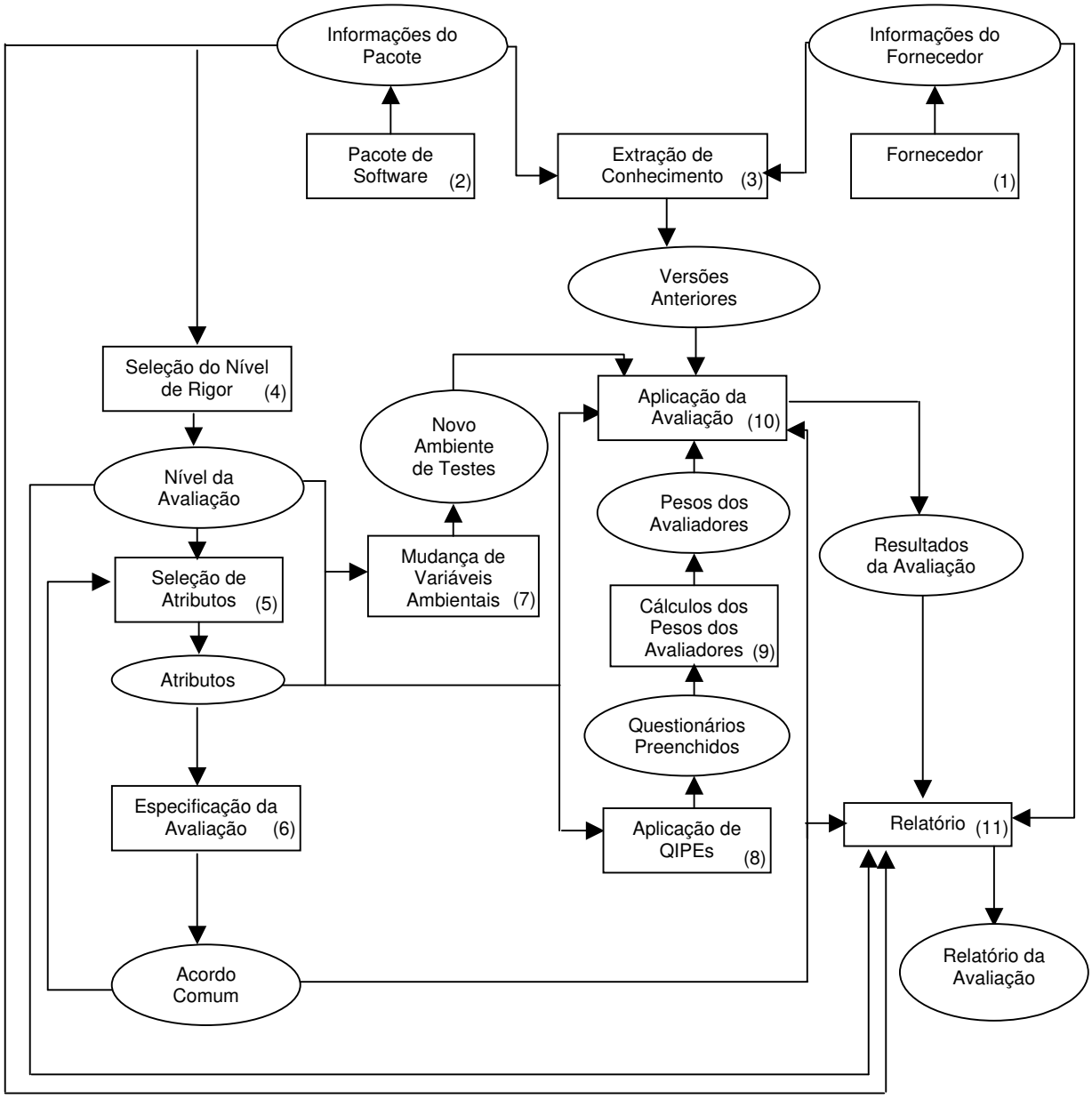


Figura 4.1: Esquema Completo de Aplicação da Metodologia

Os componentes retangulares do esquema indicam tarefas do processo de avaliação, enquanto os elípticos indicam resultados de uma tarefa, que podem ser elementos de entrada para uma outra tarefa. Cada tarefa e seus resultados serão brevemente comentados para um melhor entendimento da metodologia. O número entre parênteses que acompanha um elemento da metodologia em negrito no texto indica a seção onde será explicado com maiores detalhes neste capítulo. Cada tarefa é comentada a seguir:

(1) "Fornecedor": esta tarefa consiste em consultar um desenvolvedor de um pacote de *software* biométrico com o objetivo de extrair informações sobre ele, como sua origem e objetivos, tipos de produto desenvolvidos, existência de alguma avaliação de qualidade passada em seus produtos, processos ou serviços, etc.

(2) "Pacote de *Software*": esta tarefa consiste em extrair informações sobre o pacote de *software* biométrico, tais como a existência de outras versões do produto e se estas versões já passaram por algum tipo de avaliação de qualidade. São extraídas informações sobre os objetivos e aplicações práticas do produto sob os aspectos biométricos e financeiros, de forma a enquadrá-lo em um **nível de rigor** (4.3).

(3) Extração de Conhecimento: esta tarefa recebe as informações das tarefas "Pacote de *Software*" e "Fornecedor" com o objetivo de gerar, caso existam informações inerentes a avaliações com versões anteriores do pacote de *software* biométrico, informações sobre em que partes do produto ou de que forma as avaliações foram aplicadas.

(4) Seleção do Nível de Rigor: esta tarefa recebe as informações da tarefa "Pacote de *Software*" relativas aos objetivos e aplicações práticas do pacote de *software* biométrico e enquadra-o em um nível de rigor.

(5) Mudança de Variáveis Ambientais: esta tarefa compreende criar novos ambientes de testes utilizando novos atributos ou modificando o nível da avaliação. Desta forma, objetivamos fornecer maiores informações sobre os limites e as capacidades do produto para o desenvolvedor.

(6) Especificação da Avaliação: A partir dos atributos selecionados, o objetivo desta tarefa é produzir um documento chamado **Acordo Comum** (4.4), que inclui o nível da avaliação, os atributos, e uma breve descrição dos seus respectivos processos avaliativos, e os pesos dos subsistemas biométricos e documentações, para que o desenvolvedor tome conhecimento de como seu produto será avaliado e possa argumentar sobre o contexto da avaliação.

(7) Seleção de Atributos: esta tarefa consiste em selecionar os **atributos** (4.6) baseado no nível de rigor da avaliação. Os atributos selecionados serão inseridos no Acordo Comum. Se ocorrer alguma alteração nos atributos que foram previamente selecionados como resultado das discussões envolvendo a confecção final do Acordo Comum, esta tarefa será realimentada por estas alterações. Como resultado serão selecionados os atributos a serem utilizados na avaliação.

(8) Aplicação de QIPEs: esta tarefa consiste na aplicação de **Questionários de Identificação de Perfil de Especialista (QIPEs)** (4.5). Estes questionários têm por objetivo extrair o conhecimento e a experiência dos avaliadores relacionados a cada atributo [67]. Os questionários respondidos são o resultado desta tarefa.

(9) Cálculo dos Pesos dos Avaliadores: esta tarefa consiste em, utilizando as respostas dos QIPEs respondidos pelos avaliadores, calcular os pesos que corresponderão aos seus graus de conhecimento e experiência em cada atributo.

(10) Aplicação da Avaliação: esta tarefa consiste em aplicar o processo avaliativo no pacote de *software* biométrico, uma vez que os pesos dos avaliadores tenham sido determinados, os atributos, o nível da avaliação, os ambientes de testes estabelecidos, o Acordo Comum tenha sido firmado e as avaliações de versões anteriores do pacote sejam conhecidas. O resultado da **aplicação da avaliação** (4.7) produz as notas finais relativas a cada atributo avaliado. O **modelo hierárquico *top-down* biométrico** (4.2) será utilizado para abrigar e hierarquizar os valores resultantes da avaliação.

(11) Relatório: esta tarefa consiste em, a partir de um modelo de **relatório padrão** (4.8), gerar um relatório final apresentando os resultados obtidos no processo avaliativo do pacote de *software* biométrico, assim como fornecer recomendações para a melhoria de qualidade do pacote.

Nas próximas seções cada um dos elementos da metodologia para avaliação de pacotes de *software* biométrico será explicado com maiores detalhes.

4.2 O Modelo Hierárquico *Top-Down* Biométrico

Conforme foi apresentado no capítulo 2 (2.4.2), a norma internacional ISO/IEC 9126 estabelece um modelo hierárquico *top-down* baseado em características, subcaracterísticas e atributos. Este modelo apresenta dificuldades quanto à sua aplicabilidade na avaliação prática de produtos de *software* [32], visto que as características de qualidade por ele definidas não são diretamente mensuráveis. O modelo não determina claramente quais partes de um produto de *software* podem apresentar ou não deficiências.

Quando avaliamos um produto de *software*, o que desejamos observar na verdade é onde estão os seus problemas e as suas deficiências para que, com base neles, possamos melhorar a qualidade do produto, corrigindo o que está errado e complementando o que está faltando. Avaliar sob o aspecto das definições subjetivas das características do modelo hierárquico ISO/IEC 9126 não dará informações claras sob em que aspectos reais o produto está comprometido em sua qualidade.

Dentro do contexto apresentado, para corrigir a deficiência apresentada pelo modelo hierárquico ISO/IEC 9126, fizemos uso da definição da divisão de um sistema biométrico em subsistemas, conforme apresentado no capítulo 3 (3.4). Esta definição tornou-se um padrão norte-americano e é adotado por órgãos governamentais ligados com avaliação de tecnologias biométricas: o *American National Standard X9.84-2001 Biometric Information Management and Security*. Fazendo uso desta desta definição, procuramos readaptar o modelo hierárquico ISO/IEC 9126 à realidade das definições envolvendo os produtos de *software* biométricos atuais. A figura 4.2 mostra o modelo hierárquico *top-down* baseado na definição da divisão de um sistema biométrico em subsistemas.

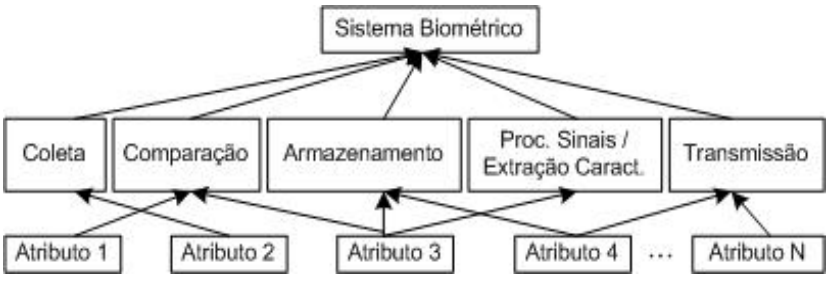


Figura 4.2: Modelo Hierárquico *Top-Down* baseado na Subdivisão de Sistemas Biométricos

Para que pudéssemos ter uma visão de um produto de *software* biométrico como um produto comercial, fizemos uso da norma ISO/IEC 12119 conforme apresentada no capítulo 2 (2.4.3) para contextualizá-lo como um pacote de *software* biométrico. Assim, um pacote de *software* biométrico envolve o sistema biométrico mais as documentações que o acompanham. As documentações devem obedecer aos requisitos da norma conforme apresentado no capítulo 2 (2.4.3). A figura 4.3 mostra o modelo hierárquico *top-down* baseado nas documentações presentes nos requisitos da norma ISO/IEC 12119. Por fim, a figura 4.4 mostra a abordagem completa do modelo hierárquico *top-down* baseado na definição de pacotes de *software* biométricos apresentada, complementado com os modelos mostrados nas figuras 4.2 e 4.3.

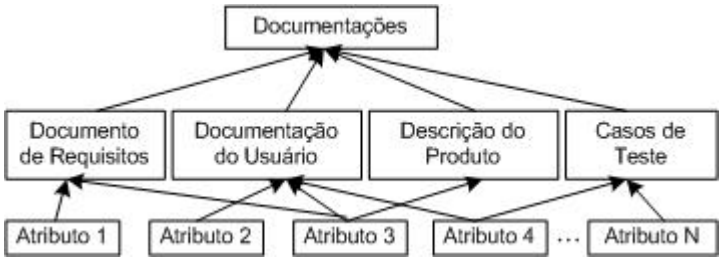


Figura 4.3: Modelo Hierárquico *Top-Down* baseado em Documentações (ISO/IEC 12119)

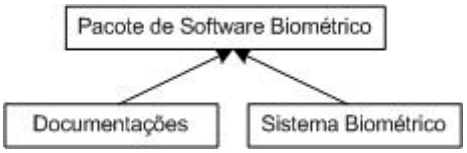


Figura 4.4: Modelo Hierárquico *Top-Down* Biométrico

4.3 Nível de Rigor

Uma avaliação é orientada por nível devido a duas motivações principais: flexibilidade e rigor na avaliação [26]. Uma avaliação é flexível quando permite classificar um produto em um determinado nível de acordo com suas características particulares. O rigor na avaliação implica que quanto maior for o nível associado ao produto mais rigorosa será a aplicação da avaliação, e, conseqüentemente, maior será o grau de confiança nos resultados produzidos pela avaliação do produto.

Tabela 4.1: Níveis de Rigor utilizados na Metodologia

		NÍVEIS DE RIGOR				
		E	**D**	**C**	**B**	**A**
Aspectos Financeiros	**Ambiental**	Nenhum risco	Pequenos danos ao Meio	Danos Significativos ao Meio, mas recuperáveis	Danos Graves ao Meio, mas recuperáveis	Danos Irrecuperáveis ao Meio
	Usuário	Nenhum Risco	Risco Mínimo	Poucas Pessoas Afetadas	Ameaça para Vidas Humanas	Muitas Pessoas Mortas
	Econômico	Nenhum Prejuízo	Pequeno Prejuízo	Prejuízo Significativo	Prejuízo Grave	Desastre Financeiro
	Aplicação Prática	Protótipos	Entretenimento, Uso Doméstico	Controle de Incêndio, Controle de Processos	Sistemas Financeiros e Hospitalares	Controle de Tráfego Aéreo e Sistemas Nucleares
Aspectos Biométricos	**Unicidade**	1:50 – 1:100	1:500 – 1:1000	1:5000 – 1:10000	1:50000 – 1:100000	1:500000 – 1:1000000
	Identificação da Pessoa Viva	Não	Não	Sim	Sim	Sim
	Segurança da Informação	C1	C1/C2	B1	B2/B3	B3
	Influências Ambientais /Temporais	Não	Não	Somente Influências Temporais	Sim	Sim

A tabela 4.1 mostra os níveis de rigor adotados e suas exigências orientadas por nível para classificar um pacote de *software* biométrico. O nível E é o mais baixo e o nível A é o mais alto. Os níveis de rigor são analisados sob dois aspectos: o aspecto financeiro e o aspecto biométrico. Os temas abordados sob o aspecto financeiro são apresentados em [68], que não inclui o nível E. Nós criamos o nível E para abrigar produtos do tipo protótipos. Os temas abordados sob o aspecto financeiro são definidos abaixo [68]:

1) Ambiental: caso o sistema perca o controle ou falhe sobre as atividades as quais automatiza e/ou controla, define como esta situação afeta o ambiente a sua volta.

2) Usuário: caso o sistema perca o controle ou falhe sobre as atividades as quais automatiza e/ou controla, define como esta situação afeta a integridade física e a saúde do usuário.

3) Econômico: caso o sistema perca o controle ou falhe sobre as atividades as quais automatiza e/ou controla, define como esta situação afeta financeiramente o seu proprietário.

4) Aplicação Prática: define exemplos de tipos de aplicações práticas onde o sistema pode ser aplicado para mensurar sua importância e abrangência.

Os temas abordados sob o aspecto biométrico envolvem definições que devem ser consideradas na caracterização de qualquer pacote de *software* biométrico atual, que são:

1) Unicidade: define quão único é um padrão biométrico dentro de uma população de usuários do sistema [66].

2) Identificação de Pessoa Viva: define a habilidade do sistema biométrico de identificar se as amostras biométricas pertencem ou não a uma pessoa viva [66].

3) Segurança da Informação: define o nível de segurança da informação transmitida e armazenada em um sistema. Esta classificação é estabelecida de acordo com a norma DoD5200-28 – *Trusted Computer Security Evaluation* – TCSEC. Esta norma define uma política de segurança da informação circulante e armazenada no sistema, considerando todos os seus elementos componentes. O nível de segurança de um sistema é dividido em quatro classes de segurança: D, C, B e A. Cada uma destas classes é dividida em três subníveis, como, por exemplo, a classe A é dividida em A1, A2 e A3. Contudo, as classes de maior relevância e mais utilizadas como referências são os níveis D1, C1, C2, B1, B2, B3 e A1 [69]. Nós removemos os níveis D1 e A1. O nível D1 representa ausência de segurança e não é sancionado. O nível A1 necessita uma análise do projeto, o que envolveria as fases de processo de desenvolvimento do sistema, o que está fora do escopo dessa dissertação. Os níveis restantes (C1, C2, B1, B2, B3) apresentam uma definição suficiente para garantir a abrangência das principais ameaças e ataques a sistemas biométricos apresentadas em [38].

4) Influências Ambientais/Temporais: Influências ambientais são definidas como os diferentes efeitos ocasionados a sistemas biométricos por fatores ambientais, como umidade, temperatura, etc [66]. Influências temporais são definidas como as transformações que as características biométricas sofrem com o passar do tempo [70].

4.4 Acordo Comum

O Acordo Comum compreende uma documentação definida a partir de uma discussão entre avaliadores e avaliados, objetivando transparecer, em linhas gerais, todo o processo de avaliação de um pacote de *software* biométrico. Neste documento estão contidos todos os procedimentos, padronizações, normas e/ou técnicas que serão utilizadas para avaliar o pacote, incluindo os atributos relacionados. Desta forma, permitimos ao desenvolvedor do pacote de *software* biométrico argumentar com relação ao processo de avaliação que será empregado. Como resultado, temos dois objetivos a alcançar com a aplicação deste acordo:

1) O desenvolvedor torna-se ciente do que será feito no transcorrer da avaliação do seu produto;

2) Como o próprio nome indica, é um acordo: uma vez que a avaliação seja aplicada conforme especificado no documento, o desenvolvedor receberá os resultados e as recomendações produzidas.

O Acordo Comum segue o modelo de documento apresentado na figura 4.5. Os tópicos apresentados na figura 4.5 abrangem as seguintes informações:

1. Informações do Pacote de *Software* Biométrico: deve ser identificado o nome e a versão do produto. Uma breve descrição sobre o pacote de *software* deve ser feita, incluindo em que linguagem de programação ou ambiente de programação foi desenvolvido, o(s) tipo(s) de característica(s) biométrica(s) utilizada(s), o meio de armazenamento (cartão, banco de dados, etc.), o coletor de amostras, etc.

2. Informações do Fornecedor: deve ser identificado o nome do fornecedor e as informações adicionais sobre ele, como endereço, telefone, CNPJ ou CPF, etc. Devem ser identificados os propósitos e objetivos do fornecedor de uma forma geral.

3. Atributos Utilizados: Devem ser identificados os atributos a serem utilizados na avaliação. Para cada atributo, devem ser identificados:

   3.1 Atributo – identifica o nome do atributo acompanhado por uma breve definição;
   3.2 Ambiente de Testes – define padronizações, normas, técnicas, métodos e/ou ferramentas que serão utilizadas para avaliar um atributo e como eles serão empregados;
   3.3 Modificações Empregadas – com base nas argumentações do fornecedor, este tópico define as modificações no processo de avaliação do atributo (PAA) que foram acordadas por ambas as partes.

4. Nível de Rigor – define o nível de rigor da avaliação. O nível de rigor deve ser acompanhado por uma justificativa sobre o enquadramento do pacote de *software* biométrico em um determinado nível. Caso haja alguma mudança no nível de rigor, a justificativa deve conter também o motivo pelo qual ocorreu a mudança e o valor do nível anterior à mudança.

5. Pesos dos Subsistemas Biométricos e Documentações – define os pesos dos subsistemas biométricos e documentações, inicialmente fornecidos de acordo com as características, funcionalidades e importância assumidas por cada um deles no pacote. Os pesos em cada subsistema e em cada documentação devem ser acompanhados por uma justificativa sobre o motivo da atribuição do peso ao subsistema ou à documentação. Caso haja alguma mudança no valor do peso, a justificativa deve conter também o motivo pelo qual ocorreu a mudança e o valor do peso anterior à mudança.

6. Informações sobre Versões Anteriores – define para o fornecedor, conjuntamente com uma breve justificativa, em que partes do produto serão feitas uma checagem de

atualização ou não. Assim evitamos avaliar o produto completamente, em caso de uma nova versão do produto. Somente as novas funcionalidades e atualizações serão avaliadas, enquanto as partes do produto da versão anterior que não foram modificadas serão checadas de forma a garantir que estas novas funcionalidades e atualizações não interferem negativamente nas partes não-modificadas do pacote.

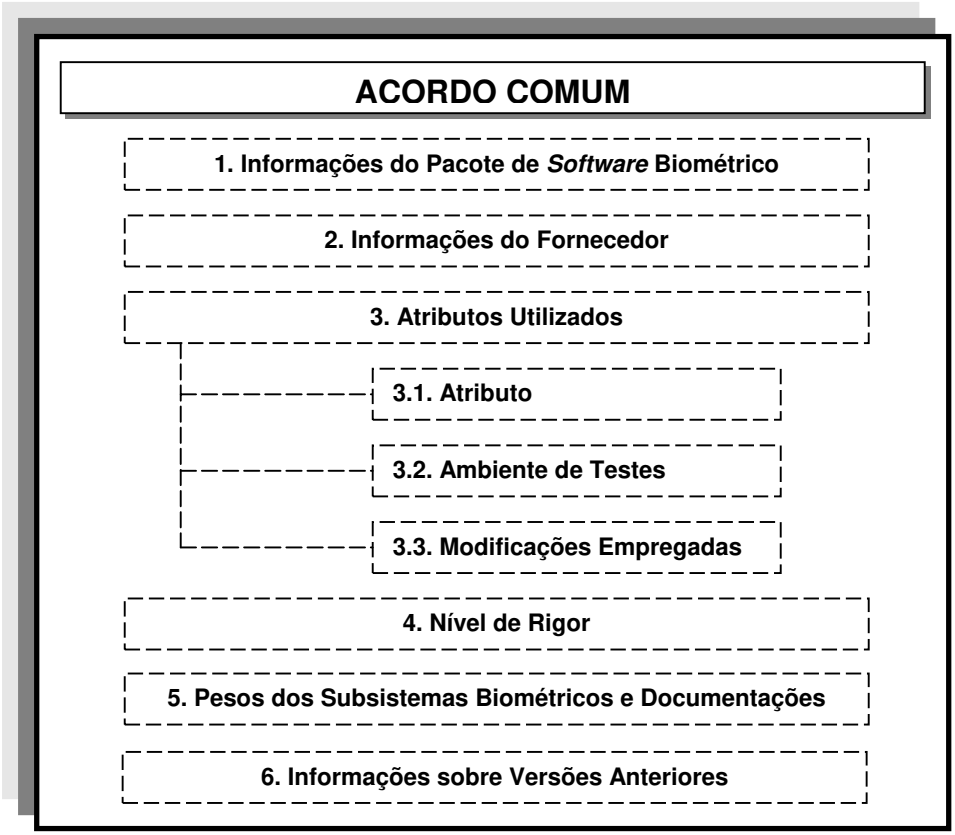


Figura 4.5: Modelo de Documento envolvendo o Acordo Comum

4.5 Questionário de Identificação de Perfil de Especialista (QIPE)

O Questionário de Identificação de Perfil de Especialista tem por objetivo extrair o conhecimento e a experiência dos avaliadores relacionados a um atributo [67]. Assim, utilizando o QIPE, nós mensuramos o conhecimento e a experiência de um avaliador sobre um determinado atributo através de um peso, resultado das suas respostas no respectivo questionário. Um exemplo de um QIPE para um atributo pode ser encontrado no anexo II desta dissertação.

Um questionário é dividido em várias questões. As questões foram classificadas em dois tipos:

1) Exclusivas: são as questões que permitem somente a escolha de uma alternativa como resposta.

2) Cumulativas: são as questões que permitem a escolha de mais de uma alternativa como resposta.

Cada atributo tem um questionário (QIPE) a ele relacionado, compondo a sua documentação formal conforme será descrito na seção Atributos (4.6) desse capítulo. Cada questão de um QIPE é composta por alternativas. Cada alternativa tem um valor inteiro associado, que determina seu peso em relação às demais alternativas de uma mesma questão. Se a questão é cumulativa, a soma de todos os pesos de suas alternativas é igual a um valor equivalente a 100%. Se a questão é exclusiva, o valor da alternativa selecionada será equivalente ao valor percentual calculado sobre o maior valor dentre as alternativas. Assim, o valor percentual resultante das questões respondidas por um avaliador determinar o seu grau de conhecimento e/ou experiência em tal questão.

A figura 4.6 ilustra o esquema apresentado para uma questão com alternativas exclusivas (a) e para uma questão com alternativas cumulativas (b). No caso da Questão A, somente uma alternativa pode ser selecionada. Neste caso, a alternativa 1 foi escolhida pelo avaliador. O valor percentual atingido nesta questão será igual a $(Valor1 \times 100) \div Valor4$, sendo *Valor1* o valor do peso atribuído à alternativa 1 e *Valor4* o valor do peso atribuído à alternativa 4, sendo esta a de maior peso dentre as alternativas da Questão A. No caso da Questão B, mais de uma alternativa pode ser selecionada. Neste caso, as alternativas 1 e 3 foram escolhidas pelo avaliador. O valor percentual atingido nesta questão será igual a $((Valor1 + Valor3) \times 100) \div \left(\sum_{N=1}^{4} ValorN \right)$, sendo *Valor1* o valor do peso atribuído à alternativa 1, *Valor3* o valor do peso atribuído à alternativa 3 e *ValorN* o valor do peso atribuído à alternativa *N*, com *N* variando de 1 a 4.

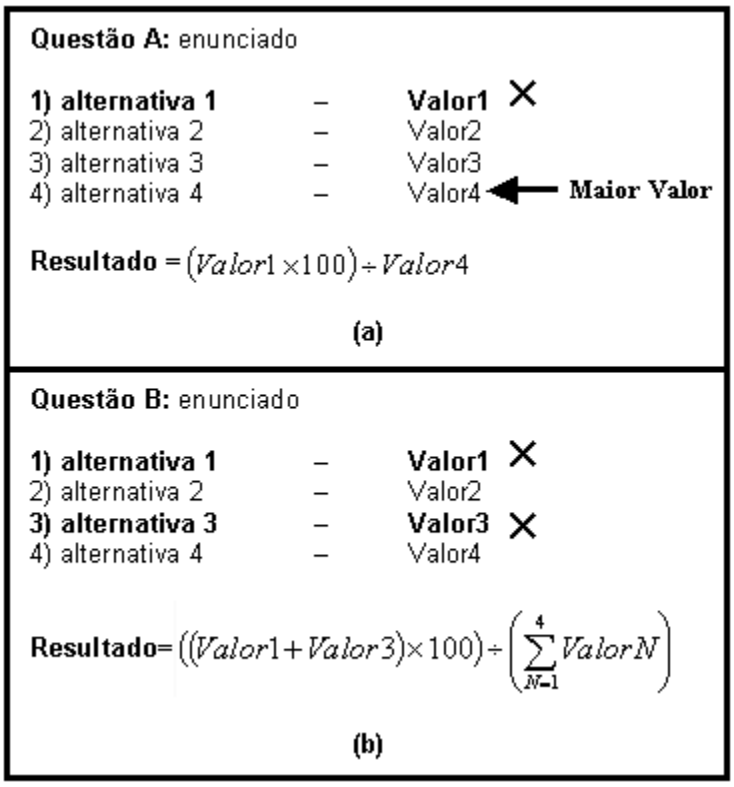


Figura 4.6: Cálculo do Percentual de uma questão do tipo (a) exclusiva ou (b) cumulativa após terem sido respondidas pelo avaliador.

Cada questão de um QIPE também possui um peso associado denominado grau de relevância. Cada grau de relevância tem um peso subjetivo associado que indica a relevância de uma questão com relação às demais dentro do QIPE. A tabela 4.2 mostra os 5 graus de relevância adotados e seus respectivos pesos subjetivos. Com o percentual de cada questão de um QIPE calculado e o seu respectivo grau de relevância, uma média ponderada é efetuada para obter o valor final *VF* de um QIPE:

$$VF(q) = \left(\sum_{i=1}^{n} Gr(i) x Pe(i) \right) \Big/ \left(\sum_{i=1}^{n} Gr(i) \right) \qquad (1)$$

onde *q* identifica o questionário (QIPE), *i* corresponde a uma questão de *q*, *Gr* indica o grau de relevância da questão *i*, e *Pe* indica o percentual obtido na questão *i* pelo avaliador.

Os valores dos pesos associados aos avaliadores variam de 1 a 5. Sendo assim, o valor final *VF* é então mapeado neste intervalo de valores de acordo com a equação abaixo, resultando no peso do avaliador *PA*:

$$PA(q) = \left((VF(q) \times 4)/100\right) + 1 \qquad (2)$$

Vale ressaltar que uma questão pode estar relacionada a mais de um atributo. Dessa forma, o peso de cada questão e/ou das alternativas podem variar dependendo do contexto da definição de um determinado atributo. Por exemplo, uma questão que relacione o contato prático de um avaliador com uma determinada medida de desempenho, como por exemplo FAR ou FRR. Se esta questão está relacionada com um atributo cujo contexto de sua definição envolva uma dessas medidas, então seu peso será maior neste QIPE do que em um QIPE de outro atributo cuja definição não as envolva com igual importância.

Tabela 4.2: Graus de Relevância associados a uma Questão

Grau de Relevância	Peso Subjetivo
1	Mínima Relevância
2	Pouco Relevante
3	Relevante
4	Muito Relevante
5	Imprescindível

4.6 Atributos

Os atributos encontram-se no nível mais baixo do modelo hierárquico, conforme apresentado no capítulo 2 (2.4.2). Os atributos são o resultado da subdivisão dos elementos superiores na hierarquia e mensuram qualitativamente determinados aspectos de um produto. Eles devem ser especificados de acordo com o tipo de produto de *software* que está sendo avaliado e com os propósitos a serem atingidos pela avaliação.

Nós definimos 54 atributos para avaliação do sistema biométrico extraídos das referências [8][9][28][38][66][68][71][72][73][74] e 45 atributos para avaliação das documentações extraídos e baseados na norma ISO/IEC 12119 [34]. Destes 99 atributos no total, 30 foram

completamente definidos e aplicados na avaliação de um pacote de *software* biométrico. Entende-se por completamente definido todos aqueles atributos que tiveram suas especificações definidas e documentadas em sua totalidade, conforme todos os itens apresentados na figura 4.7. Estes atributos foram selecionados de acordo com o tempo que dispúnhamos para a conclusão deste trabalho de dissertação, e do conhecimento e experiência das pessoas envolvidas que principalmente eram especialistas da área de biometria. As especificações de um atributo são definidas em um modelo de documento apresentado na figura 4.7. Cada um dos itens é apresentado a seguir:

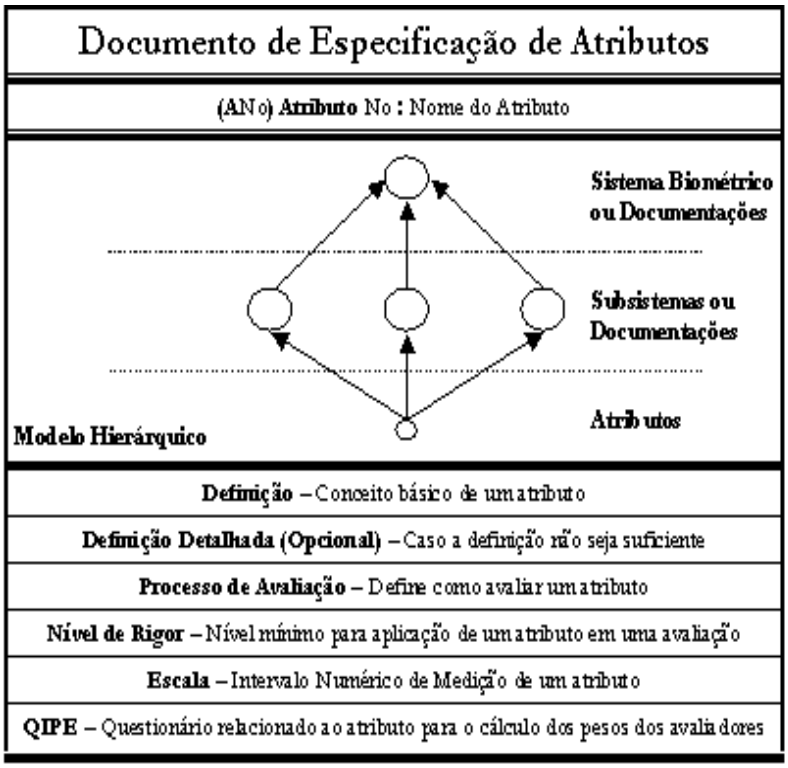


Figura 4.7: Modelo de Documento para a Especificação Completa de um Atributo

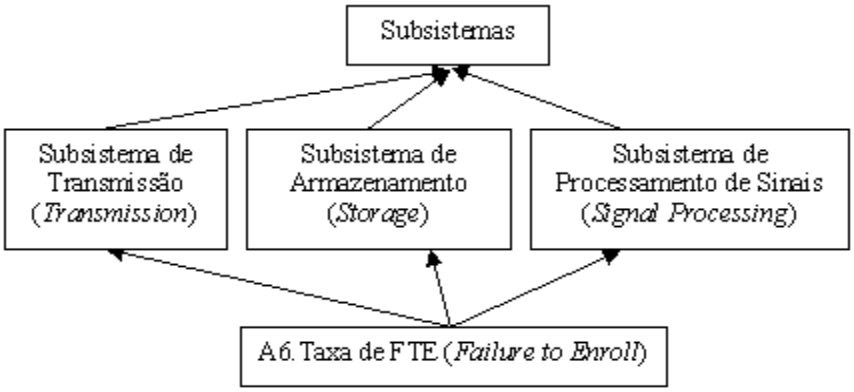
1. **(ANo) Atributo No**: neste item devem ser identificados o nome e um número que será vinculado ao atributo como um código.

⇒ Exemplo 4.1: Mostra um exemplo deste item para o atributo Taxa de FTE:

(A6) Atributo 6: Taxa de FTE (*Failure To Enroll*)

2. **Modelo Hierárquico**: neste item são indicados quais os subsistemas biométricos (documentações) de que um atributo depende hierarquicamente.

⇒ Exemplo 4.2: Na figura abaixo podemos visualizar os subsistemas dos quais o atributo Taxa de FTE é hierarquicamente dependente:



3. **Definição**: este item contém uma descrição do conceito básico do atributo, definido em linhas gerais.

⇒ Exemplo 4.3: Mostra a definição do atributo Taxa de FTE:

Definição: Atributo define a taxa de rejeição ou falha no cadastramento do usuário por quantidade de amostras apresentadas no cadastramento. [68]

4. **Definição Detalhada**: é um item opcional que fornece uma descrição detalhada de um atributo caso o item definição não seja suficiente para um bom entendimento e esclarecimento sobre do quê se trata o atributo.

⇒ Exemplo 4.4: Mostra uma descrição mais detalhada sobre o atributo Taxa de FTE como um complemento para a definição apresentada no exemplo 4.3:

Definição Detalhada: A taxa de rejeição é calculada a partir da quantidade de amostras que um usuário deve fornecer para completar o cadastramento no sistema e passar a ser parte

dele. Falhas podem ocorrer durante o processo de cadastramento. Segundo [68] três tipos de erros podem ocorrer durante o cadastramento:

(1) Falha: o sistema declara que não pode cadastrar a amostra biométrica apresentada;

(2) Expiração de Tempo: o cadastramento ultrapassa o tempo-limite estabelecido (em [68] o tempo-limite é de 15 segundos);

(3) Problemas de Processamento: o sistema apresenta problemas durante o processamento de uma amostra biométrica.

5. **Processo de Avaliação**: instrui um avaliador sobre como proceder para avaliar um atributo.

⇒ Exemplo 4.5: Mostra o processo de avaliação relacionado ao atributo Taxa de FTE.

Processo de Avaliação:

- O objetivo é obter o percentual de falhas no cadastramento dado um número de usuários. Este percentual, por sua vez, deve ser classificado em cada um dos três tipos de erros apresentados no item Definição Detalhada deste atributo, ou seja, além do percentual de falhas do sistema, deve ser informada a fatia pertinente a cada tipo de erro deste percentual.
- O cálculo dessa taxa está diretamente ligado com a quantidade de pessoas que serão usuárias do sistema. Neste caso, para cada novo usuário o sistema não deve apresentar falhas em demasia, ou criará um gargalo, interferindo em outras atividades do sistema e/ou gerando insatisfação para os seus usuários.
- O sistema entregue pelo fabricante deve estar funcionando por completo após sua instalação antes do início dos testes. Um módulo deve acompanhar o sistema para realizar a geração dos percentuais citados. O sistema deve possibilitar o processamento completo de cadastramento de um usuário, e que vários usuários possam cadastrar-se consecutivamente no sistema.
- O módulo deve ser capaz de exibir essas taxas ao final de cada cadastramento para acompanhamento pelos avaliadores.
- O módulo deve ser capaz de incorporar o conceito do atributo apresentado.

- O módulo ou o sistema deve ser capaz de transparecer que parte do sistema apresentou a falha. Desta forma, o avaliador detectará o tipo de falha, aonde ocorreu, justificar seu enquadramento naquele tipo de falha, e qual a sua causa, para que ele possa fazer suas considerações.
- Caso um subsistema não tenha apresentado nenhuma falha, este não deverá ser penalizado no cálculo da nota. Ele é considerado como se tivesse peso 0, o que anula o cálculo da sua nota hierarquicamente, seguindo o cálculo de uma nota de um subsistema.

Caso não seja possível detectar o tipo de falha, ela deve ser classificada como desconhecida, o problema deve ser descrito pelo avaliador, e ele deve justificar qual o motivo que o impediu de classificá-lo em algum tipo de erro, mas ela não pode deixar de ser contabilizada. Caso não seja possível detectar em que ponto do sistema a falha ocorreu, todo o sistema será penalizado, e o avaliador também deve descrever o problema ocorrido e porque não conseguiu enquadrá-lo.

6. **Nível de Rigor**: este item indica o nível mínimo de rigor em que um atributo pode ser aplicado em uma avaliação, ou seja, caso um pacote de *software* biométrico seja classificado no nível de rigor C, por exemplo, e neste item o atributo tenha o nível B, ele não poderá ser utilizado nesta avaliação.

⇒ Exemplo 4.6: Mostra, para o atributo Taxa de FTE, o nível mínimo de rigor que um pacote de *software* biométrico tem de ser classificado para que este atributo seja empregado em uma avaliação:

Nível: C

7. **Escala**: este item define o intervalo de valores que mensura um atributo [3]. As notas de um avaliador para um atributo são concedidas de acordo com uma escala. Dois tipos de escalas foram utilizadas: escalas objetivas e escalas subjetivas. Uma escala objetiva apresenta um intervalo de valores numéricos inteiros ou reais. Uma escala subjetiva apresenta um intervalo de valores subjetivos, como "muito bom", "regular", "excelente". Ambas as escalas, em todos os atributos, são mapeadas em uma escala padrão denominada escala de satisfação, cujo objetivo é uniformizar os valores de todas as

escalas. Esta escala apresenta um intervalo de valores numéricos reais que variam de 0 a 100. A principal vantagem desta escala é que ao calcular as notas dos subsistemas (hierarquicamente imediatamente superiores aos atributos), elas serão refletidas em percentual. Dessa forma, para a percepção humana, é fácil mensurar e definir quais subsistemas "saíram-se bem" ou "saíram-se mal" na avaliação de acordo com o percentual que lhes foi atribuído.

⇒ Exemplo 4.7: Mostra a escala definida para o atributo Taxa de FTE:

Escala: A escala para o atributo Taxa de FTE é utilizada da seguinte maneira:

1º – O avaliador identifica a quantidade de falhas de cadastramento apresentadas pelo sistema e os tipos de falhas apresentadas. Pelo comportamento dos usuários e pela freqüência e quantidade de erros o avaliador julga com relação aos critérios subjetivos apresentados.

2º – O avaliador identifica a compatibilidade do sistema com sua aplicabilidade prática a partir do comportamento dos usuários e do total de falhas e tipos de falhas. O avaliador então julga de acordo com os critérios subjetivos apresentados.

3º – As notas subjetivas são mapeadas nas suas respectivas notas objetivas. As notas objetivas obtidas nos itens 1º e 2º são somadas.

Elementos de Avaliação	Subjetivo	Objetiva
Quantidade de Falhas apresentadas pelo sistema pelo número de usuários.	Nenhuma	+50%
	Mínima	+40%
	Tolerável	+25%
	Considerável	+10%
	Inaceitável	0%
Compatibilidade com a Aplicabilidade Prática.	Sim	+50%
	Sim, porém com um número de falhas tolerável	+30%
	Sim, porém com um número de falhas considerável	+10%
	Não	+0%

8. **QIPE**: este item define o questionário relacionado ao atributo conforme apresentado na seção 4.5. Vale ressaltar que QIPE e Processo de Avaliação estão intrinsecamente ligados e foram utilizados com o objetivo de validar um ao outro. O QIPE é um questionário que tem por objetivo principal a extração do conhecimento e da experiência do avaliador sobre um atributo. O Processo de Avaliação instrui um avaliador sobre como proceder para avaliar um atributo. Sem o Processo de Avaliação, um avaliador pode aplicar uma avaliação subjetiva, de acordo com conceitos e opiniões particulares. Sem o QIPE, todos os avaliadores passam a ter a mesma importância na avaliação de um atributo, ou seja, o mesmo peso é atribuído para todos eles. Assim sendo, o QIPE tem por objetivo extrair os conhecimentos e a experiência de um avaliador sobre um atributo e mensura-o através de um peso, dando maior importância aos que tem mais conhecimento sobre o atributo. O atributo, por sua vez, é definido por um processo de avaliação que instrui e direciona como o avaliador deve proceder para avaliar um pacote de *software*, numa tentativa de eliminar a utilização de conceitos e opiniões particulares na avaliação pelo avaliador. Portanto, essa relação intrínseca entre QIPE e PAA torna a avaliação de um atributo mais robusta, de forma que os resultados obtidos tenham mais acurácia e confiabilidade.

⇒ Exemplo 4.8: Apresenta uma pergunta que está incluída no questionário (QIPE) definido para o atributo Taxa de FTE:

Pergunta: Quais taxas e medidas de desempenho de sistemas biométricos você (avaliador) conhece teoricamente?

Alternativas (cumulativas):

1 – Distribuição Discreta Genuínos (*Genuine Matching Scores*).	Valor associado: 100
2 – Distribuição Discreta Impostores (*Impostor Matching Scores*).	Valor associado: 100
3 – FMR (*False Match Rate*) / FAR (*False Acception Rate*).	Valor associado: 100
4 – FNMR (*False Non-Match Rate*) / FRR (*False Rejection Rate*).	Valor associado: 100
5 – EER (*Equal Error Rate*).	Valor associado: 100
6 – ZeroFNMR.	Valor associado: 100
7 – ZeroFMR.	Valor associado: 100
8 – Curvas de ROC (*Receiving Operating Curve*)	Valor associado: 100

9 – FTE (*Failure to Enroll*) Valor associado: 500

10 – AET (*Average Enroll Time*) Valor associado: 300

11 – AMT (*Average Match Time*) Valor associado: 100

12 – AIT (*Average Identification Time*) Valor associado: 100

Objetivo: Saber qual o conhecimento do avaliador sobre as principais medidas de desempenho de sistemas biométricos as quais está ou esteve em contato teórico.

Peso: 4 (Muito Relevante).

O exemplo completo da especificação do atributo Taxa de FTE pode ser encontrado no anexo III desta dissertação, baseado no modelo de documento mostrado na figura 4.7.

4.7 Aplicação da Avaliação

Como vimos na figura 4.1, o processo 10 – Aplicação da Avaliação só pode ser iniciado uma vez que as seguintes condições sejam satisfeitas:

- Os pesos dos avaliadores tenham sido calculados pela aplicação de QIPEs relacionados a cada um dos atributos;

- Os atributos e o nível da avaliação tenham sido determinados;

- Os ambientes de testes tenham sido estabelecidos;

- O Acordo Comum tenha sido firmado;

- As avaliações que o pacote tenha sofrido anteriormente sejam conhecidas.

Ao avaliar um atributo de um pacote de *software,* o avaliador tem que seguir o processo de avaliação presente na documentação do atributo. Após o atributo ter sido avaliado de acordo com seu processo de avaliação, o avaliador deve conceder a sua nota de acordo com a escala descrita na documentação do atributo (figura 4.7). Uma vez que o avaliador tenha dado sua nota, ele deve

apresentar uma breve justificativa convincente sobre a nota concedida, para casos de auditoria, se necessário.

Os atributos, assim como os avaliadores, também possuem pesos associados. Estes pesos são concedidos de acordo com o nível de rigor mínimo de aplicação descrito na documentação do atributo. O nível A, o mais alto, corresponde a um atributo de peso 5 e o nível E, o mais baixo, corresponde a um atributo de peso 1. Uma vez que as notas tenham sido concedidas, utilizamos a equação abaixo para calcular as notas de cada subsistema biométrico e de cada documentação hierarquicamente superior:

$$Nota(s) = \left(\sum \%NA_i \times WA_i\right) / \left(\sum \%NA_i\right) \quad (3)$$

onde NA_i é o valor percentual da nota do atributo *i*, WA_i é o peso do atributo *i*, e *s* é o subsistema ou documentação do qual o atributo *i* é hierarquicamente dependente. Nesse momento, com as notas associadas a cada subsistema e documentação presente no pacote de *software* biométrico, nós podemos intuitivamente observar quais são os seus pontos fortes e fracos. Podemos apontar que pontos do sistema apresentam deficiências utilizando o modelo hierárquico desenvolvido neste trabalho, tanto de forma gerencial como operacional, ou seja, que pode ser apresentado, por exemplo, de forma sucinta e genérica para um gerente de projetos, como de uma forma detalhada e particular para um programador de um dos módulos do pacote.

Uma vez que as notas dos subsistemas e das documentações tenham sido atribuídas, o próximo passo será calcular a nota do sistema biométrico e das documentações. Utilizando os pesos estabelecidos conjuntamente com o desenvolvedor do pacote de *software* biométrico via Acordo Comum, fazemos uso da equação abaixo para o cálculo das notas:

$$Nota(d) = \left(\sum Nota(s) \times WS_s\right) / \left(\sum Nota(s)\right) \quad (4)$$

onde *Nota(s)* é o valor percentual da nota do subsistema ou documentação *s*, WS_s é o peso do subsistema ou documentação *s*, e *d* é o sistema biométrico ou documentação do pacote do qual os subsistemas ou documentações *s* são hierarquicamente dependentes.

Como último passo, precisamos calcular a nota geral do pacote de *software* biométrico como um todo, para que possamos determinar seu nível de qualidade. Para tanto, precisamos fazer uma

consideração a respeito das documentações. As documentações são imprescindíveis no manuseio e boa utilização de um *software*. Porém, em cada nível de rigor, sua importância aumenta de acordo com dois critérios: necessidades emergenciais e importância dada pelo usuário. Quanto maior o risco apresentado pelo produto para usuários e para o meio onde atua, maior deve ser o detalhamento e clareza de uma documentação para orientar o usuário, que não pode aguardar pelo atendimento do desenvolvedor em casos de problemas ou falhas no *software*, tornando a documentação um veículo importante para solucionar dificuldades e problemas emergenciais. Na segunda coluna da tabela 4.3 podemos visualizar os pesos relacionados com as documentações de um pacote de *software* biométrico pelo nível de rigor. No nível E, a documentação é opcional, pois o produto é tratado como um protótipo. No nível A, a documentação é obrigatória e deve estar detalhada e completa, para oferecer suporte imediato no gerenciamento e manuseio do sistema. O peso atribuído ao sistema biométrico é sempre 5.

Tabela 4.3: Valores de Limiar de Qualidade e Pesos das Documentações classificados por nível

Nível de Rigor	Peso das Documentações	Valor do Limiar de Qualidade
E	1ou 0 (ausência)	70%
D	2	80%
C	3	85%
B	4	90%
A	5	95%

Para o cálculo da nota do pacote de *software* biométrico como um todo, fazemos uso de uma média ponderada da nota do sistema biométrico com a nota das documentações, com o peso do sistema biométrico igual a 5 e das documentações conforme a tabela 4.3. O valor resultante deve ser julgado por um valor de limiar de qualidade: se o valor obtido for maior que o do limiar de qualidade, isto indica que o pacote está adequado para ser aplicado no nível de rigor ao qual foi anteriormente classificado; caso contrário, o pacote deve ser reavaliado em um nível de rigor menor, caso seja possível. Em ambos os casos, as recomendações são necessárias, quando possível. Os valores de limiar de qualidade são dados por nível e são apresentados na tabela 4.3 na terceira coluna. Estes valores foram estabelecidos inicialmente utilizando os valores apresentados em [70], que foram adaptados a nossa metodologia. Porém, estes valores necessitam de um

amadurecimento maior, que só ocorrerá a partir de sua aplicação prática em um número significativo de pacotes de *software* biométricos, a ser atingido em trabalhos futuros neste sentido.

Uma vez que a avaliação foi concluída e a nota do pacote de *software* biométrico tenha sido calculada, um relatório final deve ser produzido e entregue ao desenvolvedor do pacote, com as conclusões da avaliação e as recomendações para melhorias no produto.

4.8 Relatório Padrão

O objetivo de construir um relatório padrão é documentar todo o processo de aplicação de uma avaliação e os resultados obtidos. A figura 4.8 apresenta um modelo de relatório padrão com os respectivos tópicos.

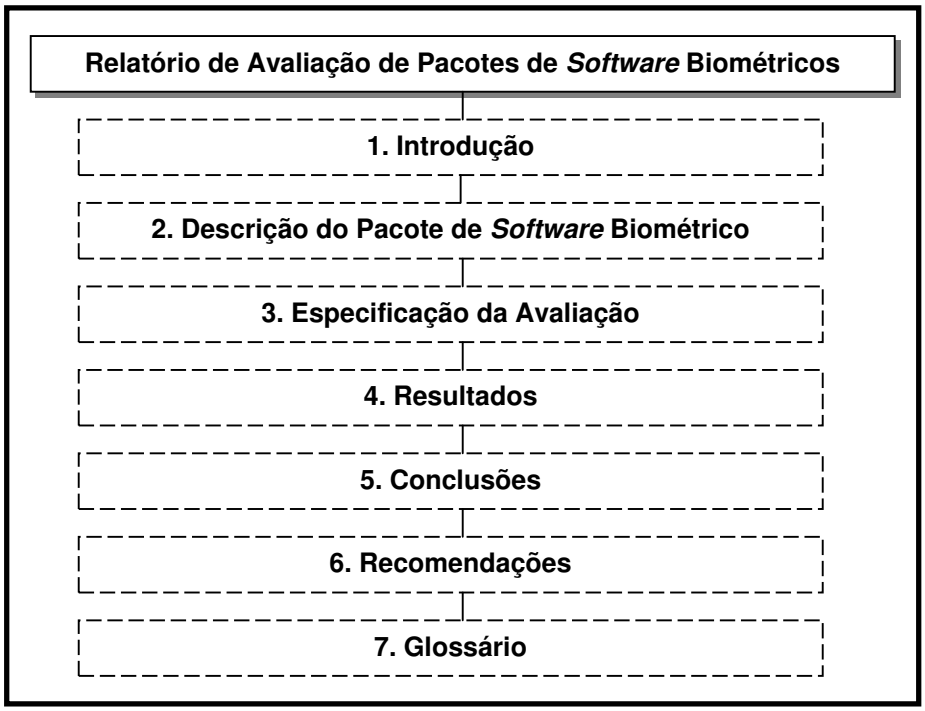


Figura 4.8: Modelo de Relatório Padrão adotado.

Cada tópico, de acordo com a figura 4.8, deve conter as seguintes informações:

1. Introdução – devem ser identificados o desenvolvedor do pacote, os avaliadores envolvidos, e o pacote de *software* biométrico avaliado. A identificação do pacote de

software biométrico deve conter, pelo menos, o nome, versão, a data de requisição e a de conclusão da avaliação.

2. Descrição do Pacote de *Software* Biométrico – devem ser descritos todos os itens físicos, lógicos e funcionais que são parte do pacote de *software* biométrico, assim como as documentações que o acompanham. Estes items, quando possível, devem ser classificados por subsistema biométrico, de acordo com sua aplicabilidade e utilidade prática.

3. Especificação da Avaliação – devem ser especificados:

    i. De uma forma geral, os atributos utilizados no processo de avaliação assim como a seqüência e em que subsistemas foram aplicados;
    ii. O essencial do consenso estabelecido no Acordo Comum;
    iii. O nível de rigor e uma breve justificativa;
    iv. De uma forma geral, os ambientes de testes utilizados para cada atributo. Devem ser especificados os ambientes de teste estabelecidos de acordo com o Acordo Comum e aqueles sugeridos pelos avaliadores, definindo e comparando o desempenho do pacote de *software* biométrico em cada ambiente de teste;
    v. As padronizações, normas, métodos e técnicas utilizadas;
    vi. As ferramentas que deram suporte para a avaliação;
    vii. Se uma avaliação foi aplicada em uma versão anterior do pacote, deve ser especificado onde e porque foram aplicados os testes na nova versão do pacote, discernindo entre as partes que foram e as que não foram modificadas, relacionando se as novas funcionalidades e modificações da atualização têm alguma interferência negativa sobre os elementos avaliados na versão anterior.

4. Resultados – devem ser especificados:

    i. As notas obtidas por cada subsistema biométrico;
    ii. As notas obtidas por cada documentação;

iii. As notas obtidas pelo sistema biométrico e pelas documentações;
iv. A nota do pacote de *software* biométrico.

Cada nota deve ser seguida por uma breve explicação, identificando em que pontos o pacote de *software* apresenta ou não deficiências.

5. Conclusões – deve ser especificado se o pacote de *software* biométrico está de acordo com os requerimentos da avaliação. Se necessário, devem ser feitas justificativas mais detalhadas sobre as notas obtidas pelos subsistemas biométricos e documentações, assim como os respectivos pontos fortes e fracos.

6. Recomendações – devem ser especificadas, caso for necessário, recomendações sobre o pacote de *software* biométrico, baseado nas conclusões e na análise dos diferentes ambientes de teste empregados pelos avaliadores e nos resultados obtidos nestes casos.

7. Glossário – devem ser especificados os termos e as abreviações utilizadas para a construção do relatório.

CAPÍTULO 5

A FERRAMENTA BIOEVA

Neste capítulo apresentamos uma ferramenta denominada BioEVA (derivada de Biometric EVAluation). Mostramos que a ferramenta foi desenvolvida com a finalidade de aplicar uma avaliação objetiva em algoritmos biométricos, isto é, sem o envolvimento de avaliadores. Apresentamos as formalidades a serem cumpridas pelos desenvolvedores para a submissão de algoritmos biométricos. Descrevemos também cada um dos módulos desenvolvidos: cadastramento, autenticação e avaliação.

5.1 Introdução

Na última década, o interesse de pesquisadores e empresas tem aumentado consideravelmente com relação às tecnologias biométricas. Um número significativo de algoritmos e equipamentos biométricos tem sido desenvolvido e comercializado, com o propósito de garantir uma maior segurança na autenticação de seus usuários [6].

Porém, é necessário também garantir qualidade a esses equipamentos e algoritmos, de forma que o consumidor não seja o maior prejudicado. Neste capítulo, propomos um processo de avaliação automatizado e objetivo, ou seja, com o intuito de realizar uma avaliação do algoritmo biométrico sem a interferência humana, excluindo assim os critérios subjetivos.

Para esta finalidade, desenvolvemos uma ferramenta que denominamos BioEVA, onde implementamos, utilizando a linguagem java (plataforma JAVA 2), um ambiente para receber um

algoritmo como uma *black-box,* ou seja, sem o conhecimento do código-fonte. Três módulos foram implementados para esta finalidade: um para cadastrar os usuários (módulo de cadastramento), outro para autenticá-los (módulo de autenticação) e, por fim, um para avaliar os algoritmos biométricos com base nos testes realizados nos dois módulos anteriores (módulo de avaliação).

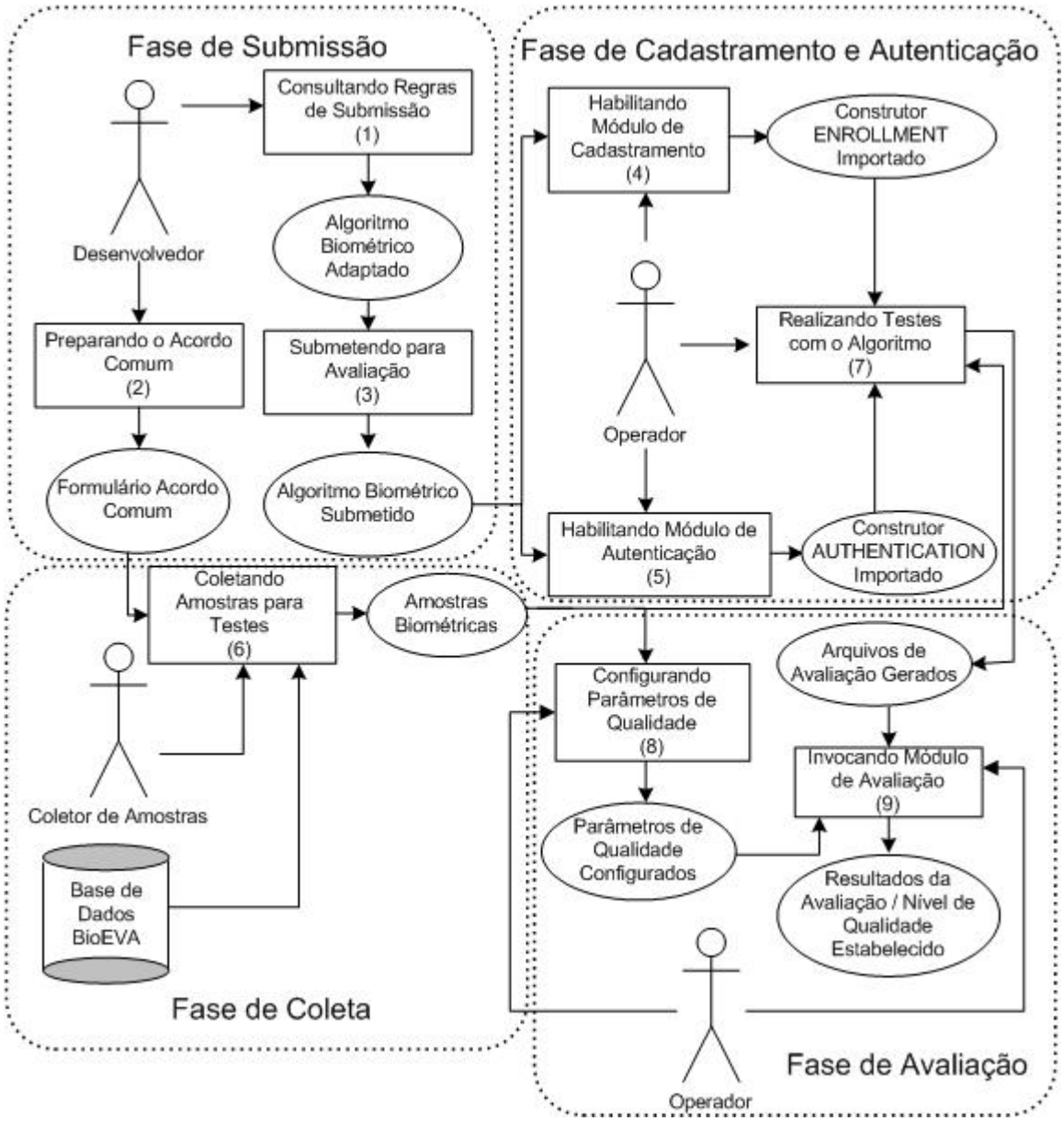


Figura 5.1: Esquema de Avaliação da Ferramenta BioEVA

A figura 5.1 mostra o esquema de avaliação utilizando a ferramenta BioEVA. Inicialmente, na fase de submissão, o desenvolvedor consulta o protocolo de submissão para adaptar o algoritmo biométrico para o ambiente da ferramenta BioEVA (Processo (1) – Consultando Regras de Submissão). O protocolo de submissão será apresentado na seção 5.4 deste capítulo. Uma vez que o algoritmo biométrico foi adaptado, o desenvolvedor submete-o para avaliação (Processo (3) – Submetendo para Avaliação). A partir de então, é possível para o Operador habilitar os módulos de cadastramento e autenticação, pela incorporação do algoritmo biométrico ao ambiente da ferramenta (Processo (4) – Habilitando Módulo de Cadastramento e Processo (5) – Habilitando Módulo de Autenticação). Para iniciar os testes com o algoritmo utilizando os módulos de cadastramento e autenticação, é necessário saber que amostras o algoritmo biométrico aceita como válidas. Neste ponto, na fase de coleta, o desenvolvedor faz uso do formulário do Acordo Comum para explicitar quais as características das amostras biométricas a serem utilizadas nos testes (Processo (2) – Preparando o Acordo Comum). Uma vez que o formulário tenha sido finalizado, caso não existam amostras na base de dados (Base de Dados BioEVA) que tenham as mesmas características daquelas mencionadas no formulário, elas precisam ser coletadas pelo Coletor de Amostras (Processo (6) – Coletando Amostras para Testes). Tendo habilitado os módulos de cadastramento e autenticação e as amostras tenham sido coletadas, o Operador pode realizar os testes com o algoritmo (Processo (7) – Realizando Testes com o Algoritmo) na fase de cadastramento e autenticação. Como resultado destes testes, na fase de avaliação, são gerados arquivos que serão utilizados pelo módulo de avaliação para produzir a nota final do algoritmo biométrico e avaliá-lo de acordo com os parâmetros de qualidade (Processo (9) – Invocando o Módulo de Avaliação). Os parâmetros de qualidade são configurados pelo Operador uma vez que se sabe qual é o tipo de tecnologia biométrica implementada no algoritmo (Processo (8) – Configurando os Parâmetros de Qualidade). Estes parâmetros foram estabelecidos de acordo com [38], [66] e [68] e serão apresentados na seção 5.7 deste capítulo.

Uma vez finalizado o processo (9) – Invocando o Módulo de Avaliação na figura 5.1, o algoritmo recebe uma nota. Esta nota definirá o nível de qualidade do algoritmo, o qual julgamos de acordo com valores de limiar de qualidade conforme mostrados no capítulo 4 (4.7) na tabela 4.3. A nota é comparada com cada valor de limiar, começando do nível de rigor E. O objetivo é buscar qual o maior nível de rigor em que o algoritmo biométrico enquadra-se e classificá-lo neste nível.

Nos tópicos seguintes, falaremos sobre uma competição denominada FVC para algoritmos biométricos baseados em digitais, mostraremos o *background* no qual a ferramenta BioEVA foi implementada, como submeter um algoritmo biométrico para avaliação, e faremos também a apresentação da ferramenta BioEVA, seus módulos e interfaces.

5.2 Fingerprint Verification Competition (FVC)

A FVC [68] emprega seus esforços em uma competição entre algoritmos biométricos baseados em digitais para verificação pessoal. A primeira e a segunda edições foram organizadas em 2000 e em 2002, e a terceira será realizada em 2004. Estas edições receberam algoritmos biométricos provindos tanto do meio acadêmico quanto de desenvolvedores atuando na indústria de *software*.

Todo o procedimento adotado na FVC para comparação de algoritmos é padronizado, desde as amostras existentes na base de dados ao processo de comparação dos algoritmos biométricos. Isto permitiu uma avaliação comparativa, sem ambigüidades, entre os algoritmos submetidos, fornecendo para a comunidade científica em biometria uma importante contribuição sobre o estado da arte em autenticação baseada em digitais. A tabela 5.1 mostra alguns dados sobre participações e sensores utilizados nas duas primeiras edições da competição.

Tabela 5.1. Dados sobre a participação e base de dados na FVC

	FVC2000	FVC2002
Número de Participantes	**11** 4 industrial, 7 academic	**31** 21 industrial, 6 academic and 4 other
Número de Base de Dados e Sensores Utilizados	**4** Keytronic, ST, Identicator, SFinGE	**4** Identix, Biometrika, PreciseB, SFinGE

Para a FVC 2004, os participantes podem submeter seus algoritmos para duas categories:

1) *Light*: criada para os algoritmos biométricos que tenham baixa necessidade computacional, limite de uso de memória, e geram pequenos *templates*. Nesta categoria os limites para o tempo de cadastramento é de 0.5 segundos, para o tempo de autenticação é de 0.3

segundos, tamanho máximo do *template* tem de ser de 2 Kbytes e a quantidade de memória alocada não mais que 4 Mbytes.

2) *Open*: criada para algoritmos biométricos que não tenham limite de memória ou tamanho de *template*. Por razões de testes práticos, o tempo máximo de cadastramento é de 10 segundos e o de autenticação é de 5 segundos.

Cada participante pode submeter somente um algoritmo em cada categoria. Para submeter o algoritmo biométrico à competição, cada participante deve submeter dois executáveis (um para aplicar o processo de cadastramento e o outro para o processo de autenticação). Estes executáveis serão testados via linha de comando, por onde também são passados os argumentos. Para preparar os executáveis que serão utilizados na FVC, os participantes devem obrigatoriamente fazer uso de dois *skeletons* escritos na linguagem C: uma para o processo de cadastramento e outro para o processo de autenticação.

Os algoritmos biométricos submetidos a FVC são testados para cada uma das bases de dados utilizadas. Os resultados dos testes são utilizados para avaliar o desempenho do algoritmo de acordo com alguns indicadores, como as taxas de FAR e FRR, o número de amostras rejeitadas durante o cadastramento, o ponto de EER, e o tempo médio de comparação, por exemplo.

Maiores detalhes sobre a FVC podem ser encontrados em [68]. Na próxima seção, mostraremos como a FVC e a metodologia apresentada no capítulo 4 contribuíram para a construção da ferramenta BioEVA.

5.3 Background da Ferramenta BioEVA

A ferramenta BioEVA foi desenvolvida baseada em dois conceitos distintos de avaliações: qualitativa e comparativa. Nesta seção apresentaremos as propostas e idéias relacionadas a dois trabalhos que motivaram o desenvolvimento dessa ferramenta.

5.3.1 Propostas e Idéias Abordadas da FVC

Neste trabalho, nós adotamos as seguintes idéias originadas da FVC:

- Estabelecimento de um protocolo para a submissão de um algoritmo biométrico para uma avaliação comparativa (competição);

- Padronizar definições e critérios para a comparação entre algoritmos biométricos, através do uso de parâmetros de qualidade.

Além disso, nós propomos que, recebendo um algoritmo biométrico como uma "*black-box*", possamos avalia-los tanto comparativamente (como a FVC) como qualitativamente. Propomos também a utilização de uma plataforma para estabelecer uma independência de linguagem e de sistema operacional, o que eliminaria os *skeletons* propostos na FVC, e automatizaria e tornaria mais eficiente o processo de aplicação das avaliações comparativa e qualitativa. Esta proposta reduziria ainda mais os esforços empregados pelos participantes na submissão de seus algoritmos biométricos e abrangeria um maior número de participantes do que o esquema montado na FVC.

Por fim, a FVC não apresenta um protocolo formal para a coleta das amostras que irão compor as bases de dados. Sendo assim, os participantes têm de adaptar seus algoritmos biométricos aos tipos dos dados que a FVC fornece, o que pode acabar por prejudicar os resultados produzidos nos testes dos seus algoritmos biométricos, ou, simplesmente, eles acabam por não submeter. Assim, a utilização do Acordo Comum é proposto, conforme foi apresentado na metodologia no capítulo 4 (4.4), para preencher esta lacuna da FVC.

5.3.2. Propostas e Idéias Abordadas da Metodologia para Avaliação de Pacotes de *Software* Biométricos

A metodologia foi apresentada no capítulo 4 e tem por objetivo aplicar uma avaliação de qualidade em pacotes de *software* biométricos. A avaliação comparativa teve suas idéias básicas extraídas e reformuladas da FVC, enquanto nós fizemos uso de alguns elementos da metodologia para implementar uma avaliação qualitativa.

O Acordo Comum foi adaptado da metodologia para solucionar um problema apresentado na FVC: a falta de um protocolo formal para estabelecer as características das amostras coletadas. Nós transformamos o Acordo Comum em um formulário com a finalidade de coletar informações a respeito das características das amostras biométricas junto aos desenvolvedores (figura 5.1 – processo (1) – Preparando o Acordo Comum). Além de coletar estas informações, o

formulário contém também informações sobre a nossa base de dados (figura 5.1 – Base de Dados BioEVA). Se o desenvolvedor optar por utilizar as amostras da base de dados, então a avaliação do algoritmo biométrico prossegue; caso contrário, as amostras serão coletadas pelo Coletor de Amostras (figura 5.1) segundo as especificações fornecidas pelo desenvolvedor (figura 5.1 – processo (6) – Coletando Amostras para Testes).

Para definir o grau de qualidade do algoritmo biométrico, baseado em seu desempenho e eficiência, fizemos uso dos níveis de rigor e dos valores de limiar definidos na metodologia. Para definir o grau de qualidade de um algoritmo biométrico, primeiro o Operador aciona o processo (9) – Invocando o Módulo de Avaliação na figura 5.1, e a ferramenta BioEVA produz a nota do algoritmo biométrico. Depois, fazemos uso dos valores de limiar definidos na segunda coluna da tabela 4.3 (capítulo 4 (4.7)) e classificamos o algoritmo biométrico: se a nota obtida for maior ou igual ao valor de limiar de qualidade, ele é aceito para o nível de rigor selecionado; caso contrário, ele é classificado em um nível de rigor inferior.

5.4 Protocolo de Submissão para a Ferramenta BioEVA

Antes de submeter um algoritmo biométrico para avaliação pela ferramenta BioEVA, o desenvolvedor do algoritmo deve obedecer a certas regras de submissão (figura 5.1 – processo (1) – Consultando Regras de Submissão). As regras a serem seguidas são:

1) Se o algoritmo biométrico foi desenvolvido usando:

- linguagem java: algoritmo é submetido como um arquivo `.jar`;
- outras linguagens: algoritmo é submetido como um *library file* (como `.dll` para Windows ou `.so` para Unix e Linux, por exemplo).

O arquivo submetido será chamado dentro do código-fonte da ferramenta BioEVA. Os desenvolvedores precisam gerar um *library file* ou um `.jar`, dependendo da linguagem que utilizaram para implementar o algoritmo e/ou da plataforma que foi desenvolvido. Assim, nós propiciaremos aos desenvolvedores a vantagem de independência de linguagem e plataforma;

2) Dois construtores (linguagem java) ou procedimentos (outras linguagens) devem ser criados: ENROLLMENT e AUTHENTICATION.

Uma vez que o algoritmo biométrico foi submetido de acordo com o protocolo de submissão, o Operador (figura 5.1) irá importá-los usando uma declaração `import` (linguagem java) ou *Java Native Interface* (JNI – outras linguagens). Este procedimento irá permitir que o Operador habilite os módulos de cadastramento e de autenticação da ferramenta BioEVA (figura 5.1 – processo (4) – Habilitando Módulo de Cadastramento e o processo (5) – Habilitando o Módulo de Autenticação). Nós iremos nos referir a ENROLLMENT e AUTHENTICATION como construtores a partir deste ponto, mas as regras contidas no protocolo de submissão são as mesmas para os procedimentos de ENROLLMENT e AUTHENTICATION escritos em outras linguagens.

3) A chamada do construtor ENROLLMENT deve obedecer à seguinte sintaxe para as variáveis de entrada:

```
ENROLLMENT ( id, samples, template_destination )
```

cujas descrições das variáveis de entrada são apresentadas na tabela 5.2.

Tabela 5.2: Descrição das Variáveis de Entrada para o Construtor ENROLLMENT

Variáveis de Entrada	Tipo	Descrição
`id`	`String`	Identificador do Usuário
`samples`	`array of string`	Conjunto de caminhos absolutos das amostras utilizadas para a geração do(s) *template(s)*
`template_destination`	`String`	Caminho absoluto aonde o(s) *template(s)* será(ão) criado(s).

4) A chamada do construtor AUTHENTICATION deve obedecer à seguinte sintaxe para as variáveis de entrada:

```
AUTHENTICATION ( id, sample, templates_location )
```

cujas descrições das variáveis de entrada são apresentadas na tabela 5.3.

Tabela 5.3: Descrição das Variáveis de Entrada para o Construtor AUTHENTICATION

Variáveis de Entrada	Tipo	Descrição
`id`	`String`	Identificador do Usuário (verificação) ou `null` (identificação)
`sample`	`String`	Caminho absoluto da amostra
`template_location`	`String`	Caminho absoluto onde estão localizados os *templates*

5) Os construtores ENROLLMENT e AUTHENTICATION deverão retornar suas saídas utilizando o método (função) como se segue:

```
string output_results ( )
```

onde `string` é a saída gerada pelos construtores de ENROLLMENT e AUTHENTICATION. A composição de `string` depende do construtor:

- ENROLLMENT: a sintaxe de `string` é "`Value+Total_samples`". `Value` indica se o processo de cadastramento ocorreu com sucesso (`Value` = 0) ou não (`Value` ≠ 0). Em caso de não ter sucesso, `Value` pode ser igual a 1 (Falha), 2 (TIMEOUT) ou 3 (CRASH), cujas respectivas definições são baseadas em [68]. `Total_samples` indica o número de amostras utilizadas para cadastrar um usuário.
- AUTHENTICATION: a sintaxe de `string` é "`&id-value`" (verificação) ou a concatenação desta sintaxe (identificação), ou seja, "`&id1-value1&id2-value2&id3-value3 ... &idN-valueN`". `Id` indica o identificador do usuário relacionado ao *template* no qual a amostra foi comparada. `Value` indica o valor produzido pelo resultado da comparação da amostra com um *template*. Ao retornar este valor, o desenvolvedor deve observar que a ferramenta BioEVA considera o valor de limiar de aceitação como os valores menores ou iguais a *t* (valor de limiar), e o valor de limiar de rejeição como os valores maiores que *t*.

A adoção do tipo `string` é motivada pelo fato de que são mais simples de implementar do que se utilizássemos uma estrutura de dados complexa para retorno das informações, o que reduz os esforços empregados pelos desenvolvedores ao adaptar seus algoritmos biométricos. Além disso, excluímos problemas relacionados à variação na forma de implementação ou a não-existência de algumas estruturas de dados quando variamos de linguagem de programação. As saídas que devem ser geradas por ambos os construtores apresentados serão utilizadas para gerar

os resultados da avaliação do algoritmo biométrico (figura 5.1 – processo (7) – Realizando Testes com o Algoritmo).

5.5 Módulo de Cadastramento

Usando este módulo o Operador pode cadastrar usuários usando o algoritmo biométrico submetido. A figura 5.2 mostra a tela representativa da interface do módulo de cadastramento. Os números mostrados na figura 5.2 identificam os campos da interface e são explicados a seguir:

(1) *Current Evaluation Directory*: este campo identifica o algoritmo que está tendo seu processo de cadastramento avaliado no momento.

(2) *The Enrollment Algorithm is*: identifica se o algoritmo implementado utiliza um (*single*) ou mais (*multimodal*) tipos de características biométricas no processo de cadastramento.

(3) *User's ID (CODE)*: identifica o código do usuário que será cadastrado.

(4) *Kind of Biometric Samples*: identifica o(s) tipo(s) de característica(s) biométrica(s) que será(ão) utilizada(s) no processo de cadastramento.

(5) *Samples*: permite selecionar ou remover os arquivos contendo as amostras biométricas que serão utilizadas no processo de cadastramento.

(6) *ENROLL*: Faz a chamada ao construtor ENROLLMENT. As informações fornecidas pelo Operador (figura 5.1) serão utilizadas como variáveis de entrada para o construtor ENROLLMENT, conforme apresentado no protocolo de submissão na seção 5.3, e para que ele possa realizar os testes necessários (figura 5.1 – processo (7) – Realizando Testes com o Algoritmo). O método `output_results` relacionado com o construtor ENROLLMENT irá retornar `string`, conforme apresentado na seção 5.3, o qual BioEVA irá utilizar para construir os arquivos com as informações que o Módulo de Avaliação usará para produzir os resultados da avaliação. Como

resultado do processo (7) – Realizando Testes com o Algoritmo na figura 5.1, três arquivos serão gerados a partir de string:

- ParameterET.dat: recebe os tempos, em milissegundos, que o algoritmo biométrico levou para completar cada um dos processos de cadastramento realizados;

- ParameterFTE.dat: recebe os valores relacionados com o sucesso ou falha de cada um dos processos de cadastramento realizados;

- ParameterTSE.dat: recebe os valores relacionados à quantidade de amostras utilizadas para cadastrar os usuários que foram utilizadas em cada um dos processos de cadastramento realizados.

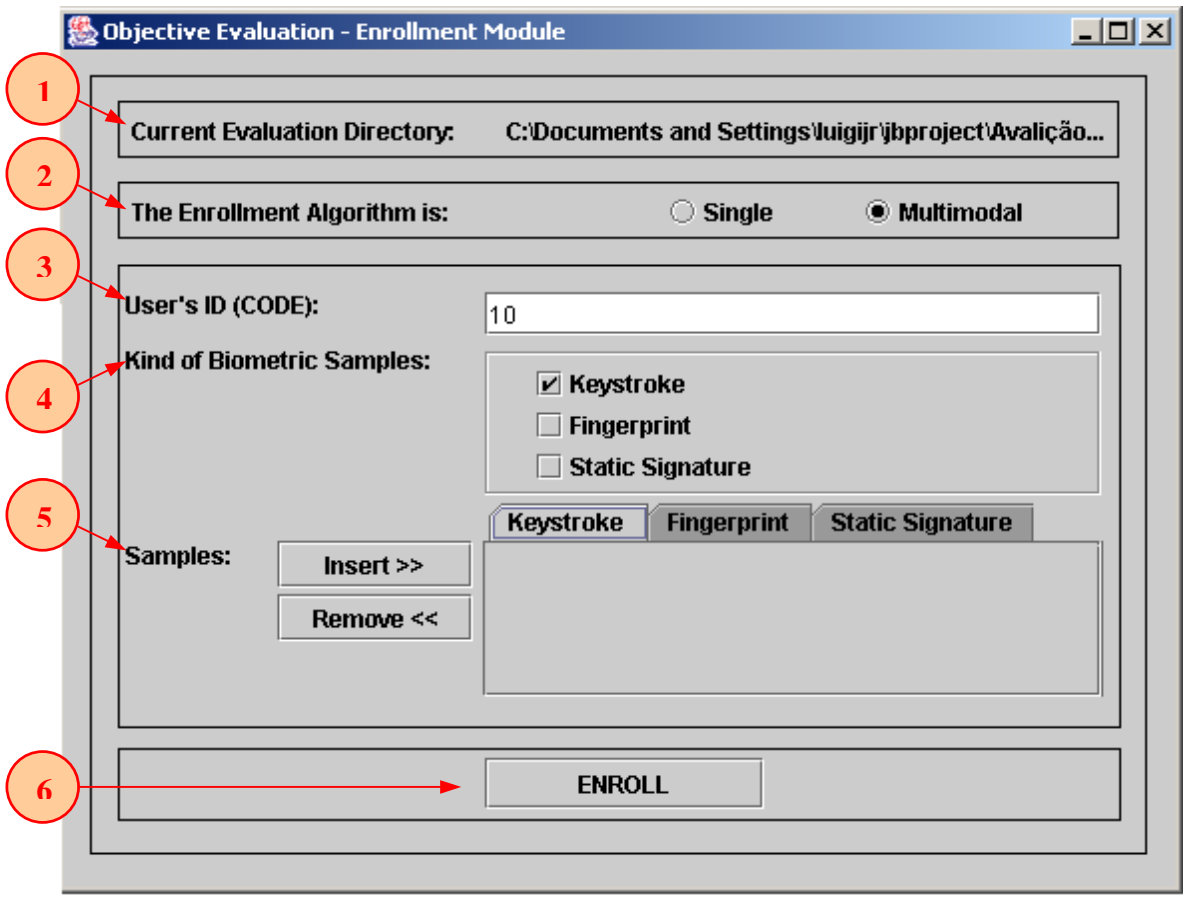


Figura 5.2: Interface do Módulo de Cadastramento salientando os principais elementos.

5.6 Módulo de Autenticação

Usando este módulo o Operador pode autenticar (verificar ou identificar) usuários usando o algoritmo biométrico submetido. A figura 5.3 mostra a tela representativa da interface do módulo de autenticação. Os números mostrados na figura 5.3 identificam os campos da interface e são explicados a seguir:

(1) *Current Evaluation Directory*: identifica o algoritmo que está tendo seu processo de autenticação avaliado no momento.

(2) *Kind of Biometric System*: identifica se o algoritmo implementado utiliza um (*single*) ou mais (*multimodal*) tipos de características biométricas.

(3) *Kind of Authentication*: possibilita identificar se o teste que será realizado será do tipo verificação ou identificação no processo de autenticação.

(4) *User's ID (CODE)*: identifica o código do usuário que será autenticado e passado como variável de entrada para o construtor AUTHENTICATION, caso seja um processo de verificação. No processo de identificação, o identificador do usuário apresentado na tela não será passado como variável de entrada para o construtor AUTHENTICATION, e no seu lugar será passado o valor `null`. O objetivo deste procedimento é associar as informações geradas pelo construtor no processo de identificação com o proprietário da amostra biométrica, já que neste processo a identidade do proprietário de uma amostra biométrica não é conhecida

(5) *Kind of Biometric Samples*: identifica o(s) tipo(s) de característica(s) biométrica(s) que será(ão) utilizada(s) no processo de autenticação.

(6) *Samples*: permite selecionar ou remover os arquivos contendo as amostras biométricas que serão utilizadas no processo de autenticação.

(7) *AUTHENTICATE*: irá fazer a chamada ao construtor AUTHENTICATION. As informações fornecidas pelo Operador (figura 5.1) serão utilizadas como variáveis de

entrada para o construtor AUTHENTICATION, conforme apresentado no protocolo de submissão na seção 5.3, e para que ele possa realizar os testes necessários (figura 5.1 – processo (7) – Realizando Testes com o Algoritmo). O método output_results relacionado com o construtor AUTHENTICATION irá retornar string, conforme apresentado na seção 5.3, o qual BioEVA irá utilizar para construir os arquivos com as informações que o Módulo de Avaliação usará para produzir os resultados da avaliação. Como resultado do processo (7) – Realizando Testes com o Algoritmo na figura 5.1, BioEVA irá gerar três arquivos a partir de string:

- Parameter_v'id'_AT.dat: este arquivo é relacionado com os testes de autenticação do tipo verificação, recebendo os tempos, em milissegundos, que o algoritmo biométrico leva para completar cada um dos processos de verificação. O 'id' no nome do arquivo é o identificador do usuário fornecido pelo Operador (figura 5.1) no módulo de autenticação.

- Parameter_v'id'_FFC_IGD.dat: este arquivo é relacionado com os testes de autenticação do tipo verificação, recebendo os valores resultantes da comparação de uma amostra de um usuário com seu respectivo *template*. O 'id' no nome do arquivo é o identificador do usuário fornecido pelo Operador (figura 5.1) no módulo de autenticação.

- Parameter_i_AT.dat: este arquivo é relacionado com os testes de autenticação do tipo identificação, recebendo os tempos, em milissegundos, que o algoritmo biométrico leva para completar cada um dos processos de identificação.

- Parameter_i_FFC_IGD.dat: este arquivo é relacionado com os testes de autenticação do tipo identificação, recebendo os valores resultantes das comparações de uma amostra biométrica com todos os *templates* existentes na base de dados.

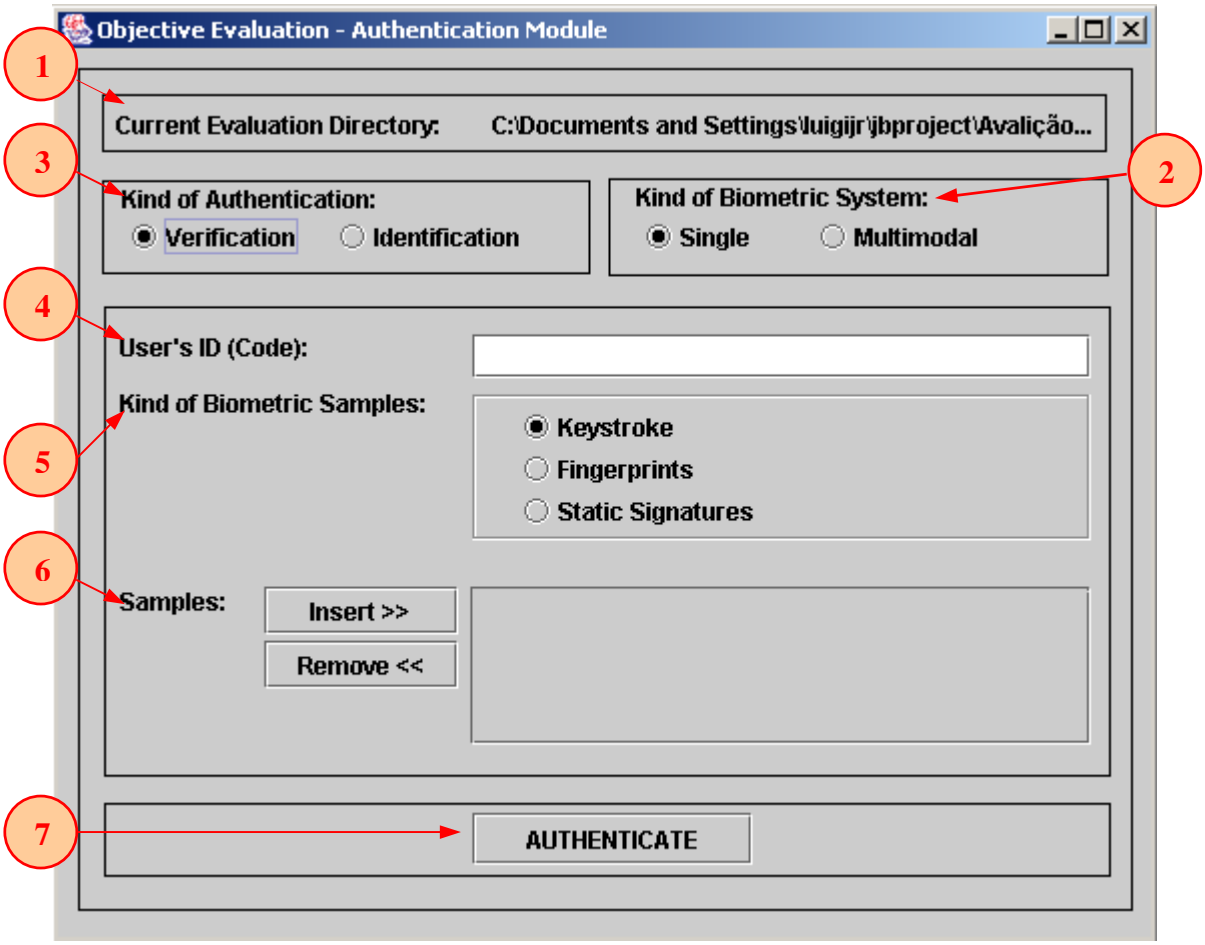


Figura 5.3: Interface do Módulo de Autenticação salientando os principais elementos.

5.7 Módulo de Avaliação

No módulo de avaliação, todos os arquivos gerados nos testes nos módulos anteriores de cadastramento e de autenticação serão utilizados para gerar os resultados da avaliação do algoritmo biométrico de forma automatizada. Estes resultados serão apresentados na interface do módulo de avaliação. Quando o Operador (figura 5.1) invoca este módulo (figura 5.1 – processo (9) – Invocando o Módulo de Avaliação), BioEVA automaticamente extrai os dados armazenados nestes arquivos para calcular a nota do algoritmo biométrico e fornecer informações relacionadas a cada um dos parâmetros de qualidade utilizados. A nota do algoritmo biométrico é expresso por

uma nota percentual que varia de 0% a 100%, calculada a partir da média das notas dos parâmetros de qualidade avaliados.

Para a obtenção dessa nota, nós fazemos uso de parâmetros de qualidade, conforme mencionado na seção 5.1. Um total de 6 parâmetros de qualidade foi utilizado. Cada um deles é apresentado nas subseções a seguir, assim como as suas respectivas interfaces.

5.7.1 Distribuição Impostor/Genuíno (IGD)

Este parâmetro de qualidade define o grau de separabilidade existente entre a distribuição de genuínos e a distribuição de impostores. Estas distribuições assemelham-se a histogramas: para cada valor de limiar adotado, uma quantidade de usuários é aceita como usuários genuínos e o restante que são aceitos como usuários impostores. Dessa forma, variando o valor de limiar, conseguimos plotar ambas as distribuições, e verificar o grau de separação existente entre elas. As informações contidas nos arquivos Parameter_v'id'_FFC_IGD.dat e Parameter_i_FFC_IGD.dat são utilizadas para construir o gráfico das distribuições. A figura 5.4 mostra a interface do módulo de avaliação correspondente a este parâmetro.

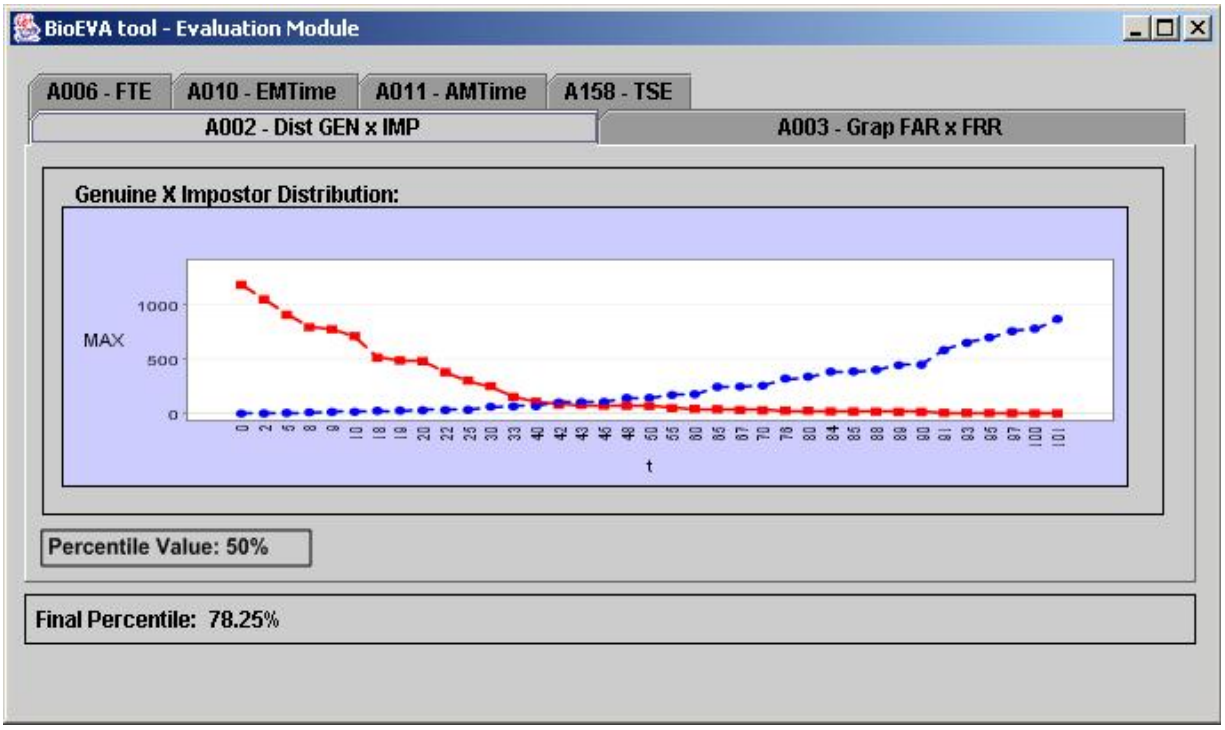


Figura 5.4: Interface do Parâmetro de Qualidade IGD.

Como pode ser observado na figura 5.4, o eixo das ordenadas apresenta a quantidade de testes de autenticação realizados, e o eixo das abscissas apresenta o valor de limiar. *Percentile Value* indica o valor percentual da nota atingida por esse parâmetro de qualidade segundo a definição apresentada. *Final Percentile* irá aparecer também em todas as interfaces apresentadas nas figuras posteriores a 5.4 neste capítulo e indica a nota final que o algoritmo atingiu conforme os parâmetros de qualidade utilizados.

5.7.2 Curvas de FAR/FRR (FFC)

Este parâmetro de qualidade define os valores das taxas de FAR e FRR de acordo com cada valor de limiar no intervalo de [0,*t*], onde *t* é o maior valor obtido pelos resultados gerados nas comparações entre amostras e *templates* no processo de autenticação. Dessa forma podemos plotar as curvas com as taxas de FAR e FRR e encontrar o ponto de intersecção entre elas, chamado de EER (*Equal Error Rate*). As informações contidas nos arquivos Parameter_v'id'_FFC_IGD.dat e Parameter_i_FFC_IGD.dat são utilizadas para construir o gráfico com as curvas de FAR e FRR. A figura 5.5 mostra a interface do módulo de avaliação correspondente a este parâmetro.

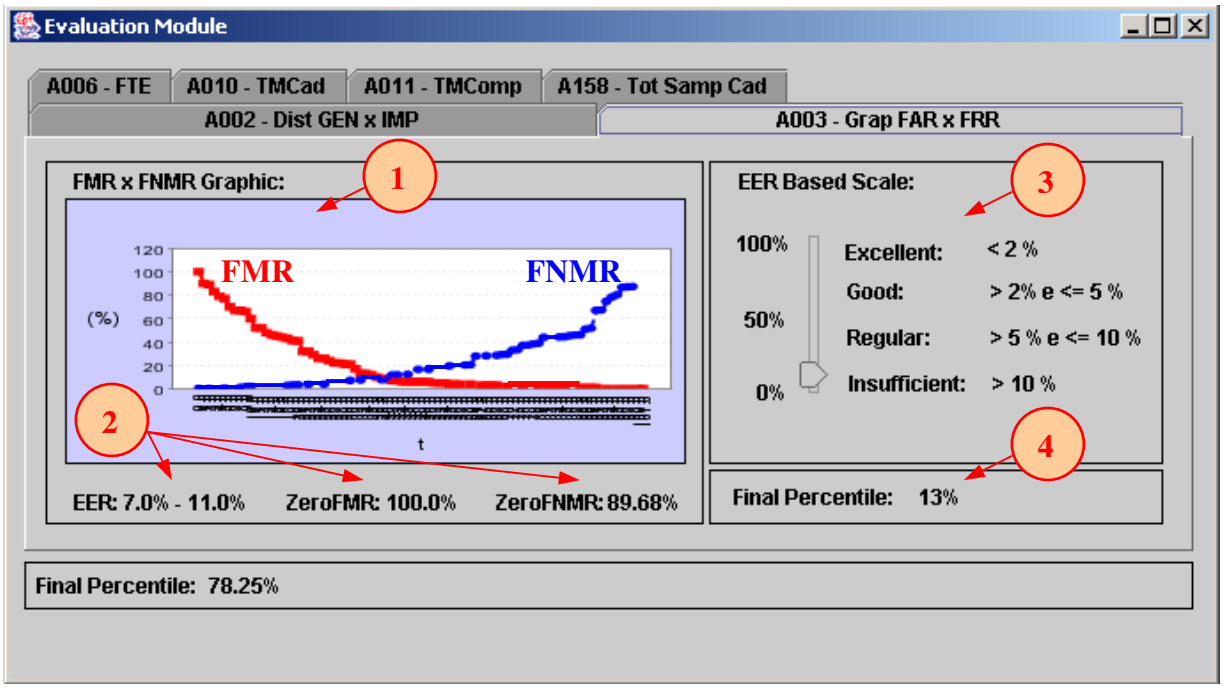


Figura 5.5: Interface do Parâmetro de Qualidade FFC.

De acordo com a figura 5.5, os elementos indicados são:

(1) Mostra o gráfico de FMR (FAR) X FNMR (FRR).

(2) Mostra os valores de EER, ZeroFAR (ou ZeroFMR) e ZeroFRR (ou ZeroFNMR), cujas definições foram apresentadas no capítulo 3 (3.2), calculados a partir dos pontos gerados no cálculo das taxas de FAR e FRR em cada valor de limiar no intervalo de [0,*l*].

(3) Mostra a escala na qual o valor de EER é mapeado e, como resultado, é produzido um valor percentual equivalente ao valor de EER calculado.

(4) Indica o valor percentual, ou a nota, concedida ao parâmetro de qualidade, baseado no mapeamento na escala, conforme item (3).

5.7.3 Tempo de Cadastramento (ET)

Este parâmetro de qualidade define a análise da média e do desvio-padrão calculados sob os tempos de cadastramento dos usuários que foram capturados no módulo de cadastramento. Uma vez com esses dois valores calculados (média e desvio-padrão), a ferramenta mapeia cada um em sua respectiva escala, e posteriormente calcula a nota final relacionada a esse parâmetro de qualidade. As informações contidas no arquivo ParameterET.dat são utilizadas para o cálculo da média e do desvio-padrão conforme descrito. A figura 5.6 mostra a interface do módulo de avaliação correspondente a este parâmetro.

De acordo com a figura 5.6, os elementos indicados são:

(1) Mostra a média calculada em segundos dos tempos de cadastramento capturados no módulo de cadastramento.

(2) Mostra a escala na qual o valor da média é mapeado e, como resultado, é produzido um valor percentual equivalente a este valor.

(3) Mostra o desvio-padrão calculado em segundos dos tempos de cadastramento capturados no módulo de cadastramento.

(4) Mostra a escala na qual o valor do desvio-padrão é mapeado e, como resultado, é produzido um valor percentual equivalente a este valor.

(5) Mostra o percentual final calculado a partir dos valores percentuais produzidos pelos mapeamentos da média e do desvio-padrão nas suas respectivas escalas.

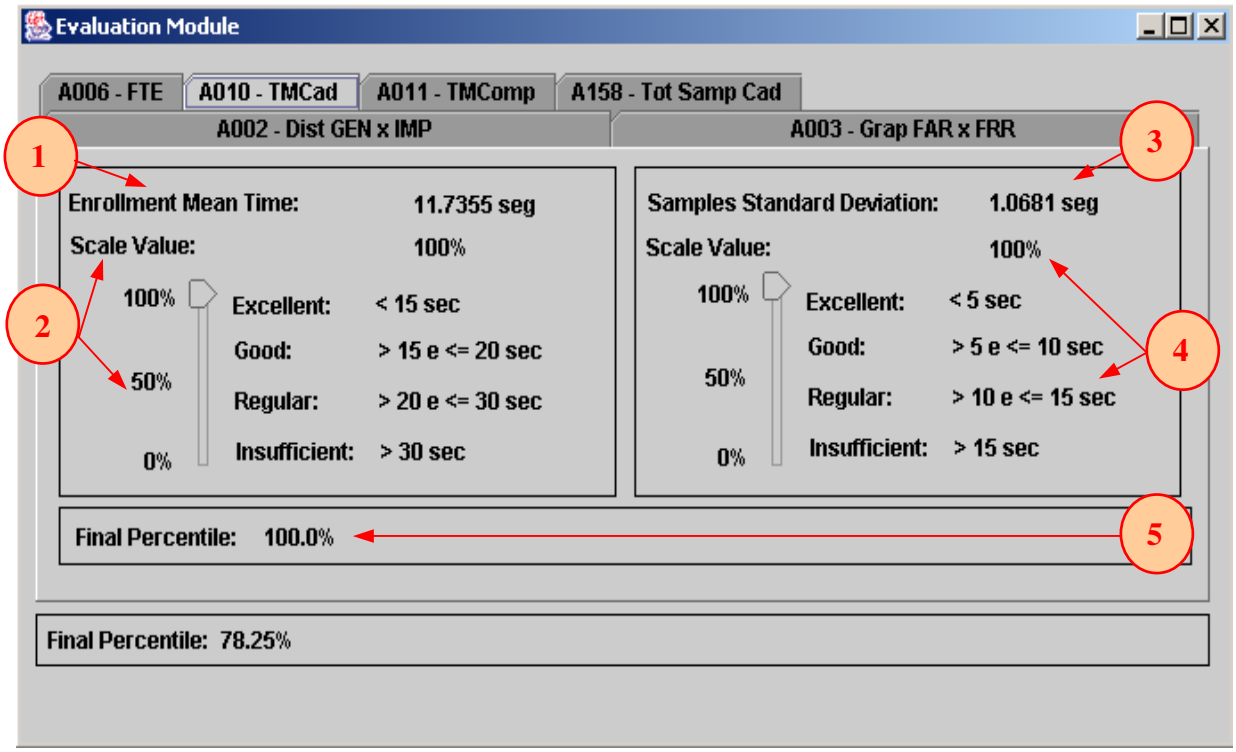


Figura 5.6: Interface do Parâmetro de Qualidade ET

5.7.4 Tempo de Autenticação (AT)

Este parâmetro de qualidade define a análise da média e do desvio-padrão calculados sob os tempos de autenticação dos usuários que foram capturados no módulo de autenticação. Esses dois valores são capturados nos dois tipos de autenticação: verificação e identificação. Uma vez com esses dois valores calculados (média e desvio-padrão) para verificação e para identificação, a

ferramenta mapeia cada um em sua respectiva escala, e calcula a nota final para cada um dos tipos de autenticação. A média das notas calculadas para verificação e para identificação resultará na nota final referente ao parâmetro de qualidade AT. Caso um sistema não implemente um dos tipos de autenticação, somente será calculada a nota e avaliado o tipo de autenticação que foi implementado pelo algoritmo biométrico. As informações contidas nos arquivos Parameter_v'id'_AT.dat e Parameter_i_AT.dat são utilizadas para calcular as respectivas média e desvio-padrão dos processos de verificação e identificação. As figuras 5.7 (verificação) e 5.8 (identificação) mostram as interfaces do módulo de avaliação correspondente a este parâmetro.

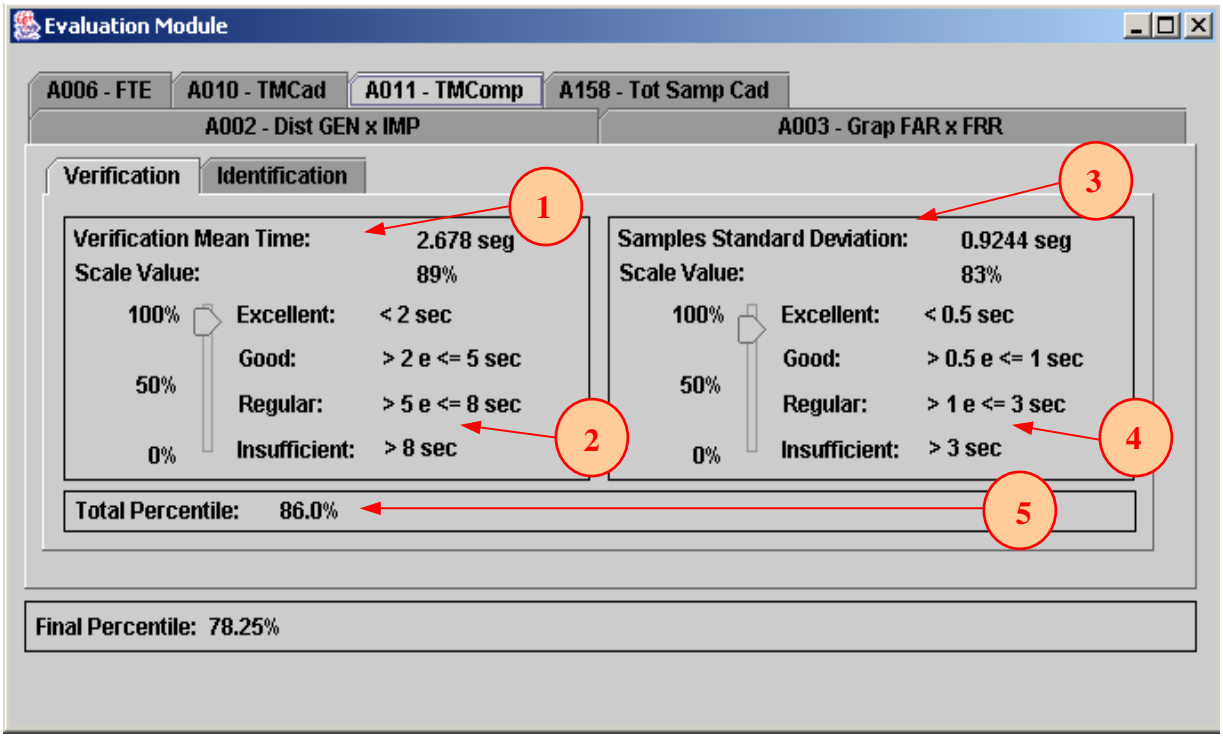


Figura 5.7: Interface do Parâmetro de Qualidade AT para Verificação

De acordo com a figura 5.7, os elementos indicados são:

(1) Mostra a média calculada em segundos dos tempos de autenticação (verificação) capturados no módulo de autenticação.

(2) Mostra a escala na qual o valor da média é mapeado e, como resultado, é produzido um valor percentual equivalente a este valor.

(3) Mostra o desvio-padrão calculado em segundos dos tempos de autenticação (verificação) capturados no módulo de autenticação.

(4) Mostra a escala na qual o valor do desvio-padrão é mapeado e, como resultado, é produzido um valor percentual equivalente a este valor.

(5) Mostra o percentual final calculado a partir dos valores percentuais produzidos pelos mapeamentos da média e do desvio-padrão nas suas respectivas escalas.

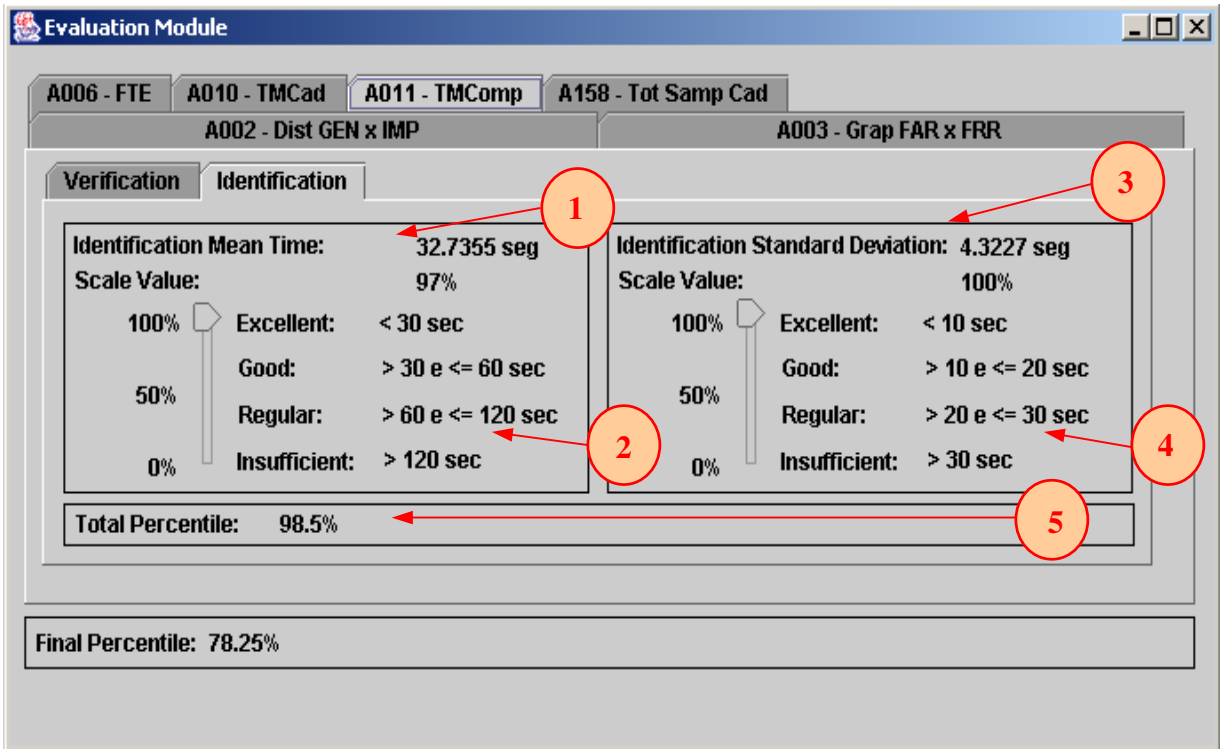


Figura 5.8: Interface do Parâmetro de Qualidade AT para identificação

De acordo com a figura 5.8, os elementos indicados são:

(1) Mostra a média calculada em segundos dos tempos de autenticação (identificação) capturados no módulo de autenticação.

(2) Mostra a escala na qual o valor da média é mapeado e, como resultado, é produzido um valor percentual equivalente a este valor.

(3) Mostra o desvio-padrão calculado em segundos dos tempos de autenticação (identificação) capturados no módulo de autenticação.

(4) Mostra a escala na qual o valor do desvio-padrão é mapeado e, como resultado, é produzido um valor percentual equivalente a este valor.

(5) Mostra o percentual final calculado a partir dos valores percentuais produzidos pelos mapeamentos da média e do desvio-padrão nas suas respectivas escalas.

5.7.5 Falha ao Cadastrar (FTE – *Failure To Enroll*)

Este parâmetro de qualidade define a análise da quantidade de falhas ocorridas no total de cadastramentos realizado pelo algoritmo biométrico, cujos valores são coletados no módulo de cadastramento. Uma vez conhecida esta quantidade de falhas, a ferramenta mapeia o percentual de falhas pelo número total de cadastramentos realizados em sua respectiva escala, resultando no percentual relativo a nota final desse parâmetro de qualidade. As informações contidas no arquivo ParameterFTE.dat são utilizadas para a análise da quantidade de falhas conforme descrito. A figura 5.9 mostra a interface do módulo de avaliação correspondente a este parâmetro.

De acordo com a figura 5.9, os elementos indicados são:

(1) Mostra o total de cadastramentos realizados no módulo de cadastramento utilizando o algoritmo biométrico fornecido.

(2) Mostra o total de falhas que ocorreram dentro do total de cadastramentos.

(3) Mostra a quantidade de cadastramentos que foram realizados com sucesso e a quantidade de cadastramentos que apresentaram erros no processo de cadastrar um usuário, categorizadas conforme apresentado na seção 5.3 deste capítulo.

(4) Mostra a escala na qual o percentual da quantidade de falhas pelo total de cadastramentos realizados é mapeado, como resultado produzindo o valor percentual equivalente a este valor.

(5) Mostra o percentual final calculado a partir do valor percentual produzido pelo mapeamento do percentual da quantidade de falhas pelo total de cadastramentos realizados.

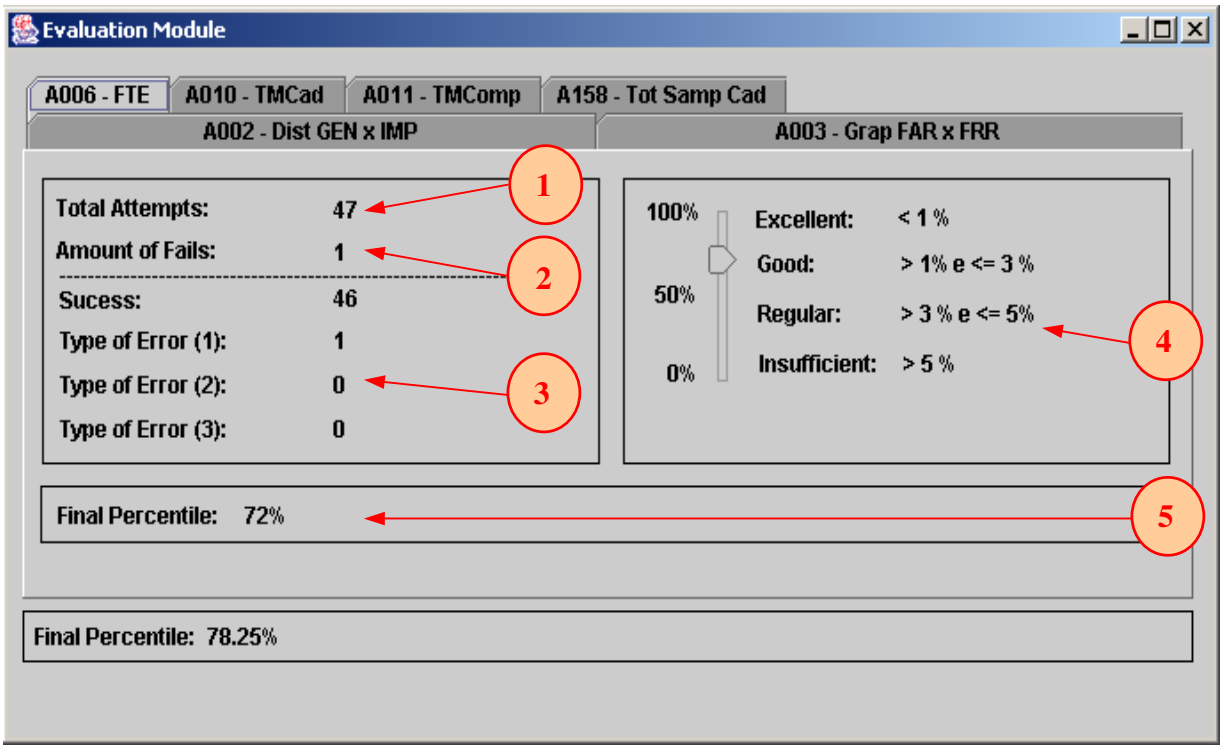


Figura 5.9: Interface do Parâmetro de Qualidade FTE

5.7.6 Total de Amostras no Cadastramento (TSE)

Este parâmetro de qualidade define a análise da quantidade de amostras utilizadas para o cadastramento de um usuário pelo algoritmo biométrico. Uma vez conhecida esta quantidade de amostras, a ferramenta mapeia-a em sua respectiva escala, resultando no percentual relativo a nota final desse parâmetro de qualidade. Esse parâmetro é julgado também levando em consideração que a quantidade de amostras a serem coletadas para a realização do processo de cadastramento não aborreça o usuário pelas sucessivas insistências em seus fornecimentos. As informações

contidas no arquivo ParameterTSE.dat são utilizadas para a análise da quantidade de amostras para o cadastramento do usuário, conforme descrito. A figura 5.10 mostra a interface do módulo de avaliação correspondente a este parâmetro.

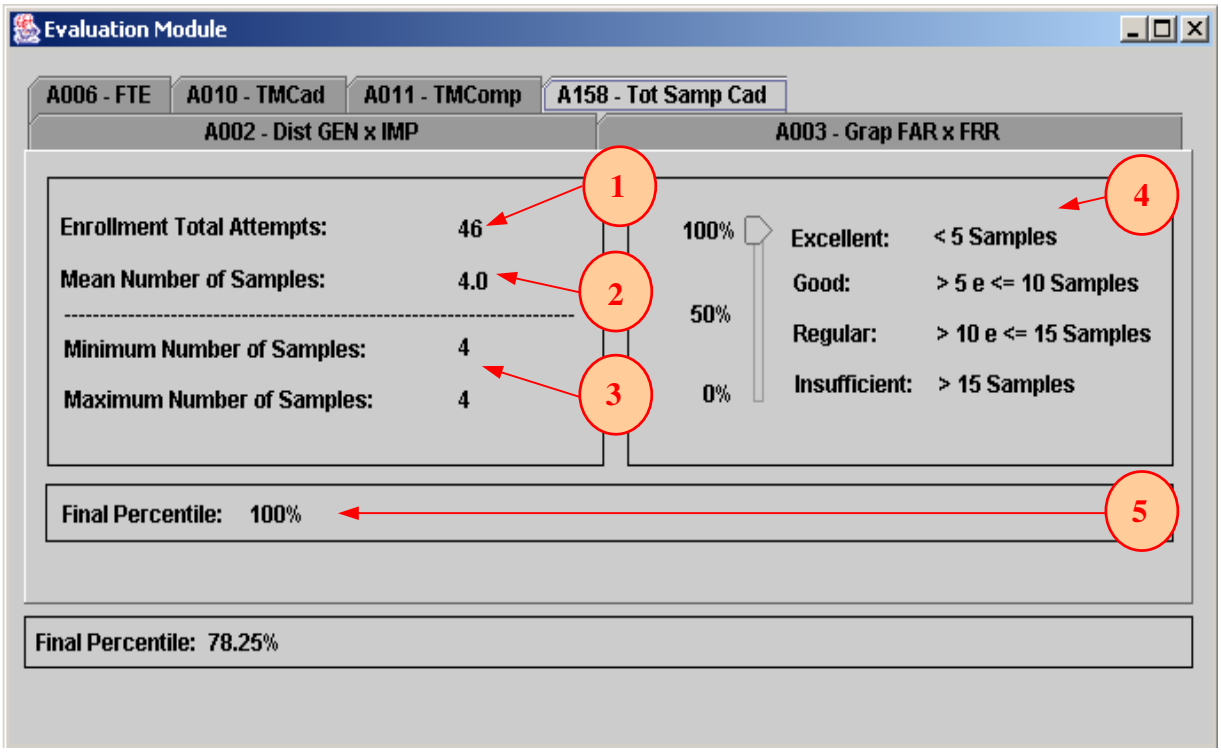


Figura 5.10: Interface do Parâmetro de Qualidade TSE

Os elementos da figura 5.10 são definidos abaixo:

(1) Mostra o total de cadastramentos realizados no módulo de cadastramento utilizando o algoritmo biométrico fornecido.

(2) Mostra o valor resultante da média das quantidades de amostras utilizada para cadastrar um usuário no total de cadastramentos realizados, coletadas no módulo de cadastramento.

(3) Mostra os valores da maior e da menor quantidade de amostras utilizados para cadastrar um usuário dentro do total de cadastramentos realizados.

(4) Mostra a escala na qual o valor médio é mapeado, produzindo, como resultado, o valor percentual equivalente a este valor.

(5) Mostra o percentual final calculado a partir do valor percentual produzido pelo mapeamento do valor médio.

CAPÍTULO 6

RESULTADOS DAS AVALIAÇÕES

Neste capítulo apresentamos os resultados obtidos a partir da aplicação da ferramenta BioEVA em três algoritmos biométricos submetidos para avaliação, e da aplicação da metodologia em um pacote de software biométrico. Comentários serão realizados ao longo da exibição dos resultados para o seu melhor entendimento. O propósito é tornar a metodologia e a ferramenta propostas cada vez mais robustas através de sucessivas aplicações práticas.

6.1 Algoritmos Biométricos Avaliados

Após projetarmos o ambiente para avaliação de algoritmos biométricos e implementá-lo na ferramenta BioEVA, e utilizando o esquema de avaliação apresentado na figura 5.1, realizamos três avaliações com algoritmos biométricos: dois algoritmos baseados em assinaturas estáticas para verificação e identificação pessoal (ASig1 e ASig2), e um algoritmo baseado em dinâmica da digitação para verificação pessoal (AKey1). As informações relacionadas a cada um deles são:

(1) Algoritmo baseado em Assinaturas Estáticas (ASig1) – este algoritmo foi submetido externamente: uma empresa colaborou conosco na avaliação do seu algoritmo biométrico. Este algoritmo aplica identificação e verificação para o reconhecimento pessoal. O processo de cadastramento necessita de 4 amostras de imagens de assinaturas para cadastrar um usuário. O desenvolvedor informou-nos que o classificador utilizado pelo algoritmo ASig1 é baseado em Redes Neurais.

(2) Algoritmo baseado em Assinaturas Estáticas (ASig2) – este algoritmo foi submetido pelo Laboratório de Reconhecimento de Padrões e Redes de Comunicações (LRPRC) da Universidade Estadual de Campinas (UNICAMP). Este algoritmo aplica identificação e verificação para o reconhecimento pessoal. O processo de cadastramento necessita de 5 amostras de imagens de assinaturas para cadastrar um usuário. O desenvolvedor informou-nos que o classificador do algoritmo ASig2 é baseado na Distância de Mahalanobis.

(3) Algoritmo baseado em Dinâmica da Digitação (AKey1) – este algoritmo também foi submetido pelo LRPRC da UNICAMP. Este algoritmo aplica verificação para o reconhecimento pessoal. O processo de cadastramento necessita que o usuário digite 10 vezes uma string contendo, pelo menos, 10 caracteres. O desenvolvedor informou-nos que o classificador do algoritmo AKey1 é basedo em Lógica Fuzzy.

Uma vez de posse dos algoritmos, nós selecionamos um microcomputador no qual pudéssemos realizar os testes (assumindo assim um ambiente de testes comum para os três algoritmos) e coletamos as amostras de assinaturas estáticas e de dinâmica da digitação. O microcomputador utilizado foi um Itautec Athlon 1.0 Ghz com 256 Mbytes de RAM. O ambiente comum foi utilizado para mostrar, utilizando os parâmetros de qualidade apresentados no capítulo 5 (5.5), a possibilidade de comparação de algoritmos biométricos que também pode ser feita utilizando a ferramenta BioEVA. Para este caso, faremos uso dos dois algoritmos baseados em assinaturas estáticas, ASig1 e ASig2, submetidos para avaliação.

6.1.1. Aquisição de Amostras

A base de dados dos algoritmos biométricos ASig1 e ASig2 foi composta pelas amostras de assinaturas estáticas de 112 usuários diferentes. Cada usuário assinou um total de 5 vezes para o conjunto de treinamento (utilizados para propósitos de cadastramento) e uma média de 4 vezes para o grupo de testes (utilizados para propósitos de autenticação), resultando em uma base de dados com um total de 1098 amostras. Todas as imagens coletadas foram digitalizadas sob uma resolução de 200 DPI. Para o algoritmo ASig1, conforme orientações do desenvolvedor, as imagens coletadas deveriam ficar em uma área retangular restrita de 4 cm de altura por 20 cm de comprimento. Para o algoritmo ASig2, conforme orientações do desenvolvedor, as imagens

coletadas não precisam ter nenhuma limitação de área. Estas informações foram coletadas e repassadas aos respectivos desenvolvedores fazendo uso do Acordo Comum, conforme mencionado no capítulo 5 (5.2.2). Desta maneira, podemos utilizar a mesma base de dados coletada para testar os dois algoritmos, seja realizando uma avaliação qualitativa quanto uma avaliação comparativa.

A base de dados para o algoritmo biométrico AKey1 foi composta pelas amostras de ritmos de digitação de 50 usuários diferentes. Cada usuário digitou uma média de 65 vezes: 10 vezes para o conjunto de treinamento, e entre 50 e 60 vezes para o conjunto de testes. Isto resultou em uma base de dados com um total de 3250 amostras. Para o caso da coleta de amostras do conjunto de testes, 20 amostras correspondiam às amostras de autenticação do próprio usuário (legítimo), e 30 a 40 amostras correspondiam às amostras de autenticação como um impostor. Para o segundo caso, nós fornecíamos a string de um usuário qualquer e pedíamos para que o impostor inserisse-a. O tamanho mínimo de cada string digitada é de 10 caracteres. Essas amostras foram coletadas utilizando um teclado de notebook e dois tipos diferentes de *layout* de teclados em máquinas desktop. As amostras foram coletadas, para cada usuário, em seções distintas, para permitir uma real intra-variabilidade pessoal das amostras coletadas.

Nas próximas subseções, nós mostraremos os resultados obtidos em cada um dos algoritmos pela aplicação da avaliação pela ferramenta BioEVA.

6.1.2. Avaliando os Algoritmos ASig1 e ASig2

O primeiro passo foi importar a classe que contêm os construtores de ENROLLMENT e de AUTHENTICATION. Dessa forma, habilitamos os módulos de cadastramento e autenticação para realização dos testes. Após isso, nós utilizamos os conjuntos de treinamento e teste coletados para gerar as informações que serão utilizadas pelo módulo de avaliação, conforme apresentado no capítulo 5.

O segundo passo foi configurar as escalas dos parâmetros de qualidade. As tabelas 6.1 e 6.2 mostram as escalas configuradas dos seus respectivos parâmetros de qualidade. Para configurar as escalas, fizemos uma consulta a diversas referências [63, 64, 65, 68, 70, 75, 76] envolvendo desempenho de algoritmos baseados em assinaturas estáticas, tanto para verificação quanto para identificação pessoal.. O desvio padrão presente nos parâmetros de qualidade ET e AT foi configurado por nós, pois nenhuma das referências citadas apresentou ou fez uso deste

parâmetro. Nós observamos que este valor pode mensurar o grau de estabilidade de um algoritmo biométrico em torno dos tempos médios calculados nos processos de cadastramento e autenticação. Assim, consideramos que este valor é relevante na avaliação do desempenho de algoritmos biométricos e que, portanto, deve ser utilizado para tanto. Por exemplo, se avaliarmos dois algoritmos, A e B, e ambos obtiveram o tempo médio de cadastramento de 20 segundos, eles são iguais sob esta perspectiva. Porém, se o desvio padrão de A for igual a 3 segundos e o de B for igual a 12 segundos, nós podemos afirmar que o sistema A é mais estável que o sistema B, ou seja, apresenta valores de tempo que ficam próximo do seu tempo médio calculado.

Tabela 6.1: Escalas dos Parâmetros de Qualidade FFC, FTE, TSE e ET para assinaturas.

Parâmetros / Escala		FFC	FTE	TSE	ET	
					μ	σ
100%	**Excelente**	$v \leq 2\%$	$v \leq 1\%$	$v \leq 5$	$v \leq 15s$	$v \leq 5s$
	Bom	$2\% < v \leq 5\%$	$1\% < v \leq 3\%$	$5 < v \leq 10$	$15s < v \leq 20s$	$5s < v \leq 10s$
50%	**Regular**	$5\% < v \leq 10\%$	$3\% < v \leq 5\%$	$10 < v \leq 15$	$20s < v \leq 30s$	$10s < v \leq 15s$
0%	**Insuficiente**	$v > 10\%$	$v > 5\%$	$v > 15$	$v > 30s$	$v > 15s$

Tabela 6.2: Escalas dos Parâmetros de Qualidade AT para assinaturas.

Parâmetros / Escala		AT			
		VERIFICAÇÃO		IDENTIFICAÇÃO	
		μ	σ	μ	σ
100%	**Excelente**	$v \leq 2s$	$v \leq 0.5s$	$v \leq 30s$	$v \leq 10s$
	Bom	$2s < v \leq 5s$	$0.5s < v \leq 1s$	$30s < v \leq 60s$	$10s < v \leq 20s$
50%	**Regular**	$5s < v \leq 8s$	$1s < v \leq 3s$	$60s < v \leq 120s$	$20s < v \leq 30s$
0%	**Insuficiente**	$v > 8s$	$v > 3s$	$v > 120s$	$v > 30s$

Os resultados para os testes com a ferramenta BioEVA aplicados no algoritmo ASig1 são apresentados na segunda coluna da tabela 6.3. Os resultados para os testes com a ferramenta BioEVA aplicados no algoritmo ASig2 são apresentados na segunda coluna da tabela 6.4. Ambas as tabelas mostram na terceira coluna o valor percentual que é o resultado do mapeamento dos valores da segunda coluna das tabelas 6.3 e 6.4 nas escalas dos respectivos parâmetros de qualidade.

Tabela 6.3: Resultados da Avaliação para o Algoritmo ASig1.

PARÂMETROS DE QUALIDADE			ASig1	
			Resultados dos Testes	Valor Percentual Obtido
IGD			-	50%
FFC			9%	13%
FTE			0.89%	100%
TSE			4 amostras	100%
ET	μ		11.7 s	100%
	σ		1.1 s	
AT	**Verificação**	μ	2.6 s	86%
		σ	0.9 s	
	Identificação	μ	32.7 s	
		σ	4.3 s	
NOTA FINAL				74.83%

Tabela 6.4: Resultados da Avaliação para o Algoritmo ASig2.

PARÂMETROS DE QUALIDADE			ASig2	
			Resultados dos Testes	Valor Percentual Obtido
IGD			-	92%
FFC			2.6%	93%
FTE			0%	100%
TSE			5 amostras	100%
ET	μ		3.4 s	100%
	σ		0.97 s	
AT	**Verificação**	μ	1.2 s	99.5%
		σ	0.5 s	
	Identificação	μ	20.5 s	
		σ	5.1 s	
NOTA FINAL				97.41%

Calculando a média dos valores obtidos na terceira coluna nas tabelas 6.3 e 6.4, resulta na nota final do algoritmo biométrico ASig1 que foi igual a 74.83%, e na nota final do algoritmo biométrico ASig2 que foi igual a 97.41%, respectivamente. De acordo com os valores de limiar estabelecidos na tabela 4.3, ASig1 é considerado um algoritmo biométrico nível E (protótipo – baixo desempenho) e ASig2 é considerado um algoritmo biométrico nível A (alta qualidade e eficiência). Estes valores para ambos os algoritmos biométricos são resultados produzidos em uma avaliação qualitativa aplicando a ferramenta BioEVA.

Numa avaliação comparativa, observando os valores atingidos por ASig1 e ASig2 na segunda coluna nas tabelas 6.3 e 6.4, o desempenho e a eficiência do algoritmo ASig2 é bem superior a do algoritmo ASig1. O algoritmo ASig1 apresenta um alto valor de EER no parâmetro de qualidade FFC e o parâmetro IGD mostra que as distribuições não são satisfatoriamente separadas, porém o algoritmo utiliza poucas amostras para o cadastramento de seus usuários e obteve resultados satisfatórios para os parâmetros de qualidade ET e AT. Já o algoritmo ASig2 obteve um excelente desempenho em todos os parâmetros de qualidade utilizados, com variações irrisórias comprometedoras dos resultados gerados.

Gostaríamos de ressaltar que os resultados documentados nas seções 6.1.2 e 6.1.3 para os três algoritmos avaliados não necessariamente irão repetir-se quando os algoritmos biométricos fizerem parte de um sistema biométrico como um todo. Para uma avaliação mais aprofundada, de forma a garantir os resultados para um produto comercial, sugerimos aos desenvolvedores que agregassem seu algoritmo a um pacote de software biométrico e produzissem as documentações necessárias. Assim, com um pacote de software biométrico, poderíamos aplicar a metodologia apresentada no capítulo 4 desta dissertação.

6.1.3. Avaliando o Algoritmo AKey1

Nós utilizamos os mesmos passos da seção 6.1.2 para avaliar o algoritmo AKey1. As tabelas 6.5 e 6.6 mostram as escalas configuradas de seus respectivos parâmetros de qualidade. Para configurá-las, fizemos uma consulta a diversas referências [60, 68, 77, 78, 79, 80, 81] envolvendo desempenho de algoritmos baseados em dinâmica da digitação para verificação pessoal.

Tabela 6.5: Escalas dos Parâmetros de Qualidade FFC, FTE e TSE para dinâmica da digitação

Escala \ Parâmetros		FFC	FTE	TSE
100%	**Excelente**	$v \leq 3\%$	$v \leq 1\%$	$v \leq 10$
	Bom	$3\% < v \leq 6\%$	$1\% < v \leq 3\%$	$10 < v \leq 15$
50%	**Regular**	$6\% < v \leq 12\%$	$3\% < v \leq 5\%$	$15 < v \leq 30$
0%	**Insuficiente**	$v > 12\%$	$v > 5\%$	$v > 30$

Tabela 6.6: Escalas dos Parâmetros de Qualidade ET e AT para dinâmica da digitação

Parâmetros / Escala		FFC		FTE	
		μ	σ	VERIFICAÇÃO μ	VERIFICAÇÃO σ
100%	**Excelente**	$v \leq 15s$	$v \leq 5s$	$v \leq 2s$	$v \leq 0.5s$
	Bom	$15s < v \leq 20s$	$5s < v \leq 10s$	$2s < v \leq 5s$	$0.5s < v \leq 1s$
50%	**Regular**	$20s < v \leq 30s$	$10s < v \leq 15s$	$5s < v \leq 8s$	$1s < v \leq 3s$
0%	**Insuficiente**	$v > 30s$	$v > 15s$	$v > 8s$	$v > 3s$

Os resultados da aplicação da ferramenta BioEVA para o algoritmo biométrico AKey1 são mostrados na segunda coluna da tabela 6.7. A tabela mostra também, na terceira coluna, o valor percentual que é o resultado do mapeamento dos valores da segunda coluna das tabela 6.7 nas escalas dos respectivos parâmetros de qualidade.

Tabela 6.7: Resultados da Avaliação para o Algoritmo AKey1.

PARÂMETROS DE QUALIDADE			AKey1	
			Resultados dos Testes	Valor Percentual Obtido
DIG			-	88.6%
CFF			3.1%	98.9%
FTE			0%	100%
TAC			8 amostras	100%
TC	μ		0.056 s	100%
	σ		0.03 s	
TA	**Verificação**	μ	0.022 s	100%
		σ	0.025 s	
NOTA FINAL				97.90%

Calculando a média dos valores obtidos na terceira coluna na tabela 6.7, resulta na nota final do algoritmo biométrico AKey1 que foi igual a 97.90%. De acordo com os valores de limiar estabelecidos na tabela 4.3, AKey1 é considerado um algoritmo biométrico nível A (alta qualidade e eficiência). Este valor para o algoritmo biométrico AKey1 é o resultado produzido em uma avaliação de qualidade aplicando a ferramenta BioEVA.

6.2. Aplicação da Metodologia na Avaliação do Pacote de Software Biométrico NS

O pacote de software biométrico avaliado nesta seção foi submetido externamente: uma empresa colaborou conosco submetendo-o para uma avaliação de qualidade de acordo com a metodologia apresentada. Este pacote é baseado na autenticação pessoal utilizando assinaturas estáticas. Nós iremos nos referir a ele, deste ponto em diante, como NS.

Seguindo o esquema apresentado na figura 4.1, nós aplicamos primeiro o processo (3) - (Extração de Informação), de forma a coletar as informações relacionadas ao fabricante e ao seu produto (processos (1) e (2) – Fornecedor e Pacote de Software, respectivamente). Baseados nestas informações, nós investigamos se alguma avaliação anterior foi aplicada no pacote ou em alguma de suas versões anteriores, caso houvesse uma. Além disso, a partir destas informações, também poderíamos enquadrar o pacote em um nível de rigor. Em suma, as informações mais importantes coletadas foram:

- O pacote NS é composto por um CD que contém o seu programa de instalação e um pequeno manual;

- O manual contém informações básicas sobre o processo de instalação e como utilizar as principais funções presentes no sistema;

- Os clientes em potencial são bancos e, principalmente, cartórios;

- O sistema utiliza o banco de dados Interbase-SQL, que suporta uma arquitetura do tipo Cliente/Servidor;

- Nenhuma avaliação anterior foi aplicada ao pacote NS, além de que esta é a primeira versão do produto.

Como nenhuma avaliação anterior foi aplicada ao pacote NS, e esta é a primeira versão do produto, nenhum tipo de conhecimento prévio ou procedimento pôde ser reaproveitado na avaliação atual. O pacote foi classificado no nível C (processo (4) – Seleção do Nível de Rigor), de

acordo com as características e informações apresentadas sobre o pacote NS, e seguindo as orientações da tabela 4.1, o que foi acordado pelo fabricante via Acordo Comum.

Aplicando o processo (5) – Seleção de Atributos, selecionamos um total de 30 atributos para avaliar o pacote, de acordo com o nível de rigor mínimo presente nas suas respectivas documentações. Esta lista de atributos foi registrada no Acordo Comum também, documento este gerado na aplicação do processo (6) - Especificação da Avaliação.

Quando construímos o documento Acordo Comum, além de incluir o nível de rigor e a lista dos atributos que serão utilizados na avaliação, introduzimos também os pesos que são atribuídos aos subsistemas biométricos e documentações, para que também sejam debatidos junto ao fornecedor do pacote NS. Os pesos dos subsistemas biométricos e das documentações são mostrados na figura 6.1, na forma de valores numéricos, que foram acordados pelo fabricante do pacote NS via Acordo Comum.

Na construção do Acordo Comum, foram detectados alguns problemas no pacote NS:

1 – O pacote NS não possuía qualquer tipo de equipamento representativo do Subsistema de Coleta de Dados. Os usuários do pacote deveriam possuir as imagens das suas assinaturas no computador aonde o pacote foi instalado, porque o sistema não possuía nenhum equipamento para capturar automaticamente estas amostras. O desenvolvedor as coleta em um papel, digitaliza-as e gera imagens a partir delas, armazenando-as no sistema ao final.

2 – O sistema não fazia uso da arquitetura Cliente/Servidor suportada pelo banco de dados. O sistema é instalado localmente.

3 – Nenhum tipo de mecanismo de adaptação das características biométricas foi utilizado. As assinaturas mudam com o decorrer do tempo e os templates armazenados no banco de dados precisam ser atualizados.

4 – O processo de instalação fatalmente não será completo: sem um equipamento para capturar automaticamente as amostras das assinaturas e sem utilizar uma arquitetura distribuída, nós não podemos mensurar o grau de dificuldade e de conhecimento reais necessários para completar uma instalação do produto com sucesso, sob este aspecto.

O próximo passo, após a conclusão do Acordo Comum e de sua discussão com o fornecedor do pacote NS, foi selecionar um grupo de cinco avaliadores. A ISO/IEC estabelece um mínimo de 4 avaliadores para aplicar uma avaliação confiável [3]. A tabela 6.8 mostra as respectivas áreas e graduações dos avaliadores selecionados. Uma vez selecionados os avaliadores, nós aplicamos o processo (8) - Aplicação de QIPEs: cada avaliador respondeu os questionários relacionados a cada um dos atributos selecionados. Como resultado da aplicação do processo (9) – Cálculo dos Pesos, cada avaliador recebeu seu peso representativo do grau de experiência e conhecimento nas definições envolvidas em cada atributo.

Tabela 6.8: Áreas do Conhecimento e Graduação dos Avaliadores

AVALIADORES	ÁREAS	FORMAÇÃO
I	Reconhecimento de Padrões, Engenharia de Software	Mestrando
II	Reconhecimento de Padrões, Banco de Dados	Mestrando
III	Reconhecimento de Padrões, Otimização	Doutor
IV	Engenharia de Software	Mestre
V	Engenharia de Software, Reconhecimento de Padrões	Graduado

Um mês foi necessário para aplicar a avaliação no pacote (processo (10) – Aplicação da Avaliação), de acordo com as especificações de avaliação presentes na documentação dos atributos. Cada avaliador concedeu uma nota para cada atributo de acordo com a sua respectiva escala. Com estas notas, calculamos as notas de cada subsistema e a nota das documentações. A figura 6.1 mostra as notas em valor percentual de cada subsistema e das documentações.

Usando os valores apresentados na figura 6.1, nós calculamos a nota do pacote de software NS, de acordo com os procedimentos apresentados na seção 4.7, que foi igual a 64.16%. Usando o valor de limiar para o nível C, apresentado na tabela 4.3, que é igual a 85%, o pacote NS não foi aprovado para o nível C.

Fazendo uso do processo (7) - Mudança de Variáveis Ambientais, nós modificamos o nível de rigor do pacote NS, reduzindo-o para o nível D. Esta mudança excluiu 6 dos atributos utilizados na avaliação no nível C, de acordo com o nível mínimo presente na documentação de cada atributo, e reduziu o rigor do processo de avaliação orientado pela especificação da avaliação dos atributos restantes, para o caso daqueles que possuem sua especificação da avaliação orientada

pelo nível de rigor. Dos 30 atributos utilizados, sobraram 24 atributos para recalcular a nota do pacote NS. Os atributos que tem sua especificação orientada por nível são reavaliados pelos avaliadores, pois o rigor com que deve ser aplicado foi reduzido. Portanto, de acordo com as modificações realizadas, a nota final do pacote de *software* biométrico NS subiu para 71.02%. Usando o valor de limiar para o nível D apresentado na tabela 4.3, que é igual a 80%, o pacote NS também não foi aprovado para o nível D.

Fazendo uso do processo (7) – Mudança de Variáveis Ambientais novamente, nós reduzimos o nível de rigor do pacote NS para o nível E. Esta mudança excluiu 8 dos atributos utilizados na avaliação no nível D, restando no total 16 atributos. Neste caso, seguiu-se o mesmo procedimento realizado para o caso da redução do nível de rigor da avaliação de C para D. A nota final do pacote de *software* biométrico NS subiu para 78.68%. Usando o valor de limiar para o nível E apresentado na tabela 4.3, que é igual a 70%, o pacote NS foi aprovado para o nível E.

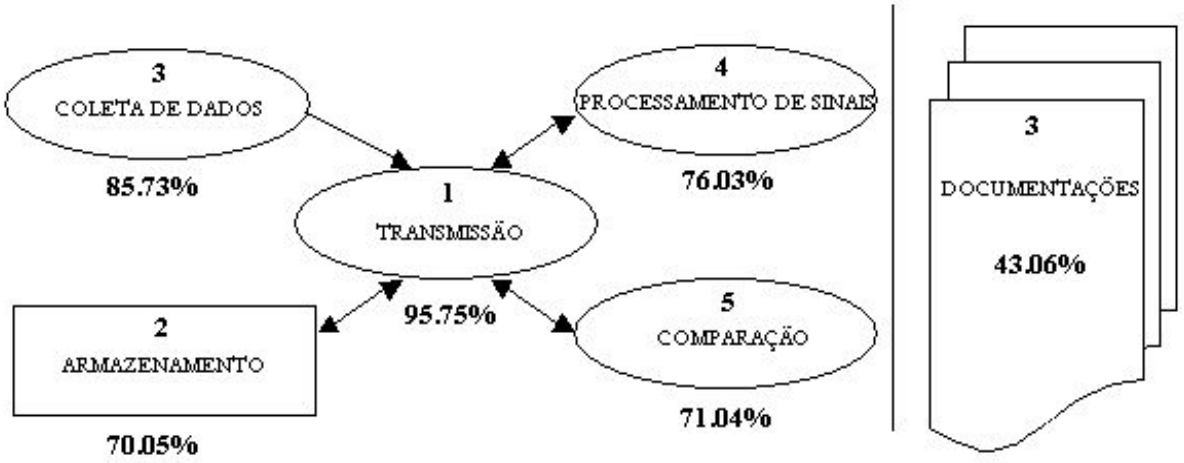


Figura 6.1: Notas e Pesos Atribuídos aos Subsistemas Biométricos e Documentações

As notas obtidas nos três níveis de rigor apresentados (C, D e E) refletem as deficiências reais do pacote de software biométrico NS: ele é ainda um protótipo e necessita de mudanças substanciais antes de tornar-se um produto comercial. A seguir, nós apresentamos os principais problemas encontrados no pacote NS, classificado por subsistema e documentação:

1) Subsistema de Coleta de Dados:

- Este subsistema não possui qualquer tipo de equipamento para capturar automaticamente as amostras de assinaturas estáticas dos usuários. Desta forma, as amostras têm de ser armazenadas localmente, o que torna os processos de cadastramento e autenticação lentos e custosos;

- Não existe um controle do sistema baseado em privilégios. Qualquer usuário pode utilizá-lo como um administrador, por exemplo.

2) Subsistema de Comparação:

- As taxas de FRR e FAR são muito altas. O fornecedor informou que as taxas do sistema estavam em torno de 4% FAR e 3% FRR. Porém, nos testes que foram realizados, o pacote apresentou uma taxa de FAR de 9% e uma taxa de FRR de 5%. Esta situação causa problemas sérios de segurança, como por exemplo, a facilidade da aplicação de ataques do tipo Zero Effort [38];

- O pacote está fora da realidade do seu potencial consumidor. Os algoritmos baseados em assinaturas estáticas, para bancos, necessitam de um erro de falsa aceitação (FAR) de 1 para cada 100.000 tentativas [76]. Além disso, o pacote apresenta processos lentos e semi-automáticos, e para a aplicação prática a qual o pacote NS se propõe necessita de soluções mais eficientes.

3) Subsistema de Processamento de Sinais / Extração de Características:

- Técnicas simples de processamento de imagens neste subsistema provavelmente foram utilizadas, o que justifica, em parte, as altas taxas de FAR e FRR apresentadas;

- Notamos que, nos testes realizados com o pacote, o sistema apresentava problemas de autenticação quando as assinaturas eram escritas com canetas de cores mais claras ou escuras do que aquelas utilizadas no conjunto de treinamento. Esta mesma observação pode ser notada em casos da caneta apresentar uma ponta mais fina ou mais grossa.

4) Subsistema de Armazenamento:

- Nenhum tipo de mecanismo de adaptação foi implementado, ou seja, nenhum tipo de atualização será aplicada aos *templates* no banco de dados com o passar do tempo;

- Nenhum tipo de criptografia foi implementada para proteger as informações dos usuários no banco de dados;

- Nenhum tipo de gerenciamento de acesso às informações no banco de dados baseado em privilégios foi implementado. Qualquer usuário pode ter acesso a estas informações como um administrador.

5) Subsistema de Transmissão:

- Todas as informações, seja armazenada ou circulante, permanecem localmente, o que não é desejado para o tipo de aplicação prática a qual o pacote se propõe;

- O pacote faz uso de um SGBD (Sistema Gerenciador de Banco de Dados), mas o fornecedor não utiliza nenhum tipo de arquitetura distribuída.

6) Documentações:

- As documentações não são claras e apresentam-se um pouco confusas, quando tentam explicar como utilizar as principais funcionalidades do pacote;

- O manual de instalação é básico: se o usuário tiver problemas no decorrer da instalação, muitas das soluções com certeza não estarão lá. Algumas palavras são ambíguas, e outras nem mesmo possuem uma definição no decorrer do manual;

- O pacote não apresenta *help on-line*, nem mesmo *off-line*;

- O suporte não está identificado nas documentações, e o número do telefone apresentado nelas raramente apresentou um suporte técnico capacitado;

Relacionado ao pacote NS como um todo, como o processo de instalação é muito simples, não é possível mensurar realmente qual o verdadeiro grau de conhecimento e quais são os problemas que o seu potencial consumidor encontrará ao instalá-lo completamente. Entende-se por completamente, a presença de um mecanismo de captura automática das assinaturas, a presença de uma arquitetura distribuída e a implementação dos elementos citados anteriormente que se apresentaram deficientes no pacote.

Baseados nos problemas apresentados e fazendo uso do processo (11) – Relatório, um relatório padrão foi entregue ao fabricante, construído conforme apresentado no capítulo 4 (4.8). O fabricante, por sua vez, propôs-se a corrigir os problemas apresentados conforme as orientações presentes neste documento.

CAPÍTULO 7

CONCLUSÕES

Neste capítulo apresentamos alguns comentários sobre o nosso trabalho, enfatizando as contribuições oferecidas e os trabalhos futuros que podem ser desenvolvidos a partir dele nesta dissertação.

7.1 CONTRIBUIÇÕES

Neste trabalho apresentamos uma metodologia para avaliação de pacotes de software biométricos e, derivada desta metodologia, uma ferramenta que denominamos BioEVA, cujo principal objetivo é promover a avaliação qualitativa e comparativa de algoritmos biométricos, de uma forma objetiva e automatizada.

A metodologia foi implementada utilizando as mais diversificadas fontes de pesquisa sobre padronizações internacionais, numa tentativa de unificar o que há de importante nestes trabalhos, e montar um esquema robusto que possa suportar a avaliação de qualquer pacote de software biométrico. Diante de tantas padronizações que divergem sobre qual o foco que deve ser dado para qualidade em sistemas biométricos, procuramos ter uma visão mais generalizada sobre o assunto, uma visão de cima para baixo, ao invés de focar somente em alguma característica, aspecto ou componente dos sistemas biométricos atuais (visão de baixo para cima), como fazem a maioria dos órgãos de padronização atuais.

Foi desenvolvida uma ferramenta que permite avaliar algoritmos biométricos como uma "*black-box*" e sem a intervenção humana, o que exclui os critérios subjetivos e permite a aplicação

de uma avaliação imparcial. Três módulos foram desenvolvidos para auxiliar nesta tarefa: cadastramento, autenticação e avaliação. Os módulos de cadastramento e autenticação possibilitam a realização de testes utilizando uma base de dados com amostras coletadas sob a especificação do desenvolvedor do algoritmo biométrico no acordo comum, e os resultados destes testes são armazenados em arquivos. Estes arquivos serão utilizados pelo módulo de avaliação para automatizar e agilizar o processo de avaliação dos algoritmos biométricos submetidos. Dessa forma, os algoritmos desenvolvidos no LRPRC da UNICAMP podem utilizar a ferramenta para realizar testes de qualidade em seus algoritmos, bastando obedecer às regras de submissão e configurar as escalas dos parâmetros de qualidade para adaptá-las ao tipo de tecnologia biométrica implementada.

Uma característica importante da metodologia é oferecer uma relação intrínseca e robusta entre os seus elementos componentes, garantindo que o resultado final seja um resultado confiável, tanto para o fabricante quanto para os avaliadores. Já uma característica importante da ferramenta BioEVA é implementar um ambiente que serve de teste e avaliação de qualidade para qualquer algoritmo biométrico que obedeça às regras de submissão, cujos testes passam a ser mais rápidos, eficientes, automatizados e padronizados.

7.2 Discussão sobre a Metodologia

A metodologia proposta para avaliação de pacotes de software biométricos fornece uma descrição simples, robusta e ambiciosa sobre como avaliá-los. O esquema construído está de acordo com conceitos básicos e padronizações do universo de princípios e definições clássicas envolvendo tecnologias biométricas. Portanto, a metodologia apresenta-se flexível e adaptável, sendo utilizada tanto para avaliar pacotes de software baseados em tecnologias biométricas atuais quanto àquelas que serão inovações futuras, assim como agregar novos conceitos que venham a surgir com estas inovações.

Nós readaptamos o modelo hierárquico top-down ISO/IEC 9126, criando um novo modelo hierárquico baseado na subdivisão de um sistema biométrico em subsistemas, conjuntamente com a definição de pacotes de software e suas documentações presentes na norma ISO/IEC 12119. Este novo modelo possibilita uma visão sobre quais são os pontos fortes e fracos do pacote de software avaliado, assim como possibilita avaliá-lo como um todo. Assim, possibilitamos uma maior clareza das informações geradas por uma avaliação de qualidade, pois,

por exemplo, no caso do modelo ISO/IEC 9126, as características de qualidade não são diretamente mensuráveis e os resultados gerados não são claramente inteligíveis.

Usando a idéia de aplicação de QIPEs aos avaliadores conjuntamente com a especificação da avaliação presente na documentação de cada atributo, procuramos garantir que somente o conhecimento e a experiência dos avaliadores sejam utilizados na avaliação de qualidade de um pacote de software biométrico usando os atributos selecionados.

Utilizando o documento Acordo Comum, nós especificamos ao fabricante o processo de avaliação que será aplicado no seu pacote de software biométrico, permitindo a ele argumentar contra ou a favor à respeito dos procedimentos que serão utilizados. Este documento é direcionado para a idéia de não beneficiar ou prejudicar a avaliação de um pacote software biométrico. Um modelo de documento Acordo Comum é apresentado na figura 4.5.

Os níveis de rigor foram adaptados para atender também aos aspectos biométricos que estão envolvidos com as tecnologias biométricas atuais, e são utilizados conjuntamente com os aspectos financeiros em caso de falhas no software.

Os modelos de documento de atributos e relatório padrão vão auxiliar como base para abrigar as definições envolvidas na documentação de um atributo e nos resultados da avaliação de um pacote de software biométrico, respectivamente. Ambos foram apresentados nas figuras 4.7 e 4.8, respectivamente.

Aplicando todos os passos da metodologia (figura 4.1) e aplicando a avaliação no pacote de software biométrico que denominamos NS, podemos acompanhar os resultados gerados pela metodologia na prática e observar, num caso real, o seu comportamento nos diversos passos do seu esquema. O resultado final, que definiu este pacote no nível E, mostrou que a metodologia comportou-se conforme o esperado, classificando o pacote como um protótipo, sujeito a severas alterações de acordo com os problemas apontados no decorrer da avaliação.

7.3 Discussão sobre a Ferramenta BioEVA

A ferramenta implementa uma idéia de avaliação automatizada e objetiva. Três módulos foram implementados para realizar o cadastramento, autenticação e avaliação de algoritmos biométricos.

Conseguimos criar um conjunto de regras de submissão (protocolo de submissão) de um algoritmo biométrico para avaliação pela ferramenta que fossem simples e que reduzisse os

esforços empregados pelo desenvolvedor na adaptação do seu algoritmo biométrico. Uma vez que o algoritmo se enquadrasse nessas regras, poderíamos inserir uma chamada à biblioteca que contém as funções de cadastramento e autenticação do algoritmo. Assim, habilitamos os módulos de cadastramento e autenticação para inicializar os testes.

Foram definidos 6 parâmetros de qualidade: Distribuição Impostor/Genuíno (IGD), Curvas de FAR/FRR (FFC), Tempo de Cadastramento (ET), Tempo de Autenticação (AT), Falha ao Cadastrar (FTE – *Failure To Enroll*) e Total de Amostras no Cadastramento (TSE). Eles são utilizados com o objetivo de testar e avaliar a eficiência e o desempenho de algoritmos biométricos. Os parâmetros de qualidade utilizados foram configurados de acordo com as referências e as características do tipo de tecnologia biométrica implementada no algoritmo biométrico avaliado. O desvio padrão é um novo valor de qualidade mencionado nesta dissertação e está presente nos parâmetros de qualidade AT e ET, e fornece informações relevantes a respeito da estabilidade dos algoritmos biométricos relacionadas aos tempos médios de cadastramento e autenticação que foram calculados. A BioEVA é capaz de realizar a avaliação de algoritmos biométricos tanto do tipo *single* quanto *multimodal*

Este trabalho melhorou vários aspectos apresentados na FVC. Os *skeletons* foram removidos para reduzir os esforços empregados pelos desenvolvedores no processo de submissão. Isto permitiu-nos a vantagem de um processo avaliativo independente da linguagem de programação no qual o algoritmo biométrico foi construído. Um documento formal foi estabelecido, chamado Acordo Comum, permitindo ao desenvolvedor formalizar e argumentar a respeito das características das amostras que serão utilizadas nos testes do seu algoritmo biométrico. Três interfaces foram implementadas na plataforma Java 2 (cadastramento, autenticação e avaliação), resultando em uma solução mais eficiente e dinâmica na avaliação de algoritmos biométricos. BioEVA também oferece independência de plataforma: os algoritmos podem ser recebidos, além de arquivos JAR, como *library files* produzidos nas suas respectivas plataformas, ou seja, no Windows, Macintosh, Solaris e Unix, por exemplo. A Máquina Virtual Java (JVM) e a tecnologia presente no Java Native Interface (JNI) fornecem esta vantagem.

Nós avaliamos três algoritmos de acordo com sua eficiência e desempenho: dois baseados em assinaturas estáticas para a autenticação pessoal e um baseado em dinâmica da digitação para verificação pessoal. Além disso, nós utilizamos BioEVA para comparar os dois algoritmos biométricos baseados em assinaturas estáticas (ASig1 e ASig2), uma vez que fizemos uso do mesmo ambiente de testes e da mesma base de dados para ambos. Nós observamos que, baseados

nos parâmetros de qualidade utilizados, o algoritmo ASig1 teve seus pontos fortes e fracos revelados, e os algoritmos ASig2 e AKey1 tiveram um excelente desempenho.

7.4 Perspectivas para Novos Trabalhos

Com relação à metodologia, é interessante desenvolver alguns estudos específicos:

1) QIPEs: desenvolver questionários envolve uma tarefa complexa sobre um tema específico. A importância que vinculamos aos questionários merece uma exploração mais aprofundada deste tema. As definições dos atributos aos quais um questionário estará vinculado devem traduzí-las muito bem, já que o objetivo de sua aplicação é extrair o conhecimento e a experiência dos avaliadores sobre os conceitos envolvidos em um determinado atributo.

2) Atributos: Nem todos os atributos foram especificados completamente, pois alguns deles envolvem além de conhecimentos teóricos, a experiência prática. Portanto, muitos deles podem influenciar trabalhos de suma importância para avaliação de qualidade de tecnologias biométricas. Além disso, um conjunto maior de atributos faz-se necessário para garantir uma maior confiabilidade nos resultados e uma abordagem maior sobre outras características de um pacote de software biométrico.

3) Realização de mais testes com um conjunto maior de pacotes de software biométricos. Dessa forma, correções podem ser feitas com base nos resultados práticos e o amadurecimento da metodologia torna-se iminente.

4) MEDE-PROS [82]: Este trabalho foi motivado pela crescente demanda de serviços para avaliação de produtos de *software* na área de tecnologia da informação nos últimos anos. Nele foi desenvolvido um ambiente para avaliação de qualidade de produtos de software (AAPQS). Para auxiliar este ambiente, ele foi baseado em uma Base de Dados de Avaliações onde estão armazenados os dados sobre as avaliações atuais e anteriores em diversos produtos de *software*, o que permite, por exemplo, reaproveitar avaliações passadas. Este trabalho pode apoiar uma linha de pesquisa para o desenvolvimento de processos sistemáticos para seleção de atributos e seus respectivos processos de avaliação. Além disso, este trabalho pode auxiliar no desenvolvimento de

um ambiente para avaliação de pacotes de *software* biométricos que permitirá uma automatização de grande parte dos procedimentos envolvidos no esquema de aplicação da metodologia, tornando-a mais eficiente e automatizada.

Com relação à ferramenta BioEVA, estudos devem proporcionar a incorporação de mais parâmetros de qualidade, relacionados com a avaliação de algoritmos biométricos. Além disso, é interessante que algoritmos biométricos baseados em outros tipos de tecnologias biométricas também sejam avaliados, gerando uma contribuição maior sob o ponto de vista da análise, em termos práticos, dos resultados gerados. Além disso, estas avaliações levam à tona a discussão a respeito de que parametrizações cada tecnologia biométrica deveria seguir de acordo com as sua vantagens, desvantagens e características particulares.

Podemos citar também como trabalho futuro para a ferramenta BioEVA a utilização de uma base única (como a FVC) e a realização de uma competição (como um desafio), no qual os desenvolvedores de algoritmos biométricos tentariam, nesta competição, obter o melhor resultado possível dentro de determinados parâmetros previamente selecionados utilizando uma base de dados confiável, como por exemplo àquelas disponibilizadas pelo NIST (*National Institute of Standard and Technology*).

REFERÊNCIAS BIBLIOGRÁFICAS

[1] Belasco, J. A., Stayer, R. C.: O vôo do búfalo: decolando para a excelência, aprendendo a deixar os empregados assumirem a direção. Editora Campus, Rio de Janeiro, 1994.

[2] Barreto Júnior, J., 2002, "Qualidade de *Software*". [*on-line*] Disponível na internet via *Web*. URL: http://www-usr.inf.ufsm.br/~oliveira/elc311/qualidadeSW.html. Arquivo consultado em 15 de outubro de 2003.

[3] Koscianski, A., Villas-Boas, A., Rêgo, C.M., Asanome, C., Scalet, D., Romero, D., Cieslak, J.M., Paludo, M., Frossard, R.S., Vostoupal, T.M., "Guia para Utilização das Normas sobre Avaliação de Qualidade de Produto de Software - ISO/IEC 9126 e ISO/IEC 14598", Associação Brasileira de Normas e Técnicas (ABNT), Subcomitê de Software (SC10), Maio, 1999.

[4] Belchior, A. D. Controle da Qualidade de Software Financeiro. Tese de Mestrado, COPPE/UFRJ, Rio de Janeiro, Julho, 1992.

[5] Bowman, E., "Everything You Need to Know About Biometrics", Identix Corporation, Final Report, January, 2002.

[6] Mansfield, T., Roethenbaugh, G., 1998, "Glossary of Biometric Terms". [*on-line*] Disponível na internet via *Web*. URL: http://www.afb.org.uk/public/glossuk1.html. Arquivo consultado em 20 de maio de 2002.

[7] Pressman, R.S.: Engenharia de Software. Makron Books, São Paulo, 1995.

[8] Rezende, D. K., "Um Modelo de Avaliação de Qualidade de Software voltado para Especificações Orientadas a Objetos", Artigo de Mestrado, Universidade Católica de Brasília (UCB), Goiânia, Novembro, 2000.

[9] Vermesan, A.I., "Some Certification for Industry - Verification and Validation Issues in Expert Systems", *Nineth International Workshop on Database and Expert Systems Applications*, pp. 03-14, 1998.

[10] Strigini, L., "Limiting the Dangers of Intuitive Decision Making", *IEEE Software*, January, 1996.

[11] Humphrey, W. S.: A Discipline for Software Engineering. Addison-Wesley, MA, 1995.

[12] Oliveira, A. M. et al., "Avaliação de Processos de Software: Modelos e o TAQS-PROC", *Workshop de Qualidade de Software*, *IX SBES*, Recife, 1995.

[13] International Organization for Standardization: ISO/IEC/12207: information technology - software life cycle processes. Geneve : ISO, 1995.

[14] Paulk, Mark et al.: The Capability Maturity Model (CMM): Guidelines for improving the software process. Addison-Wesley, Software Engineering Institute (SEI), 1995.

[15] Sanders, J., Curran, E.: Software Quality. ACM Press Books, Dublin, 1994.

[16] Humphrey, W. S. et al., "Software Process Improvement at Hughes Aircraft", *IEEE Software*, July, 1994.

[17] Weber, K. C., DeLuca, J. C. M., Rocha, A. R. C.: Qualidade e Produtividade em Software: Termo de Referência do Subprograma Setorial da Qualidade e Produtividade em Software, do Programa Brasileiro da Qualidade e Produtividade – PBQP. Makron Books, 2ª Edição, São Paulo, 1997.

[18] Bache, R., Bazzana, G.: Software Metrics for Product Assessment. Mc Graw Hill Book Company, 1994.

[19] Kuvaja, P. et al.: Software Process Assessment & Improvement - The Bootstrap Approach. Blackwell Publishers, Oxford, 1994.

[20] Bell Canada Inc., "Trillium: Model for Telecom Product Development and Support Process Capability", release 3.0, December, 1994.

[21] Olivé, A., Sancho, M. R., "Validating Conceptual Specifications through Model Execution", *Information Systems*, Vol. 21, no.2, pp. 167-186, 1996.

[22] Scalet, D., "Avaliação da Qualidade do Produto de Sotfware", *Workshop da Qualidade e Produtividade em Software*, *IX SBES/SBC*, Recife, Outubro, 1995.

[23] Strigini, L., "Limiting the Dangers of Intuitive Decision Making", *IEEE Software*, January, 1996.

[24] Basili, V., Rombach, H. D., "Tailoring the Software Process to Project Goals and Environments", Department of Computer Science, University of Maryland, ACM, 1997.

[25] Basili, V. R., 1992, "Software Modeling and Measurement: The Goal Question Metric Paradigm", *Computer Science Technical Report Series,* CS-TR-2956 (UMIACS-TR-92-96), University of Maryland, College Park, MD.

[26] J. Boegh, H.-L. Hausen, D. Welzel, "A Practioners guide to Evaluation of Software", *in Proc. of the IEEE Software Engineering Standards Symposium*, 1993.

[27] Bazzana, G. et al., "ISO 9126 and ISO 9000: Friends or Foes?", *Software Engineering Standards Symposium*, Brighton, UK, 1993.

[28] Rocha, A. R. C. Um Modelo para Avaliação da Qualidade de Especificações. Tese de Doutorado, PUC-RJ, Rio de Janeiro, 1983.

[29] ISO/IEC/JTC 1/SC 7. Information Technology – Software Product Quality – Quality Characteristics and Guidelines for Their Use. ISO/IEC 9126 International Standard, 1991.

[30] ISO/IEC/JTC 1/SC 7. Information Technology – Software Product Evaluation. ISO/IEC 14598 International Standard, 1999.

[31] Koscianski, A., Costa, J.C.B., "Combining Analytical Hierarchical Analysis with ISO/IEC 9126 for a Complete Quality Evaluation Framework", *Fourth IEEE International Symposium and Forum on Software Engineering Standards*, session 9, pp. 218-226, Curitiba, Brazil, 1999.

[32] Tsukumo, A. N et al., "Avaliação incremental de Qualidade de Produto de Software baseada na ISO/IEC 9126 (NBR 13596)", *SBES'96 - Workshop de Qualidade*, São Carlos, 1996.

[33] Kitchenham, B. et al., "Software Quality: The Elusive Target", *IEEE Software*, January, 1996.

[34] GEQS/INSOFT, 1998, "Tradução Livre da Norma Internacional ISO/IEC 12119: Tecnologia da informação–Pacotes de software – Requisitos de qualidade e testes". [*on-line*] Disponível na internet via *Web*. URL:http://www.insoft.softex.br/qualidadeSoftware/biblioteca/normas/download/12119.pdf. Arquivo conultado em 10 de agosto de 2002.

[35] Holanda, A. A., "Dicionário Aurélio Eletrônico". [*on line*] Disponível na internet via *Web*. URL: http://www2.uol.com.br/aurelio. Página consultada em 18 de outubro de 2003.

[36] 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.

[37] Wood, H. M., "The use of passwords for controlled access to computer resources", National Bureau of Standards Special Publication 500-9, US Dept. Of Commerce/NBS.

[38] D. Polemi, 1997, "Biometric Techniques: Review and Evaluation of Biometric Techniques for Identification and Authentication, Including an Appraisal of the Areas Where They are Most Applicable," Final Report. [*on-line*] Disponível na internet via *Web*. URL: ftp://ftp.cordis.lu/pub/infosec/docs/biomet.doc. Arquivo consultado em 18 de outubro de 2003.

[39] Mathyas, S.M., Stapleton, J., "A biometric standard for information management and security", *Computers & Security*, vol.19, no.5, p.428-441, 2000.

[40] Newman, E., "The Biometric Report", SJB Services, UK, 1995.

[41] Davies, D. W., Price, W. L.: Security for Computers Networks. John Wiley & Sons, 1984.

[42] Chen, S., Jain, A., Ratha, N., "Adaptative flow orientation-based feature extraction in Figerprint images", *Pattern Recognition*, Vol. 28, Nº 11, pp. 1647 - 1672, 1995.

[43] Hrechak, A., McHugh, J., "Automated fingerprint recognition using structural matching", *Pattern Recognition*, Vol. 23, Nº 8, pp. 893 - 904, 1990.

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

[45] Botha, E., Coetzee, L., "Fingerprint recognition in low quality images", *Pattern Recognition*, Vol. 26, Nº 10, pp. 1441 - 1460, 1993.

[46] 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.

[47] Burgess, S.P., "Law Enforcement Networks Puts Finger on Fast-Footed Criminals", *SIGNAL*, October, 1996.

[48] Thalheim, L., Krissler, J., Ziegler, P.M., 2002, "Body Check", C'T Magazine. [*on-line*] Disponível na internet via *Web*. URL: http://www.heise.de/ct/english/02/11/114/. Arquivo consultado em 28 de agosto de 2003.

[49] Matsumoto, T., Matsumoto, H., Kamada, K., Hoshino, S., "Impact of Artificial "Gummy" Fingers on Fingerprint Systems", *Proceedings of SPIE*, vol. #4677, Optical Security and Counterfeit Deterrence Techniques IV, 2002.

[50] Daugman, J., "High confidence visual recognition of persons by a test of statistical independence", *Transactions on Pattern Analysis and Machine Intelligence*, Vol. 15, Nº 11, pp. 1148 - 1161, 1993.

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

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

[53] Marsh, P., "Biometric Behavior is smart and secure", *New Electronics*, pp.25-26, July, 1996.

[54] Shu, W., Zhang, D., "Automated personal identification by palmprint", *Optical Engeneering*, Vol. 37, Nº 8, 1998.

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

[56] Pentland, A., Choudhury T., "Face recognition for smart environments", *IEEE Computer Magazine*, Vol. 33, Nº 2, pp. 46 - 49 , 2000.

[57] Harmon L., Khan, K., Lasch, R., Ramig, P., "Machine identification of human faces", *Pattern Recognition*, Vol. 13. Nº 2, pp. 97 - 110, 1981.

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

[59] Araújo, L.C.F., Sucupira Jr., L. H. R., Lizarraga, M.G., Ling, L.L., Yabuuti, J.B.T., "A Fuzzy Logic Approach in Typing Biometrics User Authentication", *Proc. of 1st Indian International Conference on Artificial Intelligence*, Hyderabad, India, December, 2003.

[60] Joyce, R., Gupta G. "Identity authorization based on keystroke latencies", *Communications of the ACM*, Vol 33. Nº 2, pp 168 - 176, 1990.

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

[62] Rosenberg, A.,"Automatic speaker verification: a review". *Proceedings of IEEE*, Vol. 64, Nº 4, pp. 475 - 487, 1976.

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

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

[65] Lizárraga, M.G. Um Sistema Biométrico de Identificação Pessoal via Internet com ênfase em Assinaturas Estáticas. Tese de Doutorado, Unicamp, Agosto, 2000.

[66] Canadian Common Criteria Evaluation and Certification Scheme, "Biometric Technology Security Evaluation under de Common Criteria (CC)", *Doc No: 1351-036-D001*, 2001.

[67] Oliveira, K.L., Belchior, A.D., "AdeQuaS: Ferramenta *Fuzzy* para Avaliação de Qualidade de *Software*", Artigo de Mestrado em Informática Aplicada. [*on-line*] Disponível na internet via *Web*. URL: http://www.comp.ita.br/~cunha/download/CES63CE235-2002/Sem11/2_AS2-1%20AdeQuaS_Ferramenta%20Fuzzy%20para%20Avaliacao%20da%20Qualidade%20de%20Software.pdf. Arquivo consultado em 02 de agosto de 2003.

[68] Maio, D., Maltoni D., Cappelli R., Wayman J. L., Jain A. K., "FVC2002: Second Fingerprint Verification Competition", *Proc. of 16th International Conference on Pattern Recognition (ICPR2002)*, Quebec City, Vol. 3, pp. 811-814, 2002.

[69] United State of America Department of Defense, 1983, "Trusted Computer System Evaluator Criteria (TCSEC)", *DoD 5200.28-STD*. [*on-line*] Disponível na internet via *Web*. URL: http://www.radium.ncsc.mil/tpep/library/rainbow/5200.28-STD.html. Arquivo consultado em 13 de julho de 2003.

[70] Bundesamt für Sicherheit in der Informationstrchnik (BSI), 2000, "Technical Evaluation Criteria for the Assessment and Classification of Biometric Systems", *Draft version 0.5-1*. [*on-line*] Disponível na internet via *Web*. URL: http://homepage.ntlworld.com/avanti/bsi1.pdf. Arquivo consultado em 5 de junho de 2003.

[71] Tsukumo, A. N., Capovilla C., Rego C., Jino M., Maldonado J.C., "*ISO/IEC 9126:* An Experiment of application on Brazilian Software Products", *proceedings in 2nd IEEE Intern.Symposium and Forum on Software Engineering Standards*, 1995.

[72] Cappelli R., Maio D., Maltoni D., "Synthetic Fingerprint-Database Generation", in proceedings *16th International Conference on Pattern Recognition (ICPR2002)*, Quebec City, vol.3, pp.744-747, August, 2002.

[73] Purser, M. Secure Data Networking. Artech House, Boston, London, 1993.

[74] The BioAPI Consortium, 2001, "BioAPI Specification Version 1.1". [*on-line*] Disponível na internet via *Web*. URL: http://www.bioAPI.org/BIOAPI1.1.pdf. Arquivo consultado em 15 de setembro de 2003.

[75] Bundesamt für Sicherheit in der Informationstrchnik (BSI), 2000, "Technical Evaluation Criteria for the Assessment and Classification of Biometric Systems", *Draft version 0.5-1*. [*on-line*] Disponível na internet via *Web*. URL: http://homepage.ntlworld.com/avanti/bsi2.pdf. Arquivo consultado em 5 de junho de 2003.

[76] Plamondon R., Srihari, S. N., "On-Line and Off-Line Handwriting Recognition: A Compreensive Survey", *IEEE Transactions on Pattern Analysis and Machine Intelligence*, Vol. 22. Nº 1, pp. 63 - 84, 2000.

[77] De Ru, W. G., Eloff, J. H. P., "Enhanced Password Authentication through Fuzzy Logic", *IEEE Expert / Intelligent Systems & Their Applications*, Vol. 17, No. 6, pp. 38-45, 1997.

[78] Robinson, J. A., Liang, V. M., Michael, J. A., MacKenzie, C. L., "Computer User Verification Login String Keystroke Dynamics", *IEEE Trans. Syst., Man, Cybern.*, Vol. 28, No. 2, pp. 236-241, 1998.

[79] Lin, D.T, "Computer-Access Authentication with Neural Network Based Keystroke Identity Verification", *Proceedings of the International Conference on Neural Networks*, Vol. 1, pp. 174-178, 1997.

[80] Bleha, S., Slivinsky, C., Hussain, B., "Computer-Access Security Systems Using Keystroke Dynamics", *IEEE Trans. Pattern Anal. Machine Intell.*, Vol. 12, No. 12, pp. 1217-1222, 1990.

[81] Haidar, S., Abbas, A., Zaidi, A. K., "A Multi-Technique Approach for User Identification through Keystroke Dynamics", *IEEE Int. Conference of Syst., Man and Cybern.*, Vol. 2, pp. 1336-1341, 2000.

[82] Martinez M., Azevedo G., Lopes S., Pagliuso P., Colombo R., Rodrigues M., Jino M., "The Software Product Evaluation Data Base: Supporting MEDE-PROS", *Proceedings of the 4th IEEE International Symposium and Forum on Software Engineering Standards*, pp.182, 1999.

ANEXO I

PASSOS PRÁTICOS PARA APLICAÇÃO DA METODOLOGIA NA AVALIAÇÃO DE PACOTES DE SOFTWARE BIOMÉTRICOS

PASSO 1 – EXTRAÇÃO DE INFORMAÇÕES

Este passo compreende a extração de informações relacionadas ao fornecedor e ao seu pacote de *software* biométrico. Estas informações são extraídas em uma entrevista com o fornecedor. Na entrevista, devem ser extraídas, por exemplo, as seguintes informações:

- Nome e origem da empresa;
- Objetivos;
- Tipos de produtos desenvolvidos e serviços prestados;
- Avaliações de qualidade utilizadas pela empresa (produtos, processos e serviços);
- Mercado em que atua;

Informações sobre o pacote de *software* biométrico a serem extraídas devem incluir:

- Nome;
- Público-alvo e aplicabilidade prática;
- Tipo de tecnologia biométrica Implementada;
- Elementos de *hardware* e *software* que o acompanham;
- Documentações que o acompanham;
- Tipos de avaliações de qualidade realizadas em versões anteriores do pacote e em que componentes do pacote elas foram aplicadas;

Na avaliação do pacote de *software* biométrico NS, podemos citar algumas informações extraídas do fornecedor, como:

- Uma empresa de consultoria e desenvolvimento de sistemas de computação;
- Atua no desenvolvimento de sistemas de apoio a decisão;
- Foi criada em 1996;
- Está sedimentada no desenvolvimento de ferramentas especializadas em Otimização e Controle de Recursos e Processos;
- Trabalha na consultoria e desenvolvimento de sistemas de apoio à decisão para uso doméstico ou pela internet dos tipos espaciais e/ou generalistas para transportadoras,

atacadistas, fábricas, bancos, imobiliárias, prefeituras e órgãos governamentais, universidades, empresas de comunicação, transportadores de pessoal;

Como informações do próprio pacote de software biométrico NS, podemos citar:

- Identifica os padrões encontrados em imagens de assinaturas estáticas;
- Faz uso do Banco de dados *Interbase-SQL*;
- Apresenta uma plataforma robusta para milhões de assinaturas;
- Foi desenvolvido utilizando a ferramenta Borland Delphi 5.0;
- Possibilita a customização de funções para atender fins específicos;
- Possibilita a utilização de uma arquitetura do tipo Cliente/Servidor;
- Aplicações Práticas envolvem principalmente Cartórios;
- O pacote é composto de um CD de instalação e um manual do usuário com o seu processo de instalação, suporte e manutenção;
- Nenhuma avaliação anterior foi aplicada ao pacote;
- O pacote está na versão 1.0.

PASSO 2 – SELEÇÃO DO NÍVEL DE RIGOR

Com base na tabela 4.1 apresentada no capítulo 4 (4.3) e utilizando as informações coletadas no passo anterior, deve-se enquadrar um pacote de software biométrico em um nível de rigor. Se as informações coletadas não forem suficientes para a conclusão deste passo, deve-se

retornar ao passo 1.

Como exemplo, para o caso do pacote de *software* biométrico NS, que foi enquadrado no nível C, podemos observar, de acordo com a tabela 4.1 e com as informações coletadas que:

- O nível B tem seu principal alvo produtos que estejam relacionados com transações financeiras ou que estão relacionadas com vidas humanas em ambientes de risco controlado. O próprio fornecedor achou este nível muito acima do seu produto, no Acordo Comum, ao observar os aspectos econômicos e biométricos apresentados. Seu alvo principal são cartórios, e, por isso, concordamos que os aspectos envolvidos neste nível estão muito acima do pacote NS;

- O nível D está abaixo do nível real do produto, mesmo porque suas aplicações práticas envolvem produtos que atingem o ambiente doméstico e *software* de entretenimento, que não envolvem muitos usuários ou causam prejuízos financeiros significativos. Desta forma, este nível não mensura o grau de abrangência no mercado para o pacote NS.

Logo, o nível C apresenta aspectos relacionados com a realidade do pacote NS. Em cartórios, a assinatura é um meio essencial para autenticar indivíduos. Identificar falsificações evita que problemas ocorram ao usuário do serviço e ao próprio cartório, assim como automatiza o processo, através de interfaces de cadastramento e autenticação e pela utilização de meios digitais de armazenamento. Os aspectos biométricos e financeiros apresentados no nível de rigor C refletem melhor o âmbito de aplicação prática do pacote NS.

PASSO 3 – SELEÇÃO DOS ATRIBUTOS

Os atributos serão selecionados inicialmente de acordo com o nível de rigor estabelecido no passo 2, a partir do nível de rigor mínimo estabelecido na documentação de cada atributo (figura 4.7). Todos os atributos que tenham o nível de rigor mínimo menor ou igual ao estabelecido no passo 2 são selecionados.

Para o pacote NS os atributos selecionados, portanto, teriam de ter os níveis de rigor apresentados nas suas respectivas documentações: E, D e C.

PASSO 4 – ESTABELECIMENTO DOS PESOS DOS SUBSISTEMAS BIOMÉTRICOS E DOCUMENTAÇÕES

De acordo com as informações extraídas do passo 1, estabelece-se o peso de cada um dos subsistemas biométricos e das documentações do pacote de software biométrico, conforme apresentados nas figuras 4.2 e 4.3, variando de 1 (menor peso) a 5 (maior peso).

O pacote de *software* biométrico NS obteve os seguintes pesos:

- Subsistema de Coleta: 3;
- Subsistema de Transmissão: 1;
- Subsistema de Processamento de Sinais: 4;
- Subsistema de Comparação: 5;
- Documentações: 3.

Cada uma das considerações para atribuições dos pesos é mencionada no capítulo 6 (6.2).

PASSO 5 – CONSTRUÇÃO DO ACORDO COMUM

O Acordo Comum é construído com base nas informações obtidas nos passos 2, 3 e 4. Este documento deve ser escrito de acordo com as especificações apresentadas no capítulo 4 (4.4) e de acordo com o modelo da figura 4.5. Uma cópia deve ser entregue ao fornecedor para que ele possa analisá-la e propor modificações no processo avaliativo. O próximo passo só terá início uma vez que o fornecedor tenha concordado com todos os quesitos apresentados no documento.

No caso do pacote NS, algumas concessões foram feitas com relação à avaliação do subsistema de coleta de dados, sob o aspecto dos elementos do passo 3. Como o produto não possuía nenhum tipo de mecanismo de captura automática das assinaturas, a avaliação foi

realizada como se ele existisse. Com relação aos elementos presentes nos passos 2 e 4, nenhuma modificação foi necessária.

PASSO 6 – SELEÇÃO DOS AVALIADORES

Pelo menos 4 avaliadores devem ser selecionados, de preferência que estão tendo ou já estiveram envolvidos com alguma atividade relacionada com biometria, independente de formação acadêmica.

5 avaliadores foram selecionados para a avaliação do pacote de *software* biométrico NS. A tabela 6.9 mostra o perfil dos avaliadores, em suma, selecionados.

PASSO 7 – APLICAÇÃO DE QIPES

Este passo envolve aplicar os QIPEs presentes na documentação dos atributos conforme apresentado no capítulo 4 (4.4) e de acordo com o modelo da figura 4.5. A estrutura e os elementos componentes dos QIPEs são apresentados no capítulo 4 (4.5). Os avaliadores não podem ter acesso a nenhum dos pesos (nem das questões ou das alternativas) nem aos objetivos de aplicação de uma determinada questão, apresentados na documentação dos atributos na seção dos QIPEs no capítulo 4 (4.4). Uma vez que o avaliador tenha respondido o QIPE relacionado a um atributo, o seu peso é calculado para àquele atributo, de acordo com o procedimento apresentado no capítulo 4 (4.5), utilizando as equações 1 e 2.

PASSO 8 – APLICAÇÃO DA AVALIAÇÃO

Cada avaliador selecionado no passo 6 utiliza os atributos selecionados no passo 3 para avaliar o pacote de software biométrico, utilizando a especificação da avaliação presente na documentação de cada um dos atributos conforme apresentado no capítulo 4 (4.4) e de acordo com o modelo da figura 4.5.

O avaliador concede uma nota de acordo com a escala do atributo, presente na documentação do atributo conforme apresentado no capítulo 4 (4.4) e de acordo com o modelo da figura 4.5.

Uma vez que todos os avaliadores selecionados no passo 6 tenham concedido suas notas para os atributos selecionados no passo 3, as notas de cada um dos subsistemas biométricos e de cada uma das documentações hierarquicamente superiores, de acordo com as figuras 4.2 e 4.3, devem ser calculadas. Este cálculo é realizado de acordo com a equação 3 no capítulo 4. Os pesos dos atributos são estabelecidos de acordo com o nível de rigor mínimo presente nas suas respectivas documentações (capítulo 4 (4.4) e figura 4.5): A = 5; B = 4; C = 3; D = 2; E = 1.

A nota do sistema biométrico e das documentações é calculada a partir das notas calculadas para os subsistemas biométricos e de cada uma das documentações, fazendo uso da equação 3 no capítulo 4. Os pesos da equação 3 são aqueles definidos no Acordo Comum no passo 5.

A nota do pacote de software biométrico é calculada a partir das notas calculadas do sistema biométrico e das documentações. O peso do sistema biométrico na equação 4 é sempre 5 e o das documentações é estabelecido de acordo com a primeira coluna da tabela 4.3.

PASSO 9 – DETERMINANDO O NÍVEL DE QUALIDADE DO PACOTE DE SOFTWARE BIOMÉTRICO

Utilizando a nota calculada no passo 8 do pacote de software biométrico determina-se o seu nível de qualidade de acordo com os valores de limiar estabelecidos na segunda coluna da tabela 4.3. O valor de limiar da segunda coluna da tabela 4.3 é selecionado a partir do nível de rigor do pacote de *software* biométrico estabelecido no passo 2.

Se a nota calculada no passo 8 for maior ou igual ao valor de limiar selecionado, o pacote de *software* biométrico é um pacote de qualidade. Caso contrário, ele não é aceito para aquele nível de rigor estabelecido no passo 2. Neste caso, um nível de rigor inferior deve ser selecionado.

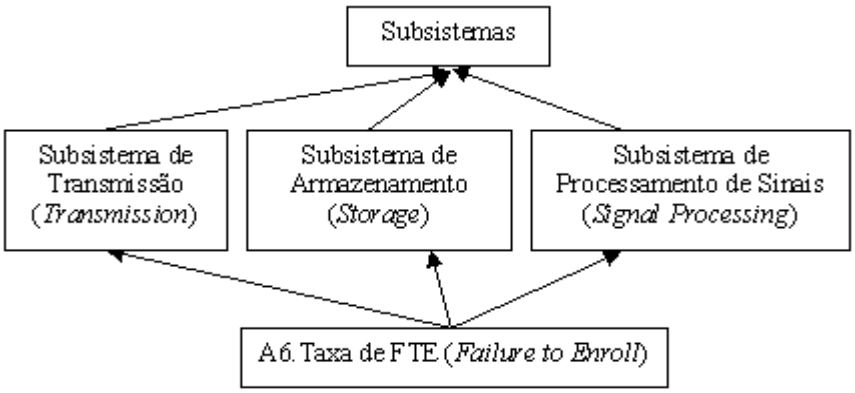
PASSO 10 – RELATÓRIO FINAL DE AVALIAÇÃO

Produzir um relatório de acordo com o modelo apresentado na figura 4.8 e com os procedimentos apresentados no capítulo 4 (4.8).

ANEXO II

EXEMPLO COMPLETO DE ESPECIFICAÇÃO DE UM ATRIBUTO

(A6) Atributo 6: Taxa de FTE (*Failure To Enroll*)



Definição: Atributo define a taxa de rejeição ou falha no cadastramento do usuário por quantidade de amostras apresentadas no cadastramento. [67]

Definição Detalhada: A taxa de rejeição é calculada a partir da quantidade de amostras que um usuário deve fornecer para completar o cadastramento no sistema e passar a ser parte dele. Falhas podem ocorrer durante o processo de cadastramento. Segundo [67] três tipos de erros podem ocorrer durante o cadastramento:

1. Falha: o sistema declara que não pode cadastrar a amostra biométrica apresentada;

2. Expiração de Tempo: o cadastramento ultrapassa o tempo-limite estabelecido (em [67] o tempo-limite é de 15 segundos);
3. Problemas de Processamento: o sistema apresenta problemas durante o processamento de uma amostra biométrica.

Processo de Avaliação:

• O objetivo é obter o percentual de falhas no cadastramento dado um número de usuários. Este percentual, por sua vez, deve ser classificado em cada um dos três tipos de erros apresentados no item Definição Detalhada deste atributo, ou seja, além do percentual de falhas do sistema, deve ser informada a fatia pertinente a cada tipo de erro deste percentual.

• O cálculo dessa taxa está diretamente ligado com a quantidade de pessoas que serão usuárias do sistema. Neste caso, para cada novo usuário o sistema não deve apresentar falhas em demasia, ou criará um gargalo, interferindo em outras atividades do sistema e/ou gerando insatisfação para os seus usuários.

• O sistema entregue pelo fabricante deve estar funcionando por completo após sua instalação antes do início dos testes. Um módulo deve acompanhar o sistema para realizar a geração dos percentuais citados. O sistema deve possibilitar o processamento completo de cadastramento de um usuário, e que vários usuários possam cadastrar-se consecutivamente no sistema.

• O módulo deve ser capaz de exibir essas taxas ao final de cada cadastramento para acompanhamento pelos avaliadores.

• O módulo deve ser capaz de incorporar o conceito do atributo apresentado.

• O módulo ou o sistema deve ser capaz de transparecer que parte do sistema apresentou a falha. Desta forma, o avaliador detectará o tipo de falha, aonde ocorreu, justificar seu enquadramento naquele tipo de falha, e qual a sua causa, para que ele possa fazer suas considerações.

• Caso um subsistema não tenha apresentado nenhuma falha, este não deverá ser penalizado no cálculo da nota. Ele é considerado como se tivesse peso 0, o que anula o cálculo da sua nota hierarquicamente, seguindo o cálculo de uma nota de um subsistema.

• Caso não seja possível detectar o tipo de falha, ela deve ser classificada como desconhecida, o problema deve ser descrito pelo avaliador, e ele deve justificar qual o motivo que o impediu de classificá-lo em algum tipo de erro, mas ela não pode deixar de ser contabilizada. Caso não seja possível detectar em que ponto do sistema a falha ocorreu, todo o sistema será penalizado, e o avaliador também deve descrever o problema ocorrido e porque não conseguiu enquadrá-lo.

Nível: C

Escala: A escala é utilizada da seguinte maneira:

1º – O avaliador identifica a quantidade de falhas de cadastramento apresentadas pelo sistema e os tipos de falhas apresentadas. Pelo comportamento dos usuários e pela freqüência e quantidade de erros o avaliador julga com relação aos critérios subjetivos apresentados.

2º – O avaliador identifica a compatibilidade do sistema com sua aplicabilidade prática a partir do comportamento dos usuários e do total de falhas e tipos de falhas. O avaliador então julga de acordo com os critérios subjetivos apresentados.

3º – As notas subjetivas são mapeadas nas suas respectivas notas objetivas. As notas objetivas obtidas nos itens 1º e 2º são somadas.

Elementos de Avaliação	Subjetivo	Objetiva
Quantidade de Falhas apresentadas pelo sistema pelo número de usuários.	Nenhuma	+50%
	Mínima	+40%
	Tolerável	+25%
	Considerável	+10%
	Inaceitável	0%
Compatibilidade com a Aplicabilidade Prática.	Sim	+50%
	Sim, porém com um número de falhas tolerável	+30%
	Sim, porém com um número de falhas considerável	+10%
	Não	+0%

QIPE (Questionário de Identificação do Perfil do Especialista):

Pergunta 1: Você (Avaliador) já possui alguma experiência em biometria, de qualquer tipo*?*

Alternativas (exclusivas):

1 – SIM. Valor Associado - 100

2 – NÃO. Valor Associado - 0

Objetivo: Saber se o avaliador teve participações em atividades envolvendo biometria.

Peso: 1 (Mínima relevância).

Pergunta 2: Você (Avaliador) participou em quantas atividades envolvendo biometria?

Alternativas (exclusivas):

1 – 0. Valor Associado - 0

2 – 1. Valor Associado - 20

3 – 2. Valor Associado - 40

4 – 3. Valor Associado - 60

5 – 4. Valor Associado - 80

6 – 5 ou mais. Valor Associado - 100

Objetivo: Extrair a experiência do avaliador em atividades práticas envolvendo biometria. Quanto mais participações ele possuir nessas atividades, então gradativamente o valor percentual que representa e resume sua experiência nessas participações é aumentado.

Peso: 2 (Pouco Relevante).

Pergunta 3: Em que atividades envolvendo biometria você (Avaliador) já participou?

Alternativas (cumulativas):

1 – Gerência de Projetos. Valor Associado: 50

2 – Analista de Sistemas. Valor Associado: 150

3 – Projetista. Valor Associado: 100

4 – Programador. Valor Associado: 50

5 – Usuário. Valor Associado: 50

6 – Pesquisas na área de Biometria. Valor Associado: 150

7 – Pesquisas e desenvolvimento de Produtos de *Software* Biométricos. Valor Associado: 150

8 – Pesquisas em avaliação de *performance* de algoritmos biométricos. Valor Associado: 300

9 – Avaliação de Produtos de *Software* Biométricos. Valor Associado: 250

10 – Avaliação de Produtos de *Software* em geral. Valor Associado: 100

11 – Coordenação de grupo de pesquisa em Biometria. Valor Associado: 100

Objetivo: Conhecer a experiência profissional em algumas atividades envolvendo biometria que o avaliador já tenha participado. Cada uma delas tem o seu grau de importância relacionado com as demais.

Peso: 3 (Relevante).

Pergunta 4: Quais taxas e medidas de desempenho de sistemas biométricos você (avaliador) conhece teoricamente?

Alternativas (cumulativas):

1 – Distribuição Discreta de Genuínos (*Genuine Matching Scores*). Valor associado: 100

2 – Distribuição Discreta de Impostores (*Impostor Matching Scores*). Valor associado: 100

3 – FMR (*False Match Rate*) ou FAR (*False Acception Rate*). Valor associado: 100

4 – FNMR (*False Non-Match Rate*) ou FRR (*False Rejection Rate*). Valor associado: 100

5 – EER (*Equal Error Rate*). Valor associado: 100

6 – ZeroFNMR. Valor associado: 100

7 – ZeroFMR. Valor associado: 100

8 – Curvas de ROC (*Receiving Operating Curve*) Valor associado: 100
9 – FTE (*Failure to Enroll*) Valor associado: 500
10 – AET (*Average Enroll Time*) Valor associado: 300
11 – AMT (*Average Match Time*) Valor associado: 100
12 – AIT (*Average Identification Time*) Valor associado: 100

Objetivo: Saber qual o conhecimento do avaliador sobre as principais medidas de desempenho de sistemas biométricos as quais está ou esteve em contato teórico.

Peso: 4 (Muito Relevante).

Pergunta 5: Quais taxas e medidas de desempenho de sistemas biométricos abaixo você (avaliador) já utilizou na prática, seja para avaliar o desempenho de algum algoritmo biométrico ou para implementação em algum produto de software biométrico?

Alternativas (cumulativas):

1 – Distribuição Discreta de Genuínos (*Genuine Matching Scores*). Valor associado: 50
2 – Distribuição Discreta de Impostores (*Impostor Matching Scores*). Valor associado: 50
3 – FMR (*False Match Rate*) ou FAR (*False Acception Rate*). Valor associado: 50
4 – FNMR (*False Non-Match Rate*) ou FRR (*False Rejection Rate*). Valor associado: 50
5 – EER (*Equal Error Rate*). Valor associado: 50
6 – ZeroFNMR. Valor associado: 50
7 – ZeroFMR. Valor associado: 50
8 – Curvas de ROC (*Receiving Operating Curve*) Valor associado: 50
9 – FTE (*Failure to Enroll*) Valor associado: 50
10 – AET (*Average Enroll Time*) Valor associado: 50
11 – AMT (*Average Match Time*) Valor associado: 500
12 – AIT (*Average Identification Time*) Valor associado: 500

Objetivo: Saber em qual das principais medidas de desempenho o avaliador teve algum contato na prática.

Peso: 5 (Imprescindível).

ANEXO III

PUBLICAÇÕES E SUBMISSÕES

III.1 INTRODUÇÃO

Durante a elaboração deste trabalho, foram aceitos para publicação os seguintes artigos:

- Sucupira Jr., L. H. R., Araújo, L. C. F., Lizárraga, M. G., Ling, L. L., "Evaluating Biometric Software Packages using a Practioners Methodology", *Proc. of ISCA 16th International Conference on Computer Applications in Industry and Engineering (CAINE-2003),* Las Vegas, Nevada, 310 - 313, 2003.
- Sucupira Jr., L. H. R., Araújo, L. C. F., Lizárraga, M. G., Ling, L. L., "BioEVA: An Evaluation Tool for Biometric Algorithms", *Proc. of International Conference on Biometric Authentication (ICBA-2004),* Hong Kong, 2004.

Este trabalho também está sendo submetido a um pedido de patente (metodologia apresentada no capítulo 4) e a um registro de *software* (BioEVA apresentada no capítulo 5).

III.2 ARTIGO CAINE-03

Evaluating Biometric Software Packages using a Practioners Methodology

Luiz Humberto Sucupira Jr.
School of Electrical and Computer Engineering,
State University of Campinas
Campinas, SP, 13083-970, Brazil
luigijr@decom.fee.unicamp.br

Lívia C. F. Araújo.
School of Electrical and Computer Engineering,
State University of Campinas
Campinas, SP, 13083-970, Brazil
liviacri@decom.fee.unicamp.br

Miguel G. Lizárraga.
School of Electrical and Computer Engineering,
State University of Campinas
Campinas, SP, 13083-970, Brazil
lizarrag@decom.fee.unicamp.br

Lee Luan Ling.
School of Electrical and Computer Engineering,
State University of Campinas
Campinas, SP, 13083-970, Brazil
lee@decom.fee.unicamp.br

Abstract

This paper presents a methodology to evaluate biometric software packages. We propose a top-down hierarchical model based on a division of a biometric system in biometric subsystems. Five basic steps compound the methodology: (1) information is collected about the biometric software product and its manufacturer, (2) a severity level is established, (3) a group of attributes is selected, and *SPIQs* (*Specialist's Profile Identification Questionnaire*) are applied to evaluators, (4) the attributes are applied to evaluate the product, and (5) a final standard report is presented. Each attribute has a *formal specification* of its evaluation process, and could be applied in different test environments with the purpose of observe the behavior of the package. **Keywords** – Evaluation Methodology, Biometric Systems, Software Quality, Software Packages.

1 INTRODUCTION

Automated systems for personal recognition need really efficient security mechanisms, especially on user's authentication. Recent researches suggest that the inclusion of biometric characteristics increases the trustworthiness degree in the authentication of user's identity [1]. In this context, we define *biometric technologies* as "automated methods for authentication and identification of the identity of a live person based on his behavioral or physiological characteristics [1]." Although, the increasing adoption of biometric technologies, nothing is mentioned about costs and damages caused by fails in these products. A software, even if is according to its specification, can contain errors, because the specification can be incorrect. A software whose specification is absent of errors and is in compliance with it, can be used improperly. Then, we observe that the consumers' requirements related to products' quality must be taken in account by the manufacturers that, consequently, certify their production processes and products. Then, we propose our methodology to guarantee products' quality.

Quality certification assures quality in processes, products and/or services that a company offers or performs. *Quality certification* identify essential characteristics and guarantee that they are in compliance with defined requirements and specifications [2][3]. It can be applied to software processes and/or software products [4]. The software process quality emphasizes the development process but without assure that the product will be the expected one. The software product quality analyses the resultant product, not considering previous phases of the software process, identifying important characteristics and judging them in compliance with requirements and specifications [2][4]. This paper focuses a quality evaluation of *biometric software products*.

This paper is divided in four sections. In section 2, we will introduce the *hierarquichal top-down model* based on a division of a biometric system in subsystems, adjusting the ISO/IEC 9126 top-down hierarquical model to the particularities of biometric software products. In section 3, we will illustrate and comment the scheme of application of the methodology. Finally, in section 4, we will make some conclusions about the methodology presented and its advantages.

2 HIERARCHICAL MODEL ADOPTED

The ISO/IEC 9126 defines a *top-down hierarchical model* [2] that can be applied to any software products. It allows that new metrics created to evaluate them, in some way, adjust to their hierarchical definition. But, because of this generalization, it is not possible to establish a specific vision of the characteristics related to a particular software product. Moreover, the model is not clear on determine which parts of the product present major deficiency. So, in the case of biometric systems, we propose a model based on ISO/IEC 9126 top-down hierarchical model, however using a definition of subdivision of a biometric system in subsystems, and the concept of *software packages* presented on norm ISO/IEC 12119.

2.1 The Composition of Biometric Systems

According to [5], all biometric systems are composed of the following subsystems: (1) Data Collection – contains the input device that reads the biometric sample and converts it to a suitable form for processing by the remainder of the system; (2) Transmission – establishes the communication channel between all subsystems; (3) Signal Processing/Feature Extraction – receives the data of the Data Collection Subsystem and converts it to a suitable form for processing by the Matching Subsystem; (4) Matching – matches the sample with its template storage in the Storage Subsystem; and (5) Storage – maintains the enrolled templates. However, if we desire to see a biometric system as a commercial product, we propose to use the concept of software packages presented on norm ISO/IEC 12119 [6], defined as a junction of the software product and its documents. Fig. 1 shows the concept applied to biometric systems. It also shows a biometric system subdivided in subsystems. The documents in fig. 1 are presented on norm ISO/IEC 12119 [6].

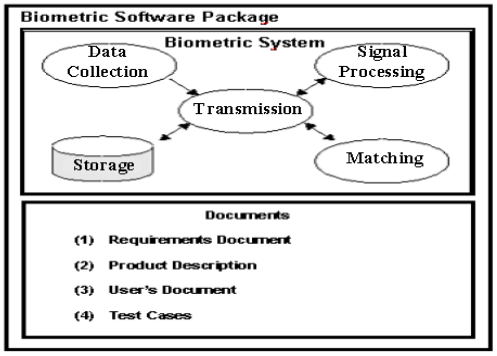


Fig. 1 The Biometric Software Package

2.2 The Biometric Top-Down Hierarchical Model

The concepts of subdivide a biometric system in biometric subsystems and the meaning of a biometric software package will be used to build the *biometric top-down hierarchical model*. The top-down hierarchical models are constructed from top to bottom, from more general to more specifics characteristics or components of a system. However, the software package is evaluated from bottom to top. Figs. 2, 3 and 4 show the adopted models.

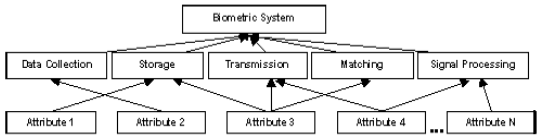


Fig. 2 Top-Down Hierarchical Model based on the subdivision of a biometric system in subsystems.

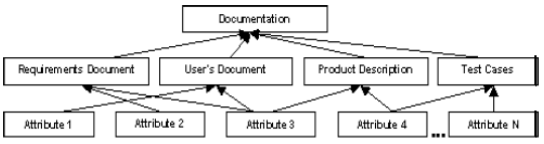


Fig. 3 Top-Down Hierarchical Model based on documentations presented on norm ISO/IEC 12119.

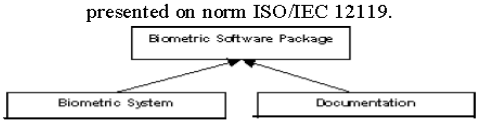


Fig 4 Top Down Hierarchical Model based on the definition of the ISO/IEC 12119 Software Package.

2.3 Selected Attributes

The attributes are in the lowest level of the biometric top-down hierarchical model. We define and/or create 54 attributes extracted from publications involving biometrics [7][8][9] and other sources. Another 45 attibutes were defined for documents evaluation based on norm ISO/IEC 12119 [6]. Both biometrics and documentation attributes will be applied in biometric software packages evaluation, according to an evaluation process specified and documented on each attribute's documentation. The evaluation process identifies norms, standardizations and/or procedures for application of the evaluation on its attribute.

3 THE METHODOLOGY SIMPLIFIED SCHEME

Fig. 5 shows a *simplified scheme* of applying the methodology proposed in this paper.

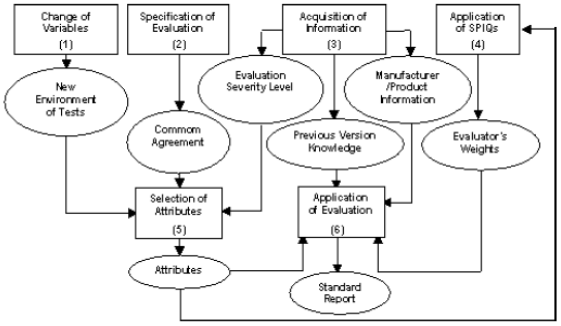


Fig. 5 Methodology Simplified Scheme

According to Fig. 5, application of evaluation (process (6)) needs three main steps: (1st) Selection of Attributes (process (5)) that involves three tasks. The first one defines the *severity level* of the software product (process (3)). Each attribute has a minimum severity level associated. All attributes fitted in the defined level or inferior are selected. The second task is the *common agreement* (process (2)) that defines the specification of the evaluation in manufacturer's presence. This

agreement contains, in a general form, all evaluation procedures and the attributes that will be used. Thus, we allow the manufacturer to argue about the evaluation procedures. Finally, the last task is the establishment of new test environments by the evaluators (process (1)), independent of the common agreement with the purpose of observe the behavior of the product. (2nd) Calculation of the Evaluator's Weights (process (4)), by the application of SPIQs. (3rd) Information about the manufacturer and his product, including information about prior versions of the product (process (3)). Finally, a *standard evaluation report* is produced at the end to document the evaluation applied.

3.1 Evaluation Severity Level

The evaluation is level oriented because of two main goals: first, allows flexibility; second, the severity of applying an attribute's evaluation [10]. TABLE I shows the evaluation severity levels adopted. Level E is the lowest one and was created to evaluate freeware and prototypes. TABLE I also shows the levels under two aspects: financial and biometric. Under financial aspects, we use severity levels presented in [10]. Under biometric aspects, we use essential characteristics to analyze any biometric software product nowadays:

1) *Uniqueness of a Biometric*: how unique a person's biometric pattern is amongst a population of users of a biometric system [9].

2) *Liveness Estimation*: ability of a biometric system to determine whether the biometric samples are from a live person [9].

3) *Information Security Levels*: determines the security level of the stored and transmitted information of a system, according to the classification established on norm DoD5200-28 - Trusted Computer Security Evaluation Criteria – TCSEC. There are four security levels: D, C, B e A [11]. Each one of them is subdivided in 3 sublevels. However, the most used and cited as references are levels D1, C1, C2, B1, B2, B3, A1. Levels D1 and A1 were removed, because level D1 represents absence of security, and level A1 involves system development that is outside of the scope of this paper. The remaining levels are enough to guarantee that the biometric systems are secure against the main threats and attacks mentioned and classified in [8].

4) *Environmental/Temporal Influences*: environmental influences are defined as the effects on the biometric system by such environmental factors as heat, humidity, etc. Temporal influences are defined as the biometric changes along the time [9].

TABLE I
Evaluation Severity Levels for Biometric Products

		Severity Level				
		E	D	C	B	A
Financial Aspects	Environment	No damage to property	Small damage to property	Damage to property	Recoverable environmental damage	Unrecoverable environmental damage
	Person	No risk to people	Minimum risk to people	Few people disabled	Threat to human lives	Many people killed
	Economic	Minimum/ none economic loss	Negligible economic loss	Significant economic loss	Large economic loss	Financial Disaster
	Application	Freeware, prototypes.	Entertainment, household.	Fire alarm, process control.	Medical and financial systems.	Railway and nuclear systems.
Biometric Aspects	Uniqueness of a Biometric	1:50 – 1:100	1:500 – 1:1000	1:5000 – 1:10000	1:50000 – 1:100000	1:500000 – 1:1000000
	Liveness Estimation	Not Necessary	Not Necessary	Must Apply	Must Apply	Must Apply
	Information Security Levels	C1	C1/C2	B1	B2/B3	B3
	Environmental /Temporal Influences	Not Necessary	Not Necessary	Must Apply only to Environmental Influences	Must Apply	Must Apply

3.2 Application of Evaluation

The evaluators will apply the evaluation using the selected attributes. If information exists about prior versions of the product, the new functionalities and updates will be evaluated. The unchanged modules will be tested to guarantee that the new funcionalities and updates do not cause improperly interferences on them. The specification of the evaluation process of an attribute describes how an evaluator must proceeds. It avoids that an attribute be evaluated by evaluator's particular opinions and conclusions. The advantage of this specification is to validate the application of SPIQs: only the evaluator's knowledge and experience is applied, judging his importance in the evaluation process of an attribute. The scores of an attribute are given by evaluators according to a scale. A scale is a range of values that measures an attribute. The scores are mapped on a pattern called *satisfaction scale* which has a percentile interval between 0 to 100%, and uniformizes the scores mapped on it.

Attributes, just like evaluators, have an associated weight that is initially established by the evaluation severity level. The lowest level, E, is correspondent to the numeric value 1, and the highest level, A, is correspondent to the numeric value 5. These weights could be modified through the common agreement: results produced by these changes will provide strong recommendations. Using the scores and weights of all attributes, the scores of each subsystem and documentation will be calculated using the equation:

$$Score\ (s) = \frac{\sum \%\ NA_i \times WA_i}{\sum \%\ NA_i} \quad (1)$$

where NA_i is the percentile score of attribute i, WA_i is the weight of attribute i, and s is the subsystem or documentation which the attribute i is hierarchically dependent. Thus, we can clearly observe which

subsystems or documentation presents fragility or not, from the respective scores. The average of each biometric subsystem scores results in the biometric system score. The average of each documentation scores results in the documentations score.

To calculate the score of the whole biometric software package, some considerations need to be done. Documentation has a different weight associated measuring its importance in each severity level. In level E the documentation could be absent but, in level A, documentation must be complete to offer immediate support and helping to manage the system. The biometric system has same weight, equal to 5. TABLE III second column shows the weights associated to documentation. The final score is calculated using a weighted mean of the biometric system score and the documentation score. After that, we will judge the quality of the package. TABLE III third column shows the quality threshold in each severity level. If the package is considered without quality, then we try to reclassify it in a lower severity level. Finally, standard evaluation report is produced following the contents presented on TABLE IV.

TABLE III
Weights of Documentations classified by severity levels

Severity Level	Document's Weight	Quality Threshold
E	1or 0 (absence)	70%
D	2	80%
C	3	85%
B	4	90%
A	5	95%

TABLE IV
Evaluation Report - Table of Contents

1	**Introduction** - manufacturer, evaluators and biometric software package identification.
2	**Description of the Biometric Software Package** – description of all items and documents.
3	**Specification of the Evaluation** – description of: attributes, severity level, test environments, and prior version evaluation.
4	**Results** – description of each score obtained.
5	**Conclusions** – evaluation result and recommendations.
6	**Glossary** - special terms and abbreviations.

4 CONCLUSION

The proposed methodology provides a rigorous, simple and robust description of a biometric software evaluation procedure. It is flexible and adaptable: new biometric technologies must be also evaluated as well as it supports facilities to aggregate innovations. We readapt the hierarchical model ISO/IEC 9126 to provide the evaluation of each biometric subsystem as well as the whole biometric system and to identify the strongest and the weakest points. The common agreement role clearly shows the procedures of the evaluation and it allows the manufacturer to argue about them. Using the SPIQs' idea and the specification of a evaluation process in the attribute's documentation, we guarantee the validity of both of them. Finally, we presented the main steps for the application of evaluation that results in a standard report.

4 ACKNOWLEDGEMENT

This work was supported in part by CAPES, CNPq and FAPESP.

5 REFERENCES

[1] E. Bowman, "Everything You Need to Know About Biometrics", *Identix Corporation*, 2002.

[2] A. Koscianski, A. Villas-Boas, C.M. Rêgo, C. Asanome, D. Scalet, D. Romero, J.M. Cieslak, M. Paludo, R.S. Frossard, T.M. Vostoupal, "Guia para Utilização das Normas sobre Avaliação de Qualidade de Produto de Software - ISO/IEC 9126 e 14598", *Associação Brasileira de Normas e Técnicas,* 1999.

[3] A.I. Vermesan, "Some Certification for Industry - Verification and Validation Issues in Expert Systems", *Ninth International Workshop on Database and Expert Systems Applications*, pp. 03-14, 1998.

[4] A. Koscianski, J.C.B. Costa, "Combining Analytical Hierarchical Analysis with ISO/IEC 9126 for a Complete Quality Evaluation Framework", proceedings in *Fourth IEEE International Symposium and Forum on Proceedings, Software Engineering Standards*, pp. 218 – 226, 1999.

[5] S.M. Mathyas, J. Stapleton. "A biometric standard for information management and security", *Computers & Security*, vol.19, no.5, p.428-441, 2000.

[6] GEQS/INSOFT, "Tradução Livre da Norma Internacional ISO/IEC 12119", http://www.insoft.softex.br/qualidadeSoftware /biblioteca/normas/download/12119.pdf, 1998.

[7] D. Maio, D. Maltoni, R. Cappelli, J.L. Wayman and A. K. Jain, "FVC2002: Second Fingerprint Verification Competition", *Proc. of International Conference on Pattern Recognition*, Quebec City, 2002.

[8] D. Polemi, "Biometric Techniques: Review and Evaluation of Biometric Techniques for Identification and Authentication, Including an Appraisal of the Areas Where They are Most Applicable," *Final Report*, 1997, http://www.cordis.lu /infosec/src/stud5fr.htm.

[9] Canadian Common Criteria Evaluation and Certification Scheme, "Biometric Technology Security Evaluation under de Common Criteria (CC)", *Doc No: 1351-036-D001*, 2001.

[10] J. Boegh, H.-L. Hausen, D. Welzel, "A Practioners guide to Evaluation of Software", *in Proc. of the IEEE Software Engineering Standards Symposium*, 1993.

[11] United State of America Department of Defense, "Trusted Computer System Evaluator Criteria (TCSEC)", *DoD 5200.28-STD*, 1983, http://www.radium.ncsc.mil/tpep/library/rainbow/ 5200.28-STD.html.

III.3 Artigo ICBA-04

BioEVA: An Evaluation Tool for Biometric Algorithms

Luiz H. R. Sucupira Jr[1], Lívia C. F. Araújo[2], Miguel G. Lizárraga[2], Lee L. Ling[2]

[1]School of Electrical and Computer Engineering, State University of Campinas
Albert Einstein Avenue, 400, PO Box 6101, Postal Code 13083-970, Campinas, SP, Brazil
luigijr@yahoo.com
[2]School of Electrical and Computer Engineering, State University of Campinas
Albert Einstein Avenue, 400, PO Box 6101, Postal Code 13083-970, Campinas, SP, Brazil
{ liviacri, lizarrag, lee} @decom.fee.unicamp.br

Abstract. This paper presents a tool, named BioEVA, to apply two forms of evaluation processes in biometric algorithms: comparative and qualitative. BioEVA has an internal engine that implements some metrics that we called quality parameters. We define some simple submission rules (protocol) must be followed before to submit a biometric algorithm to BioEVA's evaluation. The tool receives a biometric algorithm as a "black-box" and performs its automated evaluation. Using BioEVA, three biometric algorithms were evaluated: two based on static signatures and one based on keystroke dynamics. **Keywords:** Biometric Algorithms, Quality Evaluation, Software Engineering.

1 Introduction

The main purpose for development of biometric algorithms and hardware devices for biometric samples acquisition is to guarantee more security in a user's authentication process. A third-party quality evaluation of biometric algorithms and systems will give validity to the developer's tests and results. In this evaluation, it is possible to compare algorithms, but only with the same database and the test environment [1]. However, in a competitive scenario, comparative tests sometimes are not desired because the consumers think that the best products are expensive, the worst ones are not able to be trusted, and the intermediate ones follow the relation "cost-benefit".

We are proposing a qualitative evaluation, based on the results produced on tests with biometric algorithms, with the possibility to compare them too. Then, we developed a tool called BioEVA that implements an environment to receive a biometric algorithm as a "black box", i.e., without the source code opened. Because of the possibility of apply an evaluation in only one biometric algorithm, we need to establish quality parameters to evaluate each kind of biometric technology, determining how good or bad they are under some criteria and definitions.

This paper is divided in 6 sections. In section 2, we will discuss about the ideas that provides BioEVA development. In section 3, we will show how to submit a biometric algorithm for its evaluation. In section 4, we will present the modules that compound

This work was partially supported by CNPq, CAPES and FAPESP.

the tool. In section 5, we will show the results of applying the tool on an evaluation of three biometric algorithms. Finally, in section 6, we will make some conclusions about the tool and the results produced in section 5.

2 Background

Before implementing BioEVA, some ideas of two previous works in the qualitative and comparative evaluations in biometric products were used to develop BioEVA. In next subsections, we will present these works and comment them.

2.1 Fingerprint Verification Competition (FVC)

The FVC is a competition that focuses on fingerprint verification algorithms. This competition provides us the following ideas:

- The protocol about how to submit an algorithm to a competitive evaluation;
- Definitions and criteria to compare biometric algorithms, which were used to define and configure some of the quality parameters used in this work.

The protocol used in FVC is based on command-line arguments. Besides, a participant needs to take two C-language skeletons (one for enrollment and the other for authentication), inserting their algorithms there. We propose the elimination of these skeletons, performing language and platform independence. Another issue is that the databases are not collected according to a formal protocol, and the participants have to adapt their algorithms to FVC collected samples or not submit them. We also propose an improvement based on the idea of a qualitative evaluation.

2.2 Methodology for Evaluation of Biometric Software Packages

A proposed methodology for evaluation of biometric software packages is one of our previous works [2]. We will use this methodology to establish a qualitative evaluation process. The common agreement established in [2] defines the specification of the evaluation process in manufacturer's presence, and we adapt it to a form that we named common agreement form. The common agreement form will be used to collect information about the biometric samples (fig. 1, process (1) - Preparing the Common Agreement). If the biometric samples are the same that the ones in BioEVA's database, then the process (6) – Collecting Samples for Tests in fig. 1 will use them. Otherwise, a new database must be collected by the Samples Collector in fig. 1, based on the developer's information on common agreement form.

The severity levels defined in [2] will be used to define the degree of performance and efficiency of the biometric algorithm. Five levels were defined: E is the lowest one and A is the highest one. To define the level of a biometric algorithm, first we apply the process (9) – Invoking the Evaluation Module in fig. 1, and BioEVA produces a biometric algorithm's score. Finally, the thresholds defined in [2] are applied: if the score is greater or equal than the threshold level, it is accepted to the respective severity level; otherwise, it is classified in a lower severity level.

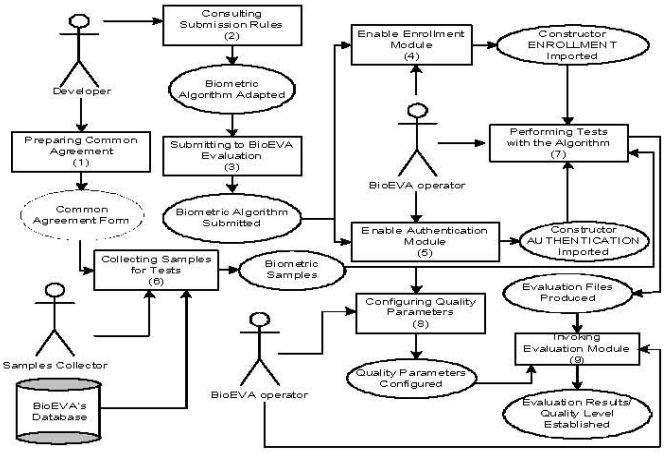


Fig. 1. BioEVA Evaluation Scheme

3 Submission Rules (Protocol)

The developer of the biometric algorithm must obey some simple rules (process (2) – Consulting Submission Rules in fig. 1) before to submit it to BioEVA evaluation (process (3) – Submitting to BioEVA Evaluation in fig. 1):

1. If the algorithm was developed in java, then the algorithm is submitted as a .jar file; otherwise it is submitted as a library file according to the platform. Thus, we provide to the participants the advantage of language and independence platform.
2. Two constructors (.jar file) or procedures (other files) must be created: ENROLLMENT and AUTHENTICATION. The BioEVA operator (fig. 1) will import the libraries that contain both constructors, using an import declaration (java sources) or the Java Native Interface (other sources), enabling the enrollment and the authentication modules (process (4) – Enable Enrollment Module and process (5) – Enable Authentication Module in fig. 1).
3. ENROLLMENT constructor's call must obey the following syntax for input data:

```
ENROLLMENT (id, samples, template_destination)
```

Input Parameters	Type	Description
`Id`	`string`	User's identification
`Samples`	`array of string`	Complete samples' path of the created templates
`template_destination`	`string`	Destination path of the created templates

4. AUTHENTICATION constructor's call follows the syntax for input data below:

```
AUTHENTICATION (id, sample, templates_location)
```

Input Parameters	Type	Description
`Id`	`string`	User's identification (verification) or `null` (identification)
`Sample`	`string`	Complete samples' path
`template_location`	`string`	Destination path of the templates

5. The outputs of both constructors will be used to generate the evaluation results (process (7) – Performing Tests with the Algorithm), using a method (function):

```
string output_results ( )
```

where `string` is the output that depends on the constructor. The syntax for ENROLLMENT constructor is "`Value+Total_samples`". `Value` indicates if the enrollment process was successful (`Value = 0`) or not (`Value ≠ 0`). If not, `Value` could be 1 (FAIL), 2 (TIMEOUT), or 3 (CRASH) [1]. `Total_samples` is the number of samples to enroll a user. The syntax for AUTHENTICATION constructor is "`&id-value`" (verification) or "`&id1-value1&id2-value2&id3-value3...&idN-valueN`" (identification). `Id` indicates the user's id related to a template which one the input sample was compared. `Value` indicates a value produced by the comparison of the input sample and one template. Using strings became the participant's efforts more simple to implement the constructor's output and solve the problems with more complex data structures.

4 BioEVA Tool

BioEVA main purposes are testing algorithm's performance and efficiency and it was implemented using Java 2 Platform. Three modules were implemented: enrollment, authentication and evaluation. In Enrollment and Authentication Modules, it is possible to BioEVA Operator selects if the algorithm is single or multimodal. Three files will be generated using the output of the method `output_results` (process (7) – Performing Tests with the Algorithm) for ENROLLMENT constructor:

- ParameterET.dat: it receives the times, in milliseconds, that the algorithm completes the enrollment processes;
- ParameterFTE.dat: it receives the values related to successful or fail in the enrollment processes;
- ParameterTSE.dat: it receives the values related to the amount of samples used to enroll the users on each enrollment process.

As result of the process (7) – Performing Tests with the Algorithm for AUTHENTICATION constructor, BioEVA will generate four files:

- Parameter_v`'id'`_AT.dat: it receives the times, in milliseconds, that the algorithm completes the verification processes. The `'id'` in the file name identifies the user's id provided by BioEVA operator (fig. 1) in the authentication module.
- Parameter_v`'id'`_FFC_IGD.dat: it receives the resultant value of a user's template matching with a user's sample. The `'id'` in the file name identifies the user's id provided by BioEVA operator (fig. 1) in the authentication module.
- Parameter_i_AT.dat: it receives the times, in milliseconds, that the algorithm completes the identification processes.
- Parameter_i_FFC_IGD.dat: it receives the resultant values of all templates matching in database with a user's sample.

In the Evaluation Module, all files generated in the previous modules (enrollment and authentication) are used to evaluate the algorithm. When the BioEVA Operator invoke this module (process (9) – Invoking Evaluation Module in fig. 1), BioEVA

automatically uses the data stored in these files to calculate the score that the algorithm had obtained. Six quality parameters were implemented:

1. Impostor and Genuine Distribution (IGD): In these distributions each threshold has a number of users that are accepted as genuine and the remaining accepted as impostors. The module observes how much they are separated.
2. FAR / FRR curves (FFC): the evaluation is made through the EER (Equal Error Rate). These curves are built calculating the users' percentile value that were false rejected (FRR) and the ones that were false accepted (FAR) on each threshold.
3. Enrollment Time (ET): the module extracts the mean and standard deviation. Both are used to evaluate the enrollment time of the enrollment process.
4. Authentication Time (AT): the module extracts the mean and standard deviation. The module evaluates verification and identification separately. The AT score is calculated using a mean of the scores obtained in both authentication processes.
5. FTE rate (FTE): the module verifies how many enrollment trials are successful or not. In the case of failed enrollment process, we classify them according to [1].
6. Total Samples to Enroll (TSE): the module verifies the average, maximum and minimum samples that were used to enroll the users.

The quality values of each quality parameter are adjusted by the BioEVA operator (Process (8) – Configuring Quality Parameters in fig. 1). They are mapped in a satisfaction scale which range is [0,100]. A mean of the percentile values of all quality produces a final percentile value that will be used to classify the biometric algorithm according to a quality level as we shown in section 2.2.

5 Practical Results

Two algorithms based on static signatures (ASig1 and ASig2), and one based on keystroke dynamics (AKey1) were evaluated. The signatures database for ASig1 and ASig2 algorithms was compounded by signatures of 112 different users that signs 5 times for enrollment and 4 to 5 times for authentication, resulting in a database size of 1098 samples. The keystroke database for AKey1 algorithm was compounded by the typing rhythm of 50 different users. Each user types 10 times for enrollment and 50 to 60 times for authentication. These results in a database size of 3250 samples.

Table 1 and 2 show the configured scales of the quality parameters according to references [1], [3]-[12]. We configured the standard deviation presented on ET and AT quality parameters without use any references because this value can measure the stability degree of a biometric algorithm related to the mean time in enrollment and authentication processes.

Table 1. Scales for Quality Parameters FFC, FTE, TSE, ET and AT for ASig1 and ASig2

Parameters \ Scale			Excellent	Good	Regular	Insufficient
FFC			v≤2%	2%<v≤5%	5%<v≤10%	v>10%
FTE			v≤1%	1%<v≤3%	3%<v≤5%	v>5%
TSE			v≤5	5<v≤10	10<v≤15	v>15
ET	**μ**		v≤15s	15s<v≤20s	20s<v≤30s	v>30s
	σ		v≤5s	5s<v≤10s	10s<v≤15s	v>15s
AT	**Verification**	**μ**	v≤2s	2s<v≤5s	5s<v≤8s	v>8s
		σ	v≤0.5s	0.5s<v≤1s	1s<v≤3s	v>3s
	Identification	**μ**	v≤30s	30s<v≤60s	60s<v≤120s	v>120s
		σ	v≤10s	10s<v≤20s	20s<v≤30s	v>30s

Table 2. Scales for Quality Parameters FFC, FTE, TSE, ET and AT for AKey1

Parameters \ Scale			Excellent	Good	Regular	Insufficient
FFC			v≤3%	3%<v≤6%	6%<v≤12%	v>12%
FTE			v≤1%	1%<v≤3%	3%<v≤5%	v>5%
TSE			v≤10	10<v≤15	15<v≤30	v>30
ET	**μ**		v≤15s	15s<v≤20s	20s<v≤30s	v>30s
	σ		v≤5s	5s<v≤10s	10s<v≤15s	v>15s
AT	**Verification**	**μ**	v≤2s	2s<v≤5s	5s<v≤8s	v>8s
		σ	v≤0.5s	0.5s<v≤1s	1s<v≤3s	v>3s

Table 3. Evaluation Results for Algorithms ASig1, ASig2 and AKey1

Quality Parameters			ASig1		ASig2		AKey1	
			Results	**Mapped**	**Results**	**Mapped**	**Results**	**Mapped**
GID			-	50%	-	92%	-	88.6%
FFC			9%	13%	2.6%	93%	3.1%	98.9%
FTE			0.89%	100%	0%	100%	0%	100%
TSE			4 samples	100%	5 samples	100%	8 samples	100%
ET	**μ**		11.7s	100%	3.4s	100%	0.056s	100%
	σ		1.1s		0.97s		0.03s	
AT	**Verification**	**μ**	2.6s	86%	1.2s	99.5%	0.022s	100%
		σ	0.9s		0.5s		0.025s	
	Identification	**μ**	32.7s		20.5s		-	
		σ	4.3s		5.1s		-	

The results of the BioEVA tool tests for algorithms ASig1, ASig2 and AKey1 are shown at second, fourth and sixth columns of table 3 respectively. The third, fifth and seventh columns of table 3 show the mapped percentile values. The mean of these values results in the final score of the ASig1 (74.83%), ASig2 (97.41%) and AKey1 (97.90%) respectively. According to the thresholds established in [2], ASig1 is a Level E, and ASig2 and AKey1 are Level A. In a comparative evaluation, observing the second and fourth columns in table 3, the performance and efficiency of ASig2 algorithm is better than ASig1.

6 Conclusion

The BioEVA tool was developed to evaluate biometric algorithms like a "black-box", performing comparative and qualitative evaluations. Some simple rules (protocol) must be followed by the developers. The tests results in enrollment and authentication modules are stored in files. These files will be used by the evaluation module to make an automated evaluation. We establish 6 quality parameters and a novel quality value using the standard deviation for AT and ET. The BioEVA tool performs an evaluation in single or multimodal biometric algorithms.

This work improves some issues presented in the FVC competition. The C-language skeletons were removed, which provides language independence, and a formal document was established named common agreement form. BioEVA supports platform independence: the Java Virtual Machine (JVM) and the Java Native Interface (JNI) will provide this feature through library files. Finally, we tested three algorithms: two based on static signatures and one based on keystroke dynamics.

References

1. Maio, D., Maltoni, D., Cappeli, R., Wayman, J.L., Jain, A. K.: FVC2002: Second Fingerprint Verification Competition, *Proc. of Int. Conf. on Pattern Recognition*, Quebec City (2002).
2. Sucupira Jr., L.H., Araújo, L.C.F., Lizárraga, M.G., Ling, L.L., "Evaluating Biometric Software Packages using a Practioners Methodology", *Proc. of ISCA 16th Int. Conference on Computer Applications in Industry and Engineering (CAINE-2003)*, USA (2003) 310-313.
3. Wirtz, B.: Average Prototypes for stroke-based signature verification, *ICDAR 97*, vol. 1, Germany, (1997) 268-272.
4. Lee, L.L., Lizárraga, M.G.: Off-line methods for human signature verification, *Proceedings of IASTED International Conference on Signal and Image Processing SIP-96*, USA (1996).
5. Lizárraga, M.G.: Um Sistema Biométrico de Identificação Pessoal via Internet com ênfase em Assinaturas Estáticas. Doctorade Thesis, UNICAMP, August (2000).
6. Plamondon, R., Srihari, S.N.: On-Line and Off-Line Handwriting Recognition: Compreensive Survey, *IEEE Trans. Patt. Anal. Mach. Intell.*, Vol. 22, N° 1, (2000) 63-84.
7. Joyce, R., Gupta, G.: Identity authorization based on keystroke latencies, *Communications of the ACM*, Vol 33. N° 2, (1990) 168-176.
8. De Ru, W.G., Eloff, J.H.P.: Enhanced Password Authentication through Fuzzy Logic, *IEEE Expert / Intelligent Systems & Their Applications*, Vol. 17, No. 6, (1997) 38-45.
9. Robinson, J.A., Liang, V.M., Michael, J.A.: Computer User Verification Login String Keystroke Dynamics, *IEEE Trans. Syst., Man, Cybern.*, Vol. 28, No. 2, (1998) 236-241.
10. Lin, D.T.: Computer-Access Authentication with Neural Network Based on Keystroke Identity Verification, *International Conference on Neural Networks*, Vol. 1, (1997) 174-178.
11. Bleha, S., Slivinsky, C., Hussain, B.: Computer-Access Security Systems Using Keystroke Dynamics, *IEEE Trans. Pattern Anal. Machine Intell.*, Vol. 12, No. 12, (1990) 1217-1222.
12. Haidar, S., Abbas, A., Zaidi, A.K., A Multi-Technique Approach for User Identification through Keystroke Dynamics, *IEEE Int. Conf Syst.,Man Cybern.*, Vol. 2, (2000) 1336-1341.

III.4 Pedido de Patente

"METODOLOGIA PARA AVALIAÇÃO DE PACOTES DE SOFTWARE BIOMÉTRICOS"

A presente patente é de uma metodologia para avaliação de qualidade em pacotes de software biométricos. A metodologia permite que, sob determinados parâmetros de qualidade, denominados atributos, seja possível investigar e determinar o grau de qualidade do pacote de software biométrico. Entende-se por qualidade a capacidade de satisfazer seus usuários finais e de isentar o pacote de erros que venham à causa-lhes prejuízos financeiros e ambientais.

A biometria é o ramo da ciência que estuda a mensuração dos seres vivos. Tecnologias biométricas são definidas como "métodos automáticos de verificação ou identificação da identidade de uma pessoa viva baseados em características fisiológicas ou comportamentais". Métodos automáticos englobam elementos componentes de um sistema biométrico 2. Um sistema automático baseado em características biométricas pode ser classificado com relação à maneira com que o sistema autentica a identidade dos seus usuários. Neste caso, duas categorias podem ser definidas: verificação e identificação. Na verificação o sistema compara a informação biométrica apresentada por um indivíduo com a informação biométrica armazenada em uma base de dados correspondente àquele indivíduo. Em contrapartida, na identificação, o sistema 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. Outra definição inerente a tecnologias biométricas é a diferença

III.5 Registro de *Software*

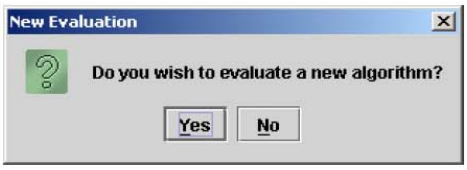
REGISTRO DE SOFTWARE

FERRAMENTA BioEVA

CRIADORES: **Luiz Humberto Rabelo Sucupira Júnior (Principal)**
Lee Luan Ling

Resumo:
No presente registro de software a ferramenta que denominamos BioEVA oferece um ambiente para o recebimento de algoritmos biométricos como um arquivo jar (para aqueles implementados na linguagem java) ou um *libray file* (para aqueles implementados em outras linguagens), contendo os dois principais processos existentes em algoritmos biométricos: cadastramento e autenticação. O algoritmo será chamado dentro do código-fonte da BioEVA. Ambos os processos serão testados por dois módulos implementados na BioEVA: o módulo de cadastramento e o de autenticação. Um terceiro módulo denominado avaliação, utiliza os resultados gerados pelos módulos de cadastramento e autenticação para realizar a avaliação do algoritmo biométrico, finalidade desta ferramenta.

Interface gerada pelo arquivo TelaInicial.java:



Arquivo TelaInicial.java:

– O questionamento é feito para o usuário da ferramenta: caso ele deseje avaliar um novo algoritmo ele seleciona "YES", que chama o frame CasoPositivoAlgoritmoFrame; caso contrário, se ele deseja realizar mais testes com um algoritmo pré-existente ou visualizar novamente seus resultados, ele seleciona "NO", que chama o frame CasoNegativoAlgoritmoFrame.

Código-Fonte:

```
package AvaliacaoObjetiva;

import javax.swing.JOptionPane;
import java.awt.Dimension;
```