Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Ciência da Computação

Verificação Automática de Assinaturas On-line Utilizando Descritores de Fourier em Janelas de Tamanho Fixo

Wesley Ferdinando Rodrigues de Carvalho

Monografia apresentada como requisito parcial
para conclusão do Bacharelado em Engenharia de Computação

Orientador
Prof. Dr. Bruno Luiggi Macchiavello Espinoza

Brasília
2015

Universidade de Brasília — UnB
Instituto de Ciências Exatas
Departamento de Ciência da Computação
Bacharelado em Engenharia de Computação

Coordenador: Prof. Dr. Ricardo Zelenovsky

Banca examinadora composta por:

Prof. Dr. Bruno Luiggi Macchiavello Espinoza (Orientador) — CIC/UnB
Prof. Dr. Alexandre Zaghetto — CIC/UnB
Prof. Dr. Flávio de Barros Vidal — CIC/UnB

CIP — Catalogação Internacional na Publicação

Carvalho, Wesley Ferdinando Rodrigues de.

Verificação Automática de Assinaturas On-line Utilizando Descritores de Fourier em Janelas de Tamanho Fixo / Wesley Ferdinando Rodrigues de Carvalho. Brasília : UnB, 2015.
131 p. : il. ; 29,5 cm.

Monografia (Graduação) — Universidade de Brasília, Brasília, 2015.

1. biometria comportamental, 2. assinatura *on-line*, 3. transformada rápida de Fourier, 4. verificação, 5. performance

CDU 004.4

Endereço: Universidade de Brasília
Campus Universitário Darcy Ribeiro — Asa Norte
CEP 70910-900
Brasília–DF — Brasil

Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Ciência da Computação

Verificação Automática de Assinaturas On-line Utilizando Descritores de Fourier em Janelas de Tamanho Fixo

Wesley Ferdinando Rodrigues de Carvalho

Monografia apresentada como requisito parcial
para conclusão do Bacharelado em Engenharia de Computação

Prof. Dr. Bruno Luiggi Macchiavello Espinoza (Orientador)
CIC/UnB

Prof. Dr. Alexandre Zaghetto
CIC/UnB

Prof. Dr. Flávio de Barros Vidal
CIC/UnB

Prof. Dr. Ricardo Zelenovsky
Coordenador do Bacharelado em Engenharia de Computação

Brasília, 27 de agosto de 2015

Dedicatória

Dedico esse trabalho à minha mãe Marinalva Rodrigues de Carvalho, por sua incansável dedicação em manter meu bem estar físico e emocional, ao meu irmão Wanderson Valério Rodrigues de Carvalho, por todo seu orgulho expressado por conta de minhas conquistas, e em especial, ao meu pai Graciliano Marques de Carvalho, por desde sempre enfatizar a importância da educação, por sua perseverança em minha pessoa e por todo o apoio e confiança oferecidos durante essa longa jornada.

Agradecimentos

Agradeço primeiramente à Deus, por me permitir conhecer tantas pessoas especiais durante esse tempo de estudos na Universidade de Brasília, além de me abençoar com a superação desta etapa da minha vida. Agradeço o meu orientador Bruno L. M. Espinozza, por toda sua prestatividade em me ajudar quando precisei. Ao Nilson D. G. Júnior, por sua imprescindível assistência no desenvolvimento da aplicação proposta neste trabalho. Aos professores Marcus V. Lamar e Arthur V. F. de Azevedo, por seus conselhos nos momentos mais difíceis da minha vida acadêmica. Ao meu primo Marcelo A. Lima, pelos velhos tempos de vestibulando, em que subíamos a pé para a biblioteca da UPIS para estudar. À Fabiana Pacheco, ao Fábio Soares e ao Abimael Tedesco, por todo o apoio e pelo carinho em me levar sorvete um dia antes do início das provas do vestibular da UnB. Aos meus grandes e especiais amigos Leonardo Mendes de Araújo e Renato Vieira Silveira Martins, pelo cuidado, preocupação e solidariedade inigualáveis à minha pessoa. Ao Sérgio Ricardo Farias, o qual foi fundamentalmente importante no acesso ao meu primeiro trabalho enquanto universitário. Aos queridos Daniel C. Spehar e Isaac Newton, pelas boas lembranças deixadas em estudos para matérias como Cálculo de Probabilidade e Geometria Diferencial, na época em que eu era aluno do curso de Bacharelado em Matemática. Aos meus ex-companheiros de trabalho, Harudgy Amano e Thiago Godoi, pelas nossas polêmicas e divertidas saídas. Aos parceiros Marco Antônio M. Pinheiro e Willian O. Barreiros Júnior, pela amizade e pelos engraçados momentos vividos durante estudos para as provas de Circuitos Elétricos Aplicados. Por fim, à minha querida Ingrid Felix Millan, por toda compreensão e ajuda prestados durante o período de conclusão deste trabalho, pois, sem ela, as coisas seriam mais difíceis.

Resumo

O objetivo deste trabalho é descrever o desenvolvimento da implementação de um sistema que realiza a autenticação de usuários através do uso de assinaturas manuscritas. O sistema proposto é composto por quatro módulos principais: coletor do sinal de entrada, pré-processador, gerador de perfil biométrico da assinatura do usuário e o comparador/classificador do sinal de entrada. O módulo coletor do sinal de entrada é responsável pela obtenção de amostras do traço das assinaturas, através de um tablet sensível ao toque. O módulo de pré-processamento é responsável pela adaptação ou remoção de variações nos dados de entrada, visando melhorar o desempenho geral do sistema. O módulo de gerador do perfil biométrico da assinatura do usuário extrai características biométricas de um conjunto de assinaturas de referência, sendo que as características são determinadas pelos espectros de frequência obtidos de segmentos de tamanho fixo da assinatura, através da Transformada Rápida de Fourier (do inglês, *Fast Fourier Transform* (FFT)). Por último, o módulo de comparação e classificação realiza a comparação das características biométricas obtidas da assinatura de teste (assinatura a ser verficada) e do perfil biométrico do usuário (armazenado no sistema), por meio do cálculo da norma Euclidiana entre os segmentos (janelas) correspondentes de cada assinatura. Por seguinte, obtém-se a média das distâncias dessas janelas, a qual será comparada a um valor limiar definido, que serve como parâmetro na tomada de decisão da autenticidade do sinal de entrada. Para a análise da eficácia do sistema foram consideradas as medidas de taxa de aceitação falsa (do inglês *False Acceptance Rate* (FAR)), taxa de rejeição falsa (do inglês *False Rejection Rate* (FRR)) e taxa de erro equivalente (do inglês *Equal Error Rate* (EER)), obtidas a partir de testes submetidos a um conjunto de 5000 assinaturas, dividido em um mesmo número de assinaturas genuínas e forjadas.

Palavras-chave: biometria comportamental, assinatura *on-line*, transformada rápida de Fourier, verificação, performance

Abstract

The objective of this study is to describe the development of the implementation of an system that performs user authentication through the use of handwritten signatures. The proposed system consists of four main modules: input signal collector, preprocessor, user signature biometric profile generator and the comparator/sorter input signal. The input signal from the collector module is responsible for obtaining subscription trace of samples through a pressure sensitive tablet. The pre-processing module is responsible for the adaptation or removal of variations in the input data, to improve the overall system performance. The generator module of biometric profile of a signature belonging a user extracts biometric features of a set of reference signatures, the characteristics of which are determined by the frequency spectra of fixed size segments of the signature by Fast Fourier Transform. Finally, the comparison and classification module performs the comparison of biometric data obtained from the test signature (signature to be verified) and biometric user profile (stored in the system), by calculating the Euclidean norm between the segments (windows) corresponding to each subscription. In the following, we obtain the average of the distances of these windows, which is compared to a defined threshold, that serves as a parameter in making decision of the authenticity of input signal. To analyze the effectiveness of the system were considered measures of false acceptance rate, false rejection rate and equivalent error rate obtained from tests subjected to a set of 5000 signatures, divided into the same number of genuine and forged signatures.

Keywords: behavioral biometric, on-line signature, Fast Fourier Transform, verification, performance

Sumário

Lista de Figuras

Lista de Tabelas

Lista de Siglas e Acrônimos

DF	Descritores de Fourier
DFT	Discrete Fourier Transform (tradução: Transformada Discreta de Fourier)
DTW	*Dynamic Time Warping* (tradução: Sincronização Temporal Dinâmica).
EER	*Equal Error Rate* (tradução: Taxa de Erro Equivalente)
EHU	*University of the Basque Country*
EUPMt	*Escola Universitária Politécnica de Mataro*
FAR	*False Acceptance Rate* (tradução: Taxa de Aceitação Falsa)
FFT	*Fast Fourier Transform* (tradução: Trasformada Rápida de Fourier)
FRR	*False Rejection Rate* (tradução: Taxa de Rejeição Falsa)
HMM	*Hidden Markov Model* (tradução: Modelos Ocultos de Markov)
MCYT	*Ministerio de Ciencia y Tecnología*
PAS	Processamento Analógico de Sinais
PDS	Processamento Digital de Sinais
TFTC	Trasformada de Fourier de Tempo Contínuo
TFTD	Trasformada de Fourier de Tempo Discreto
UPM	*Universidad Politecnica de Madrid*
UVA	*University of Valladolid*

Capítulo 1

Introdução

A verificação automática de assinaturas manuscritas é uma importante área de pesquisa, pois, estuda o tipo de biometria mais utilizado em contextos formais, além da larga aceitação social e legal como método de autenticação de pessoas. Quando necessário, a verificação de assinaturas é realizada de maneira não automatizada por profissionais especialistas em comparar e avaliar a similaridade entre uma ou mais assinaturas. Esse processo costuma ser lento e torna-se inviável em casos onde o número de assinaturas a serem verificadas é relativamente alto. Desta forma, a automatização do processo de verificação de assinaturas visa melhorar a segurança de transações contra fraudes, pois, por meio desse tipo de tecnologia, é possível se aumentar o número de verificações de documentos sem a necessidade da análise de um especialista.

A verificação automática de assinaturas pode ser dividida em duas áreas principais: verificação de assinatura *on-line* e *off-line*. Na verificação de assinaturas *off-line*, geralmente a assinatura está disponível em um documento que necessita primeiramente ser digitalizado, obtendo-se sua representação digital de imagem, a qual será posteriormente processada pelo sistema. Já a verificação de assinaturas *on-line*, utiliza dispositivos eletrônicos especiais, como *tablets* capazes de obter sequências temporais associadas à posições e medidas de pressão da ponta da caneta. Ambos os métodos possuem vantagens e desvantagens.

Dados *off-line* são de maneira geral, mais fáceis de se adquirir, pois necessita-se somente de um dispositivo digitalizador (*scanner*) para obtê-los. Por outro lado, as etapas de pré-processamento necessários para extrair informações importantes da assinatura são mais difíceis como, por exemplo, a diferenciação e separação do traço da assinatura com referência ao fundo da imagem coletada [7].

Assinaturas *on-line* são mais flexíveis em relação às *off-line* no que se refere à quantidade de componentes os quais se pode extrair alguma informação útil para o processo de verificação. Uma de suas vantagens sob sistemas *off-line* é a possibilidade de se coletar dados espaço-temporais da assinatura, além de dados relacionados à pressão, inclinação da caneta, intervalos de suspensão da caneta durante a escrita, dentre outros, que permitem que se obtenham melhores resultados no processo de autenticação.

Assim, sistemas de verificação *on-line*, geralmente são mais difíceis de se fraudar quando comparados à sistemas *off-line*, onde o falsificador preocupa-se unicamente em reproduzir a forma da assinatura, ou seja, seu desenho e proporções, não preocupando-se com a reprodução paralela de informações relativas à velocidade e/ou aceleração de es-

crita, ângulo de azimute (ângulo de projeção da caneta com relação a um referencial no plano do *tablet*), além daqueles já supracitados.

As aplicações de reconhecimento de assinaturas *on-line* abrangem autenticações de documentos legais, contratos executivos, acordos formais, serviços recebidos, cheques e cartões de crédito [12]. A possibilidade de se coletar uma assinatura, representá-la digitalmente e processá-la em tempo real, introduz uma série de novos domínios de aplicação. Por exemplo, muitos programas baseados em senhas ou PIN's (do inglês, *Personal Identification Number*) para acessar seus recursos e serviços, podem substituir tal metodologia por um sistema de verificação automática de assinaturas. Essa possível substituição pode oferecer várias vantagens por meio de um sistema biométrico dessa categoria, pois, uma assinatura é mais difícil de roubar do que uma senha, além de ser mais fácil de se recordar pelo usuário [7].

Sistemas de verificação automática de assinaturas fazem parte do conjunto de sistemas chamados de sistemas biométricos. Sistemas biométricos geralmente são classificados em uma de duas categorias, as quais dependem da natureza da característica biométrica coletada: fisiológica ou comportamental. A biometria fisiológica vale-se da medida de partes específicas do corpo de um indivíduo [6], enquanto a biometria comportamental concentra-se em medir padrões comportamentais de um indivíduo. Sistemas de verificação *on-line* ou *off-line* de assinaturas são classificados como sistemas biométricos comportamentais, pois, a assinatura é uma biometria que depende predominantemente de características comportamentais do indivíduo.

Quando comparados à sistemas baseados em biometria fisiológica, sistemas baseados em biometria comportamental geralmente possuem performance pouco satisfatória em contextos que demandam requisitos de alta segurança. Isso se deve por conta dos desafios que sistemas biométricos comportamentais devem superar, no que se refere à variação das medidas das características biométricas, que ocorrem a cada processo de verificação. Considerando os sistemas de verificação de assinaturas em particular, duas assinaturas de uma mesma pessoa nunca são iguais, e além disso, ruídos podem ser introduzidos no sinal de entrada. No entanto, a verificação automática de assinaturas pode ser combinada a outros métodos biométricos, caso seja necessária uma maior segurança. Com efeito de ilustração, a Figura 1.1 mostra a variação que amostras distintas de assinaturas de um mesmo indivíduo:

(a) (b)

Figura 1.1: Exemplo de (a) assinatura genuína de uma pessoa, (b) variação intrapessoal medida pela sobreposição de três assinaturas genuínas do mesmo indivíduo. [31].

1.1 Apresentação do Problema

A necessidade de se autenticar pessoas em processos relacionados a contratos e negócios em geral, remota a muitos anos da história da humanidade. Porém, a falsificação desse processo de autenticação também possui a mesma idade. Desta forma, se mostra útil a utilização de métodos de verificação automática de assinaturas online, pois, essa metodologia de verificação, pode aumentar a segurança em diversos processos dependentes de modelo de negócio, promovendo velocidade e confiança, já que, a tarefa de verificação da autenticidade de uma assinatura é realizada por profissionais especializados.

Motivado por essa questão, este trabalho propõe uma metodologia de verificação de assinaturas *on-line* manuscritas, baseada no trabalho de Yanikoglu e Kholmatov desenvolvido em [41], que envolve a extração de espectros de frequências do sinal de uma assinatura, posteriormente utilizados no processo de reconhecimento.

1.2 Objetivos

Nas Subseções 1.2.1 e 1.2.2 serão definidos os objetivos gerais e específicos, respectivamente, que deverão ser alcançados até o término do desenvolvimento deste trabalho.

1.2.1 Objetivos Gerais

- Implementar um algoritmo de verificação de assinaturas *on-line* baseado em características locais e globais da assinatura.

1.2.2 Objetivos Específicos

- Simular o processo de coleta de assinaturas.
- Estudar a biblioteca OPEN CV 2.4.10.
- Estudar a biblioteca SQLite 3.8.11.1.
- Estudar o ambiente de desenvolvimento integrado Visual Studio 2013.
- Estudar a análise de Fourier.

1.3 Revisão Bibliográfica

Dentre as técnicas mais tradicionais utilizadas para solucionar o problema da verificação de assinaturas *on-line*, estão a *Dynamic Time Warping* (DTW) (do inglês, *Dynamic Time Warping*), os *Hidden Markov Model* (HMM) (do inglês, *Hidden Markov Models*) e as Redes Neurais.

O trabalho desenvolvido em [4] por Wei-Lun Chao é voltado para o reconhecimento facial de uma imagem, que utiliza uma foto tirada de uma câmera digital, e procura reconhecer se há alguma pessoa na foto. Para isso, Wei-Lun Chao divide o procedimento de reconhecimento facial em três etapas: detecção de rosto, extração de características, e reconhecimento facial. Sua metodologia utiliza módulos direcionados a identificar alguma

característica facial que identifique um indivíduo em uma foto, como a detecção da cor da pele, a conexão de partes segmentadas do rosto, verificação da região facial e a detecção de olhos e boca. Cada um, descarta características que não servem para identificar um rosto em uma imagem. Caso se esgotem as características faciais verificáveis pelo sistema, o mesmo não consegue identificar a um indivíduo em uma foto digital.

Em [30] Napa e Memon estudam a verificação de assinaturas *on-line* em dispositivos móveis sensíveis ao toque. As assinaturas coletadas são representadas por um vetor de características discriminativo, derivado de atributos de vários histogramas que podem ser computados em tempo linear. O modelo de assinatura resultante é compacto e requer espaço constante. As características obtidas e armazenadas em histogramas são concebidas para capturar atributos essenciais da assinatura, bem como relações entre estes atributos. Os histogramas são calculados pela divisão do intervalo de valores de um dado atributo. O processo de extração de características desse sistema converte os dados da série temporal de uma assinatura para uma sequência de vetores e atributos cartesianos. Em seguida, cada vetor cartesiano também é convertido em um vetor no sistema de coordenadas polares. Finalmente, histogramas são extraídos dessas sequências de vetores, formando o *template* do usuário. Na etapa de *matching* a assinatura submetida à verificação é autenticada se a distância de Manhattan entre os vetores de características biométricas da assinatura de teste e *template* é inferior a um limiar pré-definido, caso contrário, ele é rejeitado. O algoritmo foi testado sobre as bases de dados MCYT-100 e SUSIG, tomando-se 10 assinaturas para se gerar o *template* do usuário. Os resultados mostram que o desempenho da técnica proposta é relativamente elevado, apesar da sua simplicidade e eficiência, obtendo EER's de até 0.0044 em seus testes.

Zhong-Hua Quan, *et al.* desenvolvem em [27] o projeto de verificação de assinaturas *on-line* baseado na análise de espectros de janelas de assinaturas, que possuem tamanho variável. Primeiramente as assinaturas são divididas em um número de segmentos (janelas) com larguras variáveis , de acordo com as características de suas respectivas sequências temporais, e, após submetidas à etapa de pré-processamento, é usada a FFT para extrair o espectro das assinaturas. A distância entre os coeficientes de Fourier, extraídos das janelas correspondentes da assinatura de teste e da assinatura de referência, é calculada utilizando-se a distância Euclidiana e, em seguida, é empregada a decisão *Mahalanobis* como critério de autenticação da assinatura. Os resultados dos experimentos demonstram que a análise de espectro baseada em janelas com larguras variáveis é eficaz em sistemas baseados na verificação de sinais de assinaturas *on-line*, obtendo em seus testes um EER = 0,07.

O trabalho desenvolvido por Yanikoglu e Kholmatov em [41] propõe um sistema de verificação automático de assinaturas *on-line*, baseado na análise do espectro obtido, por meio da FFT, do sinal de uma assinatura. O sinal da assinatura é coletado por um *tablet* sensível ao toque. O *tablet* oferece uma interface capaz de capturar informações espaço temporais do sinal da assinatura, como as coordenadas dos pontos amostrados do traço da assinatura. Além disso, é possível também se obter valores de pressão submetidos pela ponta da caneta durante a ação de assinar. Toda assinatura coletada é submetida a etapas de pré-processamento e extração de características biométricas. A etapa de pré-processamento inclui a remoção de tempos de suspensão da ponta da caneta, a redução dos efeitos dos ruídos provenientes da interface de entrada, utilizando-se a regressão por mínimos quadrados, e a remoção do sinal médio das assinaturas utilizadas no processo de

geração do *template* do usuário. Esse sistema requer um tamanho único para os vetores utilizados na etapa de *matching*. Para isso, padronizam-se os tamanhos dos vetores realizando uma concatenação de zeros, até se atingir o comprimento da maior assinatura. Na etapa de extração de características biométricas, utiliza-se a FFT para se obter o espectro de frequências do sinal da assinatura, o qual é normalizado pela amplitude total do sinal. Além disso, metade dos coeficientes são descartados além do primeiro componente. Logo em seguida, os descritores passam por um processo de suavização, para se diminuir o efeito das componentes de maior frequência (ruídos) sobre o sinal a ser analisado. A etapa de *matching* utiliza como critério de autenticação, a medida normalizada da distância Euclidiana calculada entre os vetores de características biométricas da assinatura de teste e do *template* do usuário, que é comparada a um valor limiar previamente definido para o sistema. Se a distância calculada for inferior a tal limiar, o sinal é classificado como autêntico, caso contrário, como falsificado. Para a medir a performance do sistema, foram utilizadas as bases de dados *Ministerio de Ciencia y Tecnología* (MCYT) e SUSIG-Visual, obtendo valores de EER iguais a 0.121 e 0.062, respectivamente.

O trabalho proposto é baseado em na metodologia abordada em [41].

1.4 Organização do Trabalho

Este trabalho está dividido em sete capítulos, incluindo esta introdução. Os Capítulos 2, 3, 4 abordam a fundamentação teórica necessária para a compreensão deste trabalho. O Capítulo 5 apresenta detalhadamente a metodologia proposta neste trabalho. O Capítulo 6 trata da descrição de como foram realizados os testes e simulações para medida da performance do sistema, além da análise dos resultados obtidos. Por fim, o Capítulo 7 apresenta as conclusões sobre os resultados obtidos na metodologia proposta e, também, encontram-se sugestões para melhorias do trabalho atual e para trabalhos futuros.

Capítulo 2

Biometria

2.1 Definição de Biometria

O termo biometria é derivado do grego *bios* (vida) e *metron* (medida). Historicamente o termo é associado à parte da biologia que aplica métodos estatísticos em seres vivos [43]. De acordo com o dicionário Michaellis, biometria significa "Ciência da aplicação de métodos de estatística quantitativa a fatos biológicos; análise matemática de dados biológicos [18]. Nas artes plásticas, biometria refere-se ao uso de partes do corpo como referência métrica de proporcionalidade, utilizadas como base para criações artísticas do referido corpo [9].

Além das duas definições supracitadas, o termo biometria também é definido como "a identificação ou a verificação automática de identidade de um indivíduo com base em suas respectivas características fisiológicas e comportamentais"[34]. Nessa descrição, duas palavras são fundamentais para diferenciar biometria de outras ciências de identificação humana: automática e indivíduo [35].

Apesar de técnicas automáticas de identificação poderem ser usadas em objetos inanimados, animais, vegetais, ou até mesmo em seres sem vida, os temas de autenticação biométrica são voltados a humanos [6, 35]. Para limitação do escopo deste trabalho, será considerada a última definição.

2.2 Breve Visão Histórica da Biometria

A literatura científica sobre a medição quantitativa de características de seres humanos, com o propósito de identificar indivíduos, remonta a anos anteriores à década de 1870 [35]. Em 1879, o criminologista francês Alphonse Bertillon foi o primeiro a desenvolver um sistema de medidas corporais com o intuito de produzir uma descrição detalhada de um indivíduo. Tal sistema, que ficou conhecido como sistema de Bertillon ou *bertillonage* [10], foi adotado oficialmente pela polícia de Paris em 1882 e em 1887 foi introduzido nos EUA pelo major R. W. McClaughry, sendo rapidamente reconhecido e aceito como sistema de identificação em toda a Europa e Estados Unidos. Pela primeira vez na história, a padronização do sistema de Bertillon no mundo civilizado significava que qualquer indivíduo, devidamente classificado, poderia ser identificado positivamente em uma data

futura [21]. A Figura 2.1 a seguir, ilustra um cartão utilizado para registrar medidas antropométricas baseados no *bertillonage*.

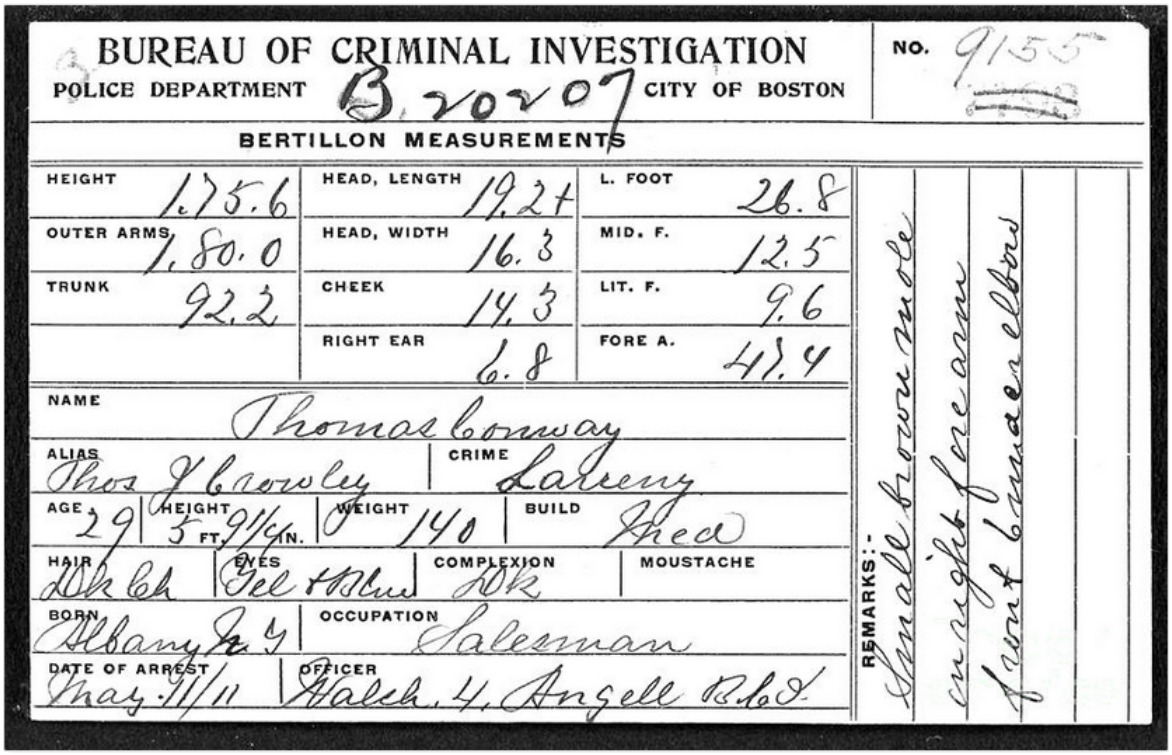

Figura 2.1: Cartão de medidas antropométricas do sistema de Bertillon, utilizado pelo Departamento de Polícia da cidade de Boston, EUA [1].

O sistema de Bertillon foi dominante como método de identificação criminal, tanto na Europa e nos EUA, até o início da década de 1920. Em 1903, o caso *West Brothers* demonstrou a confiabilidade da ciência emergente da identificação da impressão digital, proposta inicialmente na década 1880 por Henry Faulds, William Herschel e Francis Galton [5, 8, 10].

O desenvolvimento de técnicas de processamento de sinais digitais no século XX, permitiu a automação do processo de identificação humana, tomando-se como base ideias e técnicas concebidas a séculos ou milhares de anos atrás [17, 35]. Sistemas biométricos de reconhecimento de voz e impressão digital estavam entre os primeiros que foram experimentados com o advento dos computadores, obtendo no início da década de 1960, o reconhecimento do potencial de aplicabilidade de tais tecnologias no processo de reconhecimento e identificação de pessoas. Na década de 1970, sistemas biométricos já eram testados em larga escala, como o sistema baseado na geometria da mão, bastante utilizado por instituições governamentais. Sistemas de verificação de retina e assinatura se tornaram viáveis na década de 1980, seguidos por sistemas de verificação facial. Na década de 1990 foi desenvolvido o sistema de reconhecimento de retina, bastante utilizado em enredos de filmes de ficção científica [35].

2.3 Conceitos e Taxionomia de Uso

A escolha adequada do identificador biométrico a ser coletado por uma determinada aplicação depende de uma variedade de questões, além de seu desempenho correspondente. Uma característica fisiológica ou comportamental é assumida como um identificador biométrico caso satisfaça aos seguintes requisitos básicos [11, 12]:

- Universalidade: todo indivíduo a ser autenticado pela aplicação deve possuir a característica biométrica.
- Unicidade: a probabilidade de dois indivíduos distintos possuírem características idênticas deve ser nula ou desprezível.
- Permanência: a característica biométrica deve ser suficientemente invariante sob um período de tempo, para se poder assegurar a performance do respectivo algoritmo de correspondência.
- Aceitabilidade: os indivíduos direcionados ao uso da aplicação, devem estar dispostos a apresentar seus traços biométricos requisitados.
- Performance: a precisão e os recursos utilizados no processo de reconhecimento, devem atender às restrições impostas pela aplicação.
- Mensurabilidade: a característica a ser coletada deve ser passível de mensuração por meio de um dispositivo adequado.
- Proteção: consiste na facilidade ou dificuldade de impostores conseguirem burlar o sistema, por meio de técnicas fraudulentas.

Características classificadas como fisiológicas relacionam-se às medidas físicas do corpo de uma pessoa e, geralmente, são as mais utilizados em sistemas biométricos. Exemplos de identificadores fisiológicos: a face, íris, retina, impressão digital, geometria da mão e veias das mãos. Já as características classificadas como comportamentais, relacionam-se à padrões comportamentais de um indivíduo, que incluem o ritmo de digitação, a forma como anda, voz, letras manuscritas e padrão de assinatura [12].

Um sistema biométrico pode ser designado a testar uma, e somente uma, de duas hipóteses possíveis [35]:

1. as amostras submetidas pertencem a um indivíduo conhecido para o sistema;
2. as amostras submetidas pertencem a um indivíduo desconhecido para o sistema.

Aplicações que testam a primeira hipótese são conhecidas como sistemas de identificação positiva, enquanto as aplicações que testam a segunda hipótese são conhecidas como sistemas de identificação negativa. Qualquer sistema biométrico enquadra-se exclusivamente em uma das hipóteses, já que, as identificações positiva e negativa são duais reciprocamente. Essa distinção entre tais sistemas é fundamental, pois, possui potencial influência em arquiteturas, vulnerabilidades e as taxas de erro da aplicação [35].

Sistemas de identificação positiva geralmente servem para prevenir a associação de múltiplos usuários a uma única identidade, enquanto os sistemas de identificação negativa servem para prevenir a associação de múltiplas identidades a um único usuário [35].

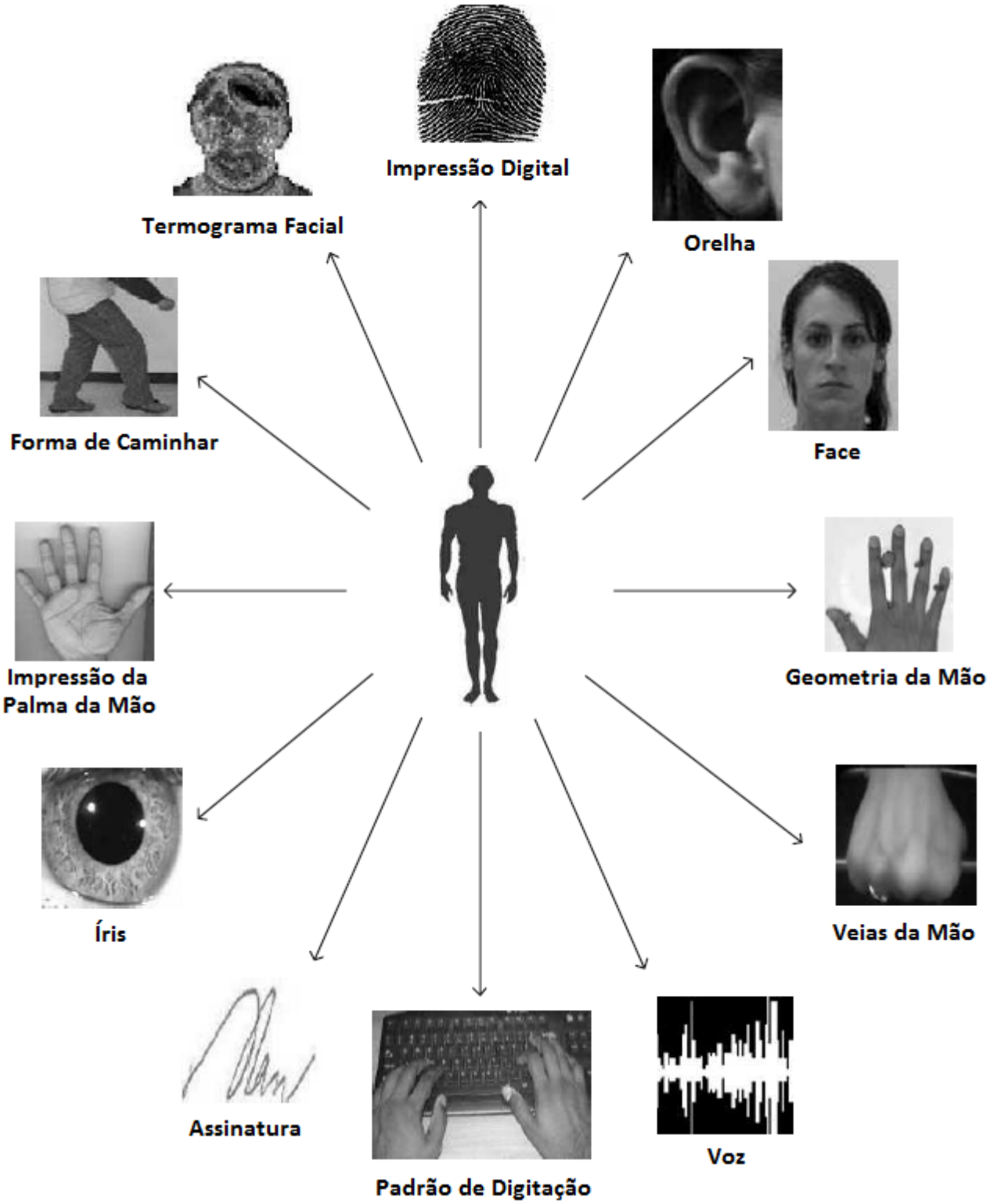

Figura 2.2: Exemplos de características biométricas que podem ser utilizadas no processo de autenticação de um indivíduo. Traços físicos incluem impressão digital, íris, face e geometria da mão, enquanto traços comportamentais incluem assinatura, dinâmica de digitação e forma de caminhar [12].

Em sistemas de identificação positiva, as características biométricas de referência de cada usuário podem ser armazenadas de maneira centralizada ou descentralizada, pois, uma amostra submetida ao sistema é comparada a somente uma amostra de referência registrada. Já em sistemas de identificação negativa, há a exigência de um modelo de armazenamento centralizado, uma vez que, a amostra submetida à aplicação deve ser comparada com todas as amostras armazenadas no sistema [35].

É importante saber que sistemas biométricos podem analisar as características biométricas de um sinal sob duas perspectivas distintas, que são a análise global ou local de características. Sistemas biométricos que se baseiam em características globais de um sinal, geralmente extraem informações do sinal como um todo. Já sistemas baseados em características locais, extraem informações biométricas de partes do sinal, de maneira independente. Tais abordagens podem influenciar diretamente a performance do sistema, além de poderem ser combinadas no processo de reconhecimento de um indivíduo [7].

2.4 Terminologias

Historicamente, sistemas de identificação positiva e negativa foram associados a termos que denotam suas diferenças. O primeiro passou a ser conhecido, também, como um sistema que produz como resultado uma verificação (correspondência 1:1), enquanto o segundo, como um sistema que produz como resultado uma identificação (correspondência 1:N) [35, 40].

Porém, os termos reconhecimento, verificação e identificação são muitas vezes utilizados de maneira indistinta. Em particular, a dicotomia entre os termos verificação e identificação fica ainda mais obscura com a criação de sistemas poucos-para-muitos que não podem ser consistentemente classificados como de verificação ou identificação exclusivamente. Estratégias de busca e usos de sistemas biométricos têm-se expandido ao ponto onde a distinção entre verificação e identificação, em conjunto com as correspondências 1:1 e 1:N, já não é totalmente informativa [35]. Para elucidar a diferença entre tais termos, uma breve descrição de cada uma deles é dado a seguir:

- **Reconhecimento:** é um termo genérico e não implica necessariamente qualquer atividade de verificação ou identificação. Todos os sistemas biométricos executam reconhecimento de uma pessoa que tenha sido previamente registrada no sistema [22];
- **Verificação:** conhecido também como autenticação, é o processo em que o sistema biométrico tenta confirmar a identidade de um indivíduo, já registrado, que se declara usuário do sistema, a partir da submissão de uma nova amostra que é comparada a um ou mais modelos previamente inscritos [2, 22];
- **Identificação:** é uma tarefa em que o sistema biométrico tenta determinar a identidade de um indivíduo. Uma nova amostra é recolhida e comparada a todos os modelos biométricos de usuários previamente cadastrados em um banco de dados. A aplicação deve determinar se o indivíduo está registrado no banco de dados do sistema [22].

2.5 Tipos de Tecnologias Biométricas

As características biométricas podem ser classificadas como pertencentes a uma das seguintes classes: fisiológica ou comportamental. A Figura 2.3 ilustra a classificação de alguns sistemas biométricos.

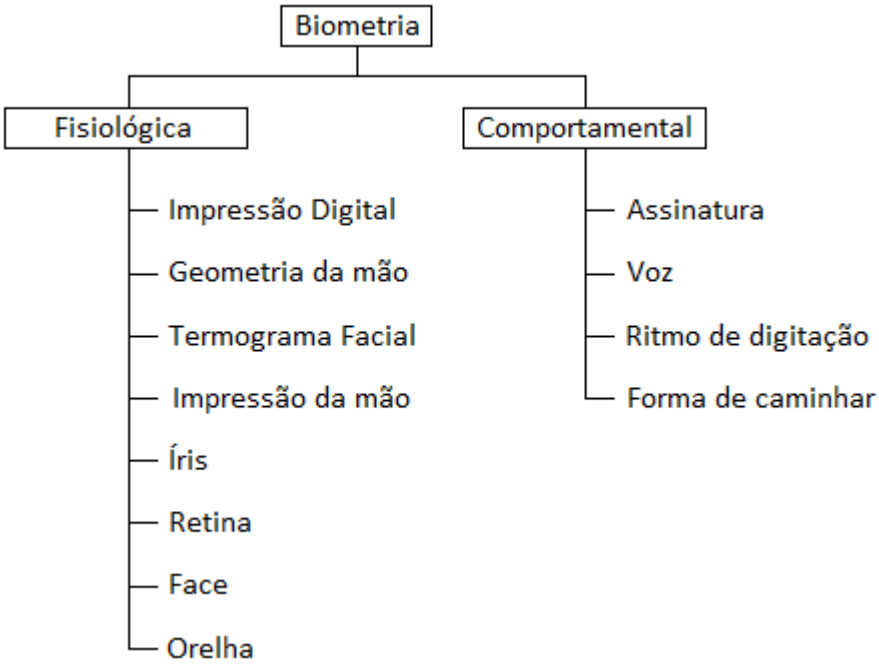

Figura 2.3: Classificação das características biométricas: Fisiológica ou Comportamental. (adaptada de [6])

A biometria fisiológica mede partes específicas do corpo de um indivíduo [6]. Os principais sistemas biométricos classificados como fisiológicos, incluem:

- **Reconhecimento de impressão digital**: Considerada a "mãe"dos sistemas biométricos [43], baseia-se no padrão de nervuras e sulcos na superfície de uma ponta do dedo, determinado durante o período fetal. Tais nervuras e sulcos são tão diferentes entre pessoas que até mesmo as impressões digitais entre gêmeos univitelinos são diferentes como, também, são as impressões em cada dedo da mesma pessoa [15].
- **Reconhecimento de geometria da mão**: A geometria de toda mão humana é bastante singular, quase tanto como impressões digitais. Sistemas de reconhecimento da geometria da mão são baseadas em medições que podem levar em consideração a forma da mão, o tamanho da palma da mão, comprimentos e larguras dos dedos, ângulos entre dedos, geometria de toda a coleção de 27 ossos, além de músculos, ligamentos e outros tecidos [6, 12].
- **Reconhecimento de termograma facial**: A tecnologia é baseada no reconhecimento de padrões extraídos do sistema vascular subjacente ao tecido facial do indivíduo. Tais padrões podem ser capturados utilizando uma câmara de infravermelhos, resultando em uma imagem chamada *termograma facial*. Afirma-se que

um termograma facial é exclusivo a cada indivíduo e não é vulnerável a disfarces. Mesmo quando submetido a uma cirurgia plástica, caso não ocorra algum redirecionamento do fluxo de sangue através das veias do rosto do indivíduo, acredita-se que não afeta a performance do sistema de termograma facial [11].

- **Reconhecimento de impressão da palma da mão**: As palmas de mãos humanas contêm padrões de nervuras e sulcos bastante semelhantes às apresentadas por impressões digitais. Porém, como a área da palma da mão é relativamente maior que a área da superfície de um dedo, espera-se que as impressões palmares possuam um maior potencial de diferenciação quando comparadas às impressões digitais. Além disso, palmas de mãos humanas contêm outras características distintivas adicionais, tais como as linhas e rugas principais que podem ser coletadas por digitalizadores de imagem de baixa resolução [42].

- **Reconhecimento de veias da mão**: O sistema de reconhecimento de padrões vasculares de veias da mão, utiliza uma câmera infravermelha para adquirir o modelo dos vasos sanguíneos do dorso da mão. Quando submetida à radiação infravermelha, a hemoglobina desoxidada nos vasos sanguíneos absorve os raios infravermelhos, que permite à câmera captar os padrões vasculares contidos na mão que, em seguida, passam por um ou mais algoritmos de processamento de sinais digitais. Por fim, o padrão vascular extraído é então comparado com padrões pré-registados em dispositivos de armazenamento, concluindo o processo de autenticação ou identificação do indivíduo [12].

- **Reconhecimento de íris**: A íris humana é o conjunto de músculos responsáveis pelo controle da dilatação ou contração da pupila, e estão compreendidos entre a pupila e a esclera (parte branca do olho). A estrutura complexa desses músculos, que podem se apresentar nas cores marrom, cinza, azul ou verde, se mostra útil como recurso para o desenvolvimento de um sistema biométrico. O reconhecimento da íris inicia-se com a demarcação da íris em uma imagem, a partir de suas fronteiras internas e externas, detectando os limites da pálpebra superior e inferior, excluindo os cílios sobrepostos ou reflexões a partir da córnea ou óculos. Em seguida, essa imagem passa por outras etapas de pré-processamento, para então, ser utilizado um algoritmo adequado de correspondência[6, 11, 12, 28].

- **Reconhecimento de retina**: A retina compõe a superfície da parte traseira do interior do olho. Normalmente, não é possível enxergá-la a olho nú exceto sob a consulta de médicos oftalmologistas ou quando mostra-se em fotos com olho vermelho, que é o reflexo da retina quando submetida ao *flash* da máquina fotográfica [6]. Para o funcionamento do sistema, o olho do usuário deve ser posicionado em frente a um dispositivo ocular, a uma distância aproximada de 7,5 cm, buscando focar um ponto verde por alguns segundos. Isso é necessário para que o digitalizador de imagens possa capturar o padrão da retina com seu posicionamento suficientemente centralizado. Uma área conhecida como *fóvea*, situada no centro da retina e responsável pela formação das imagens que serão transmitidas ao cérebro, é digitalizada e o padrão único dos vasos sanguíneos é capturado [43].

- **Reconhecimento facial**: As abordagens utilizadas em sistemas de reconhecimento facial geralmente são baseadas na localização e na forma de alguns componentes que

compõem o rosto do usuário. O sistema utiliza medidas do formato dos olhos, sobrancelhas, nariz, lábios e queixo, além de suas relações espaciais [11]. O processo de reconhecimento de um indivíduo, registrado na base de dados da aplicação, é dividido em três fases de maneira simplificada: detecção, normalização e reconhecimento de faces. A fase de detecção é o momento em que a imagem facial é obtida. Já a fase de normalização possui função fundamental de padronização das imagens obtidas, para que se possa unificar a maneira como são tratadas as imagens registradas no banco de dados da aplicação. Finalmente, após a fase de detecção e normalização contemplamos a fase de reconhecimento de face, a qual avalia a imagem a ser reconhecida, comparando com as imagens de referência persistidas no banco de dados da aplicação [4].

- **Reconhecimento auricular**: O sistema baseia-se em padrões extraídos de partes da orelha, como: lobo, concha, escafa e hélice. Alfred Iannarelli desenvolveu um sistema de classificação de orelhas por volta da década de 1950, o qual consistia em obter oito medidas de uma imagem auricular, que era dividida em forma de pizza, com cada fatia separada por um ângulo de 45 graus a partir de um referencial previamente definido [12].

Já a biometria comportamental concentra-se em medir padrões comportamentais do indivíduo, obtendo características de natureza dinâmica, ao contrário das características fisiológicas, que são consideradas estáticas [6]. Os principais sistemas biométricos classificados como comportamentais, incluem:

- **Reconhecimento de assinaturas**: Os sistemas de reconhecimento de assinaturas utilizam métodos para reconhecer automaticamente assinaturas a mão de um indivíduo, sendo esses sistemas classificados em duas categorias: *off-line* (estática) ou *on-line* (dinâmica). [20]. Sistemas baseados em assinaturas *off-line* utilizam somente a forma (desenho) da assinatura digitalizada de algum documento, obtendo-se características geométricas que, em seguida, são submetidas a uma série de procedimentos necessários para que seja possível extrair padrões adequados e suficientes para se realizar a tarefa de reconhecimento biométrico. Em sistemas baseados em assinaturas *on-line*, as assinaturas são obtidas em tempo real, a partir de dispositivos especializados em coletar medidas dinâmicas através do tempo, incluindo [29]: posição da caneta, pressão da caneta, azimute e o ângulo inclinação da caneta com relação ao plano da assinatura (ver Figura 6.2). Depois de capturadas tais características, o sistema pode analizar padrões contidos na assinatura relativos à forma da assinatura, velocidade, aceleração, tempo de suspensão da ponta da caneta, dentre outros [41].

- **Reconhecimento de Voz**: Sistemas de reconhecimento de voz utilizam um captador de áudio para obter a fala de um usuário, que pode ser uma palavra previamente selecionada (sistema dependente de texto) ou uma frase aleatória (sistema independente texto). Esse processo geralmente é repetido um número determinado de vezes para construir um perfil de voz do usuário [43]. Abordagens dependentes de texto são computacionalmente menos custosas que as independentes de texto, uma vez que, o sistema busca uma correspondência direta da palavra ou frase falada pelo usuário e seu modelo de referência armazenado [29].

- **Ritmo de Digitação**: Atua sobre a suposição de que cada pessoa possui sua própria maneira de digitar. Porém, não se espera que essa evidência biométrica seja única para cada indivíduo, entretanto, esse traço pode oferecer informações suficientes para permitir a verificação da identidade de uma pessoa. Uma das vantagens apresentadas por este tipo de tecnologia é a possibilidade de se permitir uma verificação contínua do usuário, a partir da monitoração de combinações de teclas digitadas durante o intervalo de tempo de uso do sistema [12].
- **Forma de Caminhar**: Baseia-se no padrão de caminhada de uma pessoa. As principais abordagens utilizadas na implementação desse tipo de biometria são baseadas em visão computacional ou em uso de sensores. A abordagem baseada em sensores é menos tradicional e menos flexível que a baseada em visão computacional, e pode se valer do uso de acelerômetros presos à tíbia de uma pessoa, que adquirem dados dinamicamente, obtendo a aceleração dos movimentos da perna em três direções ortogonais [29].

2.6 Funcionamento de Sistemas Biométricos

O reconhecimento biométrico é alcançado pela comparação de amostras biométricas adquiridas (amostras de consulta) com uma ou mais amostras que foram capturadas e armazenadas previamente na base de dados do sistema (amostras de referência) [14]. Geralmente, todos os sistemas biométricos são divididos em duas partes, parte de inscrição e parte de autenticação/identificação [43], as quais, em conjunto, podem ser subdivididas em cinco subsistemas: coleta de dados, pré-processamento, extração de características biométricas, gerador de *template* e o comparador e classificador de amostras, como ilustrado na Figura 2.4:

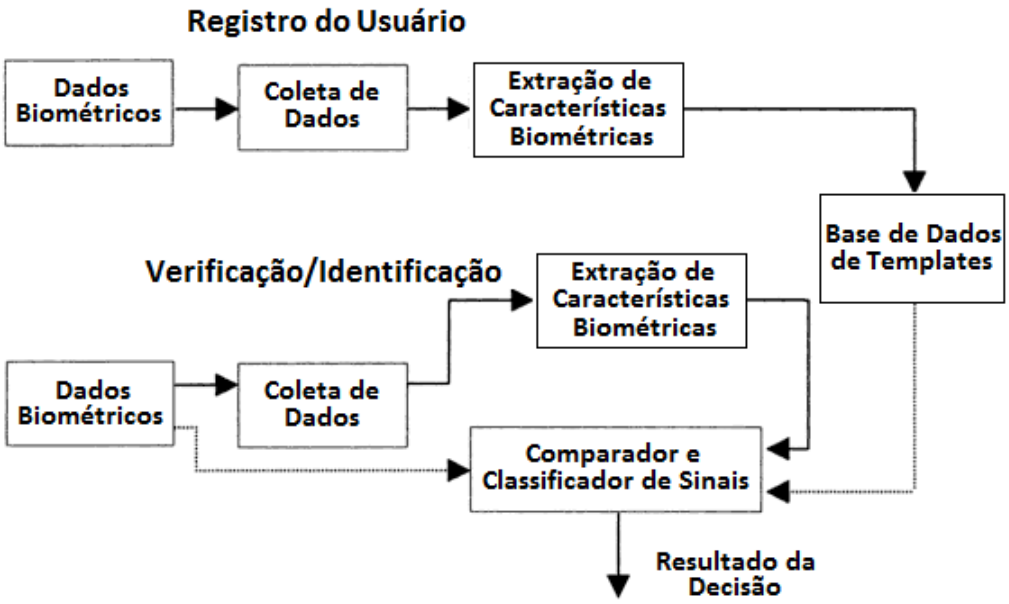

Figura 2.4: Procedimentos gerais de um sistema biométrico (adaptada de [43]).

O processo de criação da base de dados é chamado de *inscrição*. Já o processo de comparação de amostras é chamado de *verificação*, caso a amostra de consulta venha acompanhada de uma identidade reivindicada do usuário, ou identificação, se nenhuma reivindicação de identidade é feita (neste caso, a amostra de *consulta* é comparada com todas as amostras de *referência* da base de dados) [14].

As amostras biométricas são adquiridas por dispositivos capazes de produzir uma representação eletrônica do sinal de entrada, os quais atuam como interface entre o usuário e o sistema. Tais sinais não são comparados diretamente, ao invés disso, uma representação mais compacta do sinal, chamada de *template*, é extraída e usada posteriormente para comparação [14].

Os processos usados para a realização da comparação das amostras são chamados de algoritmos biométricos e objetivam avaliar e melhorar a qualidade do sinal biométrico, extraindo e combinando suas características mais relevantes, além de fundir as informações das várias fases de processamento para se obter uma performance adequada de verificação/identificação, requerida por uma determinada aplicação [14].

No estágio de classificação da amostra de consulta, o sistema deve decidir se o modelo extraído da nova amostra corresponde ao registrado no sistema. Para isso, uma pontuação é calculada para se medir o grau de similaridade entre tais amostras, a fim de se classificar o novo sinal como *autêntico* ou *forjado*. Caso a pontuação seja inferior a um limite definido, o sistema pode classificar o sinal como autêntico ou, caso contrário, como fojado.

Pela figura 2.4 é fácil perceber que os dois primeiros estágios (coleta de dados e extração de características) são idênticos nas partes de inscrição e identificação. Desta forma, e de maneira mais geral, sistemas biométricos genéricos são concebidos para atender as quatro partes de processamento ilustradas na Figura 2.5 [43]:

Figura 2.5: Procedimentos gerais de um sistema biométrico genérico com quatro etapas de processamento (adaptada de [43]).

2.7 Performance de um Sistema Biométrico

A avaliação de um sistema de verificação exige a análise de dois tipos de erro. A percentagem de assinaturas genuínas que são erroneamente rejeitadas pelo sistema é conhecida como a taxa de falsa rejeição (do inglês, *False Rejection Rate* (FRR)). Já percentagem de falsificações indevidamente aceitas é chamada de taxa de falsa aceitação (do inglês, *False Acceptance Rate* (FAR)). Os dois tipos de erros normalmente têm diferentes custos associados à eles, dependendo dos requisitos de segurança da aplicação. [12]

O desempenho de um sistema biométrico é normalmente dado pela taxa de erro equivalente (do inglês *Equal Error Rate* EER), ou seja, é o ponto em que a taxa de falsa aceitação e a taxa de falsa rejeição são aproximadamente as mesmas. A EER pode ser obtida graficamente observando-se a ordenada do ponto de interseção entre os gráficos das FRR e FAR.

Uma medida de desempenho mais significativa é a curva DET (do inglês, *Detection Error Trade-off*), que mostra como um erro muda com relação ao outro. A Figura 2.6 ilustra o comportamento comum de uma curva de DET. O eixo x representa a taxa de falsa rejeição e o eixo y representa a taxa de falsa aceitação.

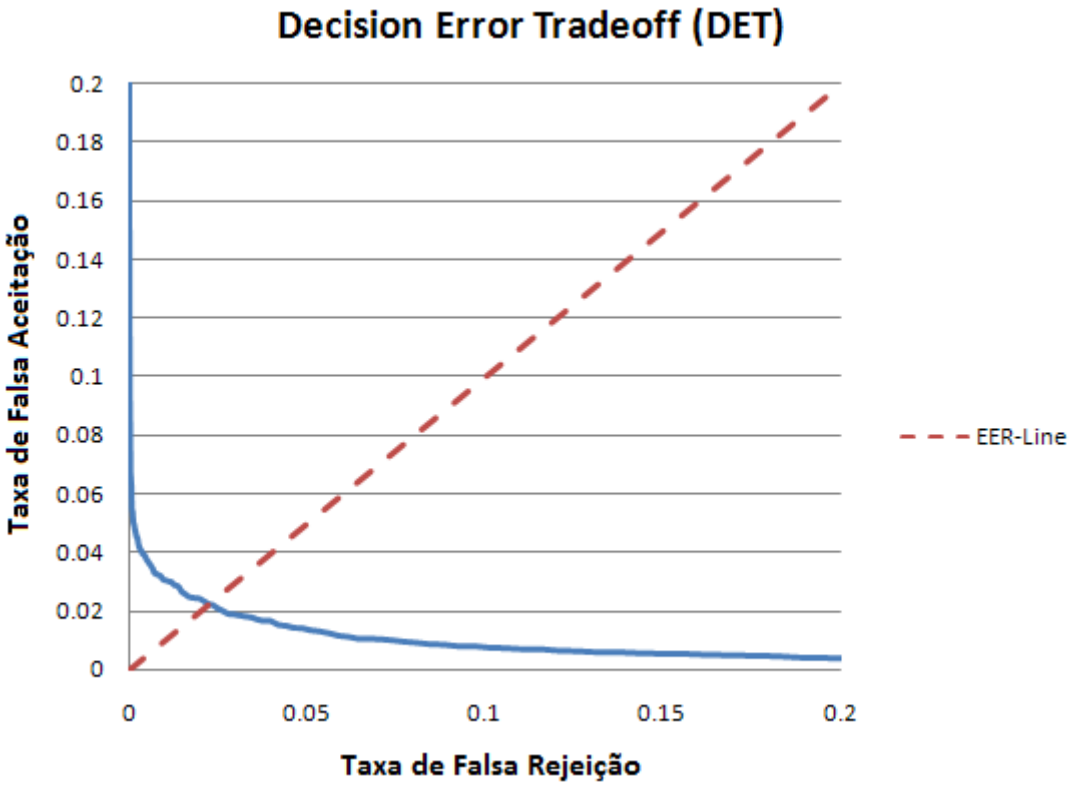

Figura 2.6: Exemplo da DET (adaptada de [3]).

Para denotar a importância das informações que podem ser extraídas da curva DET, considere um sistema possui como requisito fundamental a alta segurança, ou seja, a FAR deve ser a menor possível. Desta forma, de acordo com gráfico DET, isso eleva a FRR, podendo provocar aborrecimentos ao usuário do sistema. Esse simples exemplo mostra a relação matemática entre as FAR e FRR, que apresentam comportamento no mínimo semelhante à grandezas inversamente proporcionais. Portanto, caso uma das taxas é incrementada, necessariamente a outra será decrementada, e vice-versa.

No próximo Capítulo, *Sinais e Sistemas*, serão apresentados conceitos e definições de sinais e sistemas, além de se investigar e caracterizar os sinais periódicos, aperiódicos, contínuos ou discretos. Este Capítulo aborda também, na Seção 3.4, o tópico *Processamento de Sinais*, que apresenta os tipos de tecnologias de sistemas de processamento de sinais.

Capítulo 3

Sinais e Sistemas

Neste Capítulo serão abordados conceitos que formarão base para a compreensão do Capítulo 4. Na Seção 3.1 são definidos os significados de sinal e de sistema. A Seção 3.2 faz referência às características dos dois tipos básicos de sinais: de tempo contínuo e de tempo discreto. Na Seção 3.3 define-se o que são sinais períodicos. Por fim, na Seção 3.4 fala-se sobre processamento de sinais (atividade principal de um sistema), aprensentando metodologias utilizadas e as principais tecnologias de aplicação.

3.1 Definição de Sinais e Sistemas

Um sinal é qualquer fenômeno que pode ser descrito por uma função de variável(is) independente(s) que carrega alguma informação. Pode ser visto, também, como uma quantidade física que varia durante o tempo, espaço ou em qualquer outra variável independente, pela qual, alguma informação pode ser transportada [36]. Sinais com somenete uma variável independente são chamados de sinais unidimencionais, já aqueles com mais de uma variável independente são chamados de sinais multidimenssionais.

Já um sistema pode ser definido como uma função que transforma sinais de entrada em sinais de saída 3.1, em outras palavras, um sistema é um processador de sinais. Sistemas são frequentemente denotados por diagramas de blocos, como ilustrado na Figura, em que x representa um sinal de entrada e y um sinal de saída [36].

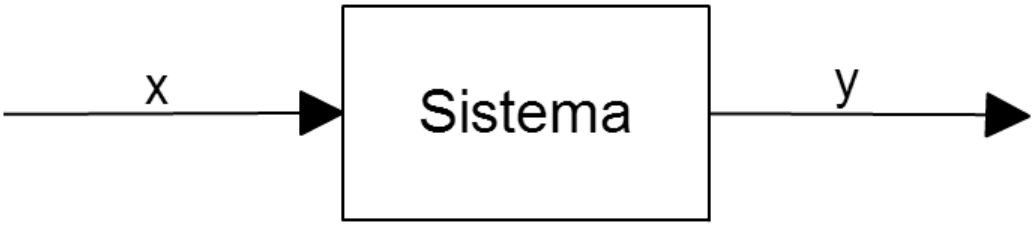

Figura 3.1: Diagrama de blocos denotando um sistema genérico.

3.2 Sinais de Tempo Contínuo e Tempo Discreto

Existem dois tipos básicos de sinais: sinais de tempo contínuo e sinais de tempo discreto. No caso de sinais de tempo contínuo, podemos representá-los como uma função cuja variável independente é contínua. Por outro lado, sinais de tempo discreto são definidos somente em instantes discretos de tempo, ou seja, tais sinais podem ser representados por funções cuja variável independente assume apenas um conjunto discreto de valores [23].

Neste trabalho, para distinguir os sinais de tempo contínuo dos sinais de tempo discreto, usaremos o símbolo t para representar a variável independente de tempo contínuo e n para representar a variável independente de tempo discreto. Além disso, encapsularemos entre parêncteses (.) a variável intependente t em funções usadas para descrever sinais de tempo contínuo, e para funções de sinais de tempo discreto, utilizaremos a variável independente n entre colchetes [.].

O desenvolvimento dos processadores digitais modernos, permitiu a implementação de vários sistemas práticos, como os de áudio e de vídeo digitais. Sistemas desse tipo necessitam criar uma versão amostrada do sinal em tempo contínuo, na forma de sequências de tempo discreto [23]. É importante salientar que a etapa de amostragem de sinais analógicos (tempo contínuo) é de suma importância para o desempenho de sistemas baseados em Processamento Digital de Sinais (PDS) que ao final do processamento retornam um sinal analógico. Tais sistemas baseam-se em teorias matemáticas como o *Teorema de Nyquist*, o qual afirma que a frequência de amostragem de um sinal analógico deve ser no mínimo igual ou superior ao dobro da frequência desse sinal, para que possa posteriormente ser recuperado com a menor perda possível de informação [24]. A Figura 3.2 ilustra a versão x[t] obtida a partir da amostragem de um sinal x(t).

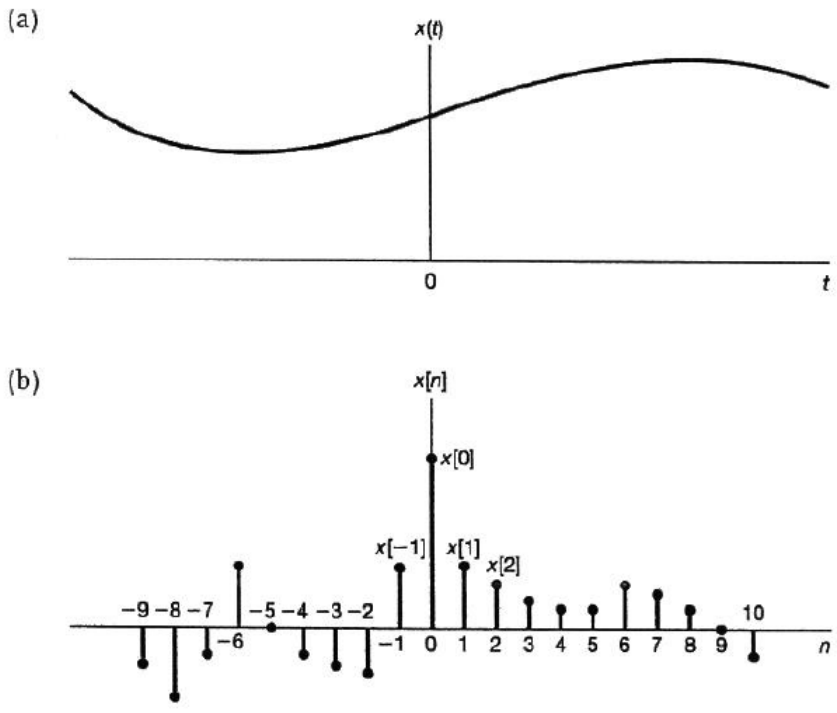

Figura 3.2: Exemplos de sinais: **(a)** sinal contínuo x(t). **(b)** sinal discreto $x[t]$

3.3 Sinais Periódicos e Sinais Aperiódicos

Um sinal $x(t)$ é dito periódico de tempo contínuo caso exista um valor positivo T em que

$$x(t) = x(t + T), \tag{3.1}$$

para todos os valores de t. Nesse caso, dizemos que x(t) é periódico com período T.

Sinais periódicos em tempo discreto são definidos de forma análoga. Um sinal x[n] é dito periódico em tempo discreto caso exista um valor N $\in \mathbb{Z}_+^*$ em que

$$x[n] = x[n + N], \tag{3.2}$$

$\forall$ n $\in \mathbb{Z}$. Caso a Equação 3.2 seja válida, então, x[n] é periódico com período 2N, 3N, ... O período fundamental N_0 é o menor valor de N para o qual a Equação 3.2 é válida [23].

Dizemos também, que sinais constantes no tempo como $x(t) = x$ ou $x[n] = k$, são periódicos para qualquer $T > 0$ e $N > 0$, respectivamente.

Já sinais aperiódicos, são aqueles que não podem ser modelados a partir das Equações 3.1 e 3.2.

3.4 Processamento de Sinais

O processamento de sinais é a tecnologia que possibilita a geração, análise, transformação e interpretação da informação, compondo a atividade principal de um sistema. A análise e a transformação tomam por base o uso de teorias, aplicações e algoritmos, de forma a extrair informações dos sinais de entrada para torná-los mais apropriados à alguma aplicação específica [26]. O processamento de sinais pode ser feito de forma analógica ou digital.

Para extrair informações em um processamento de sinal pode-se utilizar matemática, estatística, computação, heurística e representações linguísticas, formalismos e técnicas de representação, modelagem, análise, síntese, descoberta, recuperação, detecção, aquisição, extração e métodos de aprendizagem [19].

Técnicas de processamento de sinais são de interesse não somente das engenharias de forma geral, como também, podemos citar as áreas de controle, análise de sistemas físicos, economia, biologia e saúde [37]. Tecnologias de processamento de sinais podem ser classificadas como:

- **Processamento Analógico de Sinais (PAS):** É todo processamento realizado sob sinais de natureza analógica (contínuo no tempo) utilizando somente dispositivos de processamento analógico, ou seja, não digitais. Esse tipo de processamento é direcionado à sinais que ainda não foram digitalizados, como em sinais de rádio, sistemas de televisão, telefone e radar. Exemplos de sistemas de PAS incluem: filtros passivos, filtros ativos, circuitos integradores, amplificadores, osciladores, entre outros.
- **Processamento Digital de Sinais (PDS):** É todo processamento que atua sobre uma sequência temporal de valores, onde cada valor da sequência é chamado de

amostra do sinal. Essa classe de processamento geralmente utiliza funções de domínio inteiro para descrever/representar matematicamente o sinal amostrado. Desta forma, sinais de natureza contínua (sinais analógicos) podem ser analizados sob a perspectiva discreta, após a aquisição de alguns de seus valores a uma taxa definida de tempo. Normalmente, o primeiro passo para a conversão do sinal analógico para o digital, é a realização da amostragem do sinal utilizando um conversor analógico-digital, que transforma o sinal analógico em um fluxo de valores digitais discretos. A amostragem do sinal compõe uma parte de suma importância para o desenpenho de sistemas baseados em PDS, a qual, vale-se do uso de teorias matemáticas como o *Teorema de Nyquist* [24], o qual define que para um sinal poder ser reconstruído com o mínimo de perda de informação, a frequência de amostragem de um sinal analógico deve ser no mínimo duas vezes maior que a frequência do espectro desse sinal. O PDS oferece várias vantagens quando comparado ao PAS como: detecção/correção de erros de transmissão e a compressão de dados. Aplicações para PDS incluem: processamento de sinal de áudio, fala, sonar, radar, estimação espectral, estatística, imagens digitais, processamento para comunicações, controle de sistemas, biomedicina, processamento de dados sismológicos, entre outros [32].

No próximo Capítulo, *Transformadas de Fourier*, será apresentado brevemente parte da análise de Fourier, que inclui o estudo das peculiares série e transformadas de Fourier, de fundamental importância para a implementação do trabalho proposto.

Capítulo 4

Transformadas de Fourier

O desafio de decompor funções arbitrárias em termos de funções trigonométricas simples foi de interesse de grandes nomes da matemática por volta de 1750 com L. Euler (1707-1783) e D. Bernoulli (1700-1782), seguindo com J. d'Alembert (1717-1783) e J. L. Lagrange [38].

Mais tarde, o matemático e físico francês Jean-Baptiste Joseph Fourier (1768-1830), motivado por suas análises e observações sobre o fenômeno da "propagação e difusão do calor", estudou sistematicamente tais séries infinitas, na tentativa de resolver a equação da onda. Em 1811, em sua obra intitulada *Théorie mathématique de la chaleur* (Teoria matemática de condução do calor), Fourier explicitou os coeficientes de tais séries infinitas, que ficaram conhecidos como coeficientes de Fourier e, além disso, afirmou que qualquer sinal periódico, contínuo ou descontínuo, poderia ser representado por meio de sua teoria. Porém, P. G. Dirichlet (1805-1859) foi um dos primeiros a reconhecer que nem toda função poderia ser representada por uma série de Fourier [23, 38].

A análise de Fourier, também conhecida como análise harmônica clássica, é a teoria das séries e transformadas de Fourier. Tal teoria possui larga aplicabilidade em diversas áreas das ciências aplicadas e engenharia, constituindo a base do processamento de sinais, em particular [26].

Este capítulo objetiva apresentar a análise de Fourier de maneira resumida, posto que, uma de suas transformadas é utilizada como recurso fundamental pela metodologia proposta neste trabalho. Na Seção 4.1 fala-se sobre a *Série de Fourier*, apresentando sua definição e algumas de suas possíveis formas de representação. As Seções 4.2, 4.3 e 4.4 tratam das Trasformada de Fourier de Tempo Contínuo (TFTC), Trasformada de Fourier de Tempo Discreto (TFTD) e *Discrete Fourier Transform* (DFT), respectivamente. O Capítulo termina com a Seção 4.5, que aborda a FFT que é a transformada utilizada na implementação do trablho proposto.

4.1 A Série de Fourier

A série de Fourier é uma ferramenta matemática que permite a qualquer sinal periódico ser decomposto em uma soma infinita de senóides, desde que respeitadas as condições de Dirichlet [36]. É uma importante técnica para análise do conteúdo de frequência de um sinal e para o entendimento das transformadas de Fourier [13].

4.1.1 Representação da Série de Fourier na Forma Retangular

Uma série rectangular representa um sinal por meio de adições de senos e cosenos. Considere uma função $f(t)$, periódica com período T, a qual satisfaz as seguintes condições de Dirichlet [38]:

- A função é unívoca e contínua, exceto em um número finito de descontinuidades ordinárias pertencentes a qualquer intervalo de período T;
- A função tem um número finito de máximos e mínimos em um período T;
- A função é absolutamente integrável, ou seja, a integral $\int_0^T |f(t)|dt$, converge.

Então, define-se a Série de Fourier de uma função f como a série trigonométrica em termos dos coeficientes a_n e b_n, dada por:

$$f(t) = \frac{a_0}{2} + \sum_{n=1}^{+\infty} \left[a_n . \cos\left(\frac{n2\pi t}{T}\right) + b_n . sen\left(\frac{n2\pi t}{T}\right) \right], \tag{4.1}$$

em que,

$$a_n = \frac{2}{T} \int_{-\frac{T}{2}}^{\frac{T}{2}} f(t).cos\left(\frac{n2\pi t}{T}\right) dt \ , \ n \in \mathbb{Z}_+^* \tag{4.2}$$

e

$$b_n = \frac{2}{T} \int_{-\frac{T}{2}}^{\frac{T}{2}} f(t).sen\left(\frac{n2\pi t}{T}\right) dt \ , \ n \in \mathbb{Z}_+^*. \tag{4.3}$$

Sabendo que o período fundamental T_0 de f é o menor valor positivo e não nulo de T, para o qual o sinal seja periódico, podemos obter a frequência angular fundamental ω_0 do sinal f como:

$$\omega_0 = \frac{2\pi}{T_0}. \tag{4.4}$$

A frequência angular fundamental ω_0, dada em radianos por unidade de tempo, é o principal componente da série harmônica de um sinal periódico. Pela Equação 4.1, é fácil perceber que para todo $n \neq 1$ os componentes de frequência do sinal f são múltiplos inteiros da frequência fundamental.

$$\omega_0 = \frac{2\pi}{T_0} \tag{4.5}$$

Desta forma, podemos reescrever a Equação 4.1 de maneira mais consisa, mediante a substituição de cada termo $\left(\frac{2\pi nt}{T}\right)$ por $(n\omega_0 t)$:

$$f(t) = \frac{a_0}{2} + \sum_{n=1}^{+\infty} \left[a_n . \cos\left(n\omega_0 t\right) + b_n . sen\left(n\omega_0 t\right) \right]. \tag{4.6}$$

4.1.2 Representação da Série de Fourier na Forma Exponencial

A usual série de Fourier na forma retangular pode ser convertida em uma forma mais conveniente, conhecida como forma exponencial. Para isso, utiliza-se uma representação alternativa dos termos sen(x) e cos(x), por meio da equação de Euler, como apresentado a seguir [36]:

$$sen(t) = \frac{-i}{2}\left(e^{it} - e^{-it}\right) \tag{4.7}$$

e

$$cos(t) = \frac{1}{2}\left(e^{it} + e^{-it}\right). \tag{4.8}$$

Como descrito na Subseção 4.1.1 a forma retangular da série de Fourier é dada por:

$$f(t) = a_0 + \sum_{n=1}^{+\infty}\left[a_n.\cos\left(n\omega_0 t\right) + b_n.sen\left(n\omega_0 t\right)\right]. \tag{4.9}$$

Substituindo na Equação 4.9 as formas alternativas de representação do $sen(t)$ e $cos(t)$ das Equações 4.7 e 4.8, obtemos:

$$f(t) = a_0 + \sum_{n=1}^{+\infty}\left[\frac{a_n}{2}e^{in\omega_0 t} + \frac{a_n}{2}e^{-in\omega_0 t} - \frac{ib_n}{2}e^{in\omega_0 t} + \frac{ib_n}{2}e^{-in\omega_0 t}\right] \tag{4.10}$$

Organizando a Equação 4.10 em somatórios das partes positiva e negativa de n, obtemos:

$$f(t) = a_0 + \sum_{n=1}^{+\infty}\left[\frac{a_n}{2}e^{in\omega_0 t} - \frac{ib_n}{2}e^{in\omega_0 t}\right] + \sum_{n=-\infty}^{-1}\left[\frac{a_{-n}}{2}e^{in\omega_0 t} + \frac{ib_{-n}}{2}e^{in\omega_0 t}\right] \tag{4.11}$$

Colocando-se os fatores comuns em evidência:

$$f(t) = a_0 + \sum_{n=1}^{+\infty}\frac{1}{2}\left(a_n - ib_n\right)e^{in\omega_0 t} + \sum_{n=-\infty}^{-1}\frac{1}{2}\left(a_{-n} + ib_{-n}\right)e^{in\omega_0 t}. \tag{4.12}$$

Por fim, juntando-se os termos dos somatórios da Equação 4.12, obtemos:

$$f(t) = \sum_{n=-\infty}^{\infty} c_n.e^{in\omega_0 t} \tag{4.13}$$

Podemos relacionar c_n aos coeficientes a_n e b_n da forma retangular, da seguinte maneira:

$$c_n = \begin{cases} \frac{1}{2}\left(a_{-n} + ib_{-n}\right) & , n < 0; \\ a_0 & , n = 0; \\ \frac{1}{2}\left(a_n - ib_n\right) & , n > 0 \end{cases} \tag{4.14}$$

O cálculo dos coeficientes c_n podem ser obtidos diretamente, para uma função periódica de período T, da seguinte maneira:

$$c_n = \frac{1}{T} \int_{\frac{-T}{2}}^{\frac{T}{2}} f(t) e^{-in\omega_0 t} dt \tag{4.15}$$

Desta forma a série de Fourier de um sinal periódico $f(t)$ de período T, é definida como a combinação linear de exponenciais complexas harmonicamente relacionadas na forma das Equações 4.13 e 4.15, as quais são conhecidas como equação de síntese e equação de análise, respectivamente [23]. O conjunto de coeficientes c_n são frequentemente chamados de coeficientes da série de Fourier, ou coeficientes espectrais de f(t). O coeficiente c_0 é o componente constante do sinal f(t) e é dado pela Equação 4.15 com n = 0. Ou seja,

$$c_0 = \frac{1}{T} \int_{-\frac{T}{2}}^{\frac{T}{2}} f(t) dt. \tag{4.16}$$

Esses coeficientes complexos denotam a contribuição de cada parcela do conjunto de harmônicas relacionadas ao sinal f(t) [23].

É importante observar que, para sinais $f(t)$ reais, as componentes relacionadas às frequências negativas são simétricas às componentes de frequências positivas, pois:

- $\Re(c_n) = \Re(c_{-n})$;
- $\Im(c_n) = -\Im(c_{-n})$

Desta forma, para se obter a representação em série de Fourier de sinais reais (que satisfazem as condições de Dirichlet), basta-se calcular as componentes em que $n \leq 0$ ou $n \geq 0$, valendo-se da propriedade da simetria supracitada.

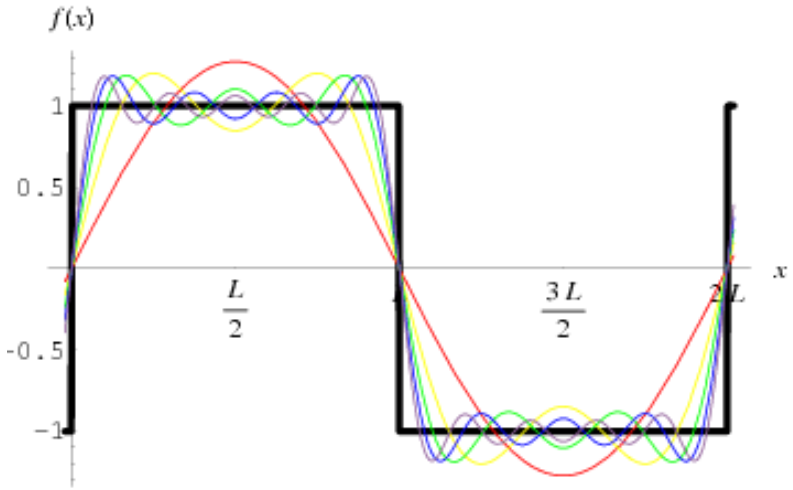

Figura 4.1: Aproximações de sinais, por séries de Fourier, de uma onda quadrada de período 2L [16].

4.2 Transformada de Fourier de Tempo Contínuo

Na Subseção 4.1.2 foi desenvolvida uma representação de sinais periódicos como combinações lineares de exponenciais complexas. Nesta Seção, apresentamos a TFTC, a qual permite converter um sinal $f(t)$ que está no dominio do tempo em seu equivalente no domínio da frequência, onde a frequência é dada em radianos por segundo (frequência angular). A TFTC é definida como [13]:"

$$F(\omega) = \int_{-\infty}^{\infty} f(t)e^{-i\omega t}dt. \tag{4.17}$$

As funções represetadas pelo termo $e^{-i\omega t}$ são conhecidas como funções "base". A TFTC é uma operação invertível, ou seja, podemos realizar uma operação que retorna um sinal $F(\omega)$ no domínio da frequência para o sinal $f(t)$ no domínio do tempo. Essa operação é dada por:

$$f(t) = \frac{1}{2\pi}\int_{-\infty}^{\infty} F(\omega)e^{i\omega t}d\omega \tag{4.18}$$

É importante salientar que um sinal $f(t)$, submetido à aplicação da TFTC, não necessita ser periódico, diferentemente dos sinais representáveis em Séries de Fourier 4.1. "Enquanto em sinais periódicos as exponenciais complexas que o representam estão relacionadas harmonicamente, para um sinal aperiódico elas estão infinitesinmalmente próximas em frequência, e a representação em termos de uma combinação linear toma a forma de uma integral, em vez de um somatório. O espectro de coeficietnes resultante nessa representaçõa é chamado de transofrma de Fourier, e a integral de síntese, que usa esses coeficientes para representar o sinal como uma conbinção linear de exponencias complexas, é donominada transformada inversa de Fourier. O desenvolvimento dessa representação para sinais aperódicos em tempo contínuo é uma das contribuições mais importantes de Fourier. Em particular, Fourier intuiu que um sinal aperiódico pode ser visto como um sinal periódico com um período infifinto. Mais precisamente, na representação da série de fourier de um sinal periódico, enquanto o período aumenta, a frequência fundamental diminui e os componentes harmonicamente relacionados tornam-se mais próximos em frequência. À medida que o período se torna infinito, os componentes de frequência se apreoximam de modo a formar um conjunto contínuo e a soma da série de Fourirer torna-se uma integral [23]."

4.3 Transformada de Fourier de Tempo Discreto

Na Seção 4.2 mostrou-se que é possível expressar um sinal contínuo $f(t)$ que está no domínio do tempo em seu equivalente $F(\omega)$ que está no domínio da frequência. Agora iremos mostrar que também é possível desenvolver uma representação análoga para sinais de tempo discreto. Para isso, primeiramente considere o sinal $f(t)$ amostrado nos istantes t = nT, resultando em uma amostra discreta $f[n]$. Essa amostragem pode ser modelada

matematicamente por meio do produto do sinal $f(t)$ pelo somatório de funções *impulso unitário* $\delta(t)$, deslocadas por intervalos de tamanho T [13]:

$$x_s(t) = \sum_{n=1}^{+\infty} x(t)\delta(t - nT) \tag{4.19}$$

Assim, nos instantes de tempo t = nT, isso se torna:

$$x_s(t) = \sum_{n=1}^{+\infty} x(nT)\delta(t - nT) \tag{4.20}$$

Desta forma, a transformada de Fourier de um sinal amostrado é dado por:

$$\begin{aligned} X(\Omega) &= \int_{-\infty}^{\infty} x_s(t)e^{-i\Omega t}dt \\ &= \int_{-\infty}^{\infty} \sum_{n=-\infty}^{+\infty} x(nT)\delta(t - nT)e^{-i\Omega t}dt \\ &= \sum_{n=-\infty}^{+\infty} \int_{-\infty}^{\infty} x(nT)\delta(t - nT)e^{-i\Omega t}dt \\ &= \sum_{n=-\infty}^{+\infty} x(nT)e^{-in\Omega T}. \end{aligned} \tag{4.21}$$

Note que a função *delta* foi usada aqui, e a propriedade que:

$$\int_{-\infty}^{\infty} \delta(t_k)f(t)dt = f(t_k). \tag{4.22}$$

Desde que t = nT (tempo) e $\omega = \Omega T$ (frequência), isto produz a transformada de fourier de um sinal amostrado como:

$$X(\omega) = \sum_{n=-\infty}^{\infty} x(n)e^{in\omega} \tag{4.23}$$

com

$$t(segundos) = n(amostras).T\frac{(segundos)}{(amostra)} \tag{4.24}$$

e

$$\omega(\frac{(radianos)}{amostra}) = \Omega\frac{radianos}{segundos}.T\frac{segundos}{amostra} \tag{4.25}$$

Desde que o espectro de frequência seja contínuo, a inversa da DTFT é assima é dada por:

$$x[n] = \frac{1}{2\pi}\int_{-\pi}^{\pi} X(\Omega)e^{jn\omega}d\omega \tag{4.26}$$

4.4 Transformada Discreta de Fourier

A DFT mapeia um sinal de tamanho N em um conjunto de N componentes discretos de frequência. Para o cálculo da DFT, é necessário obtermos uma sequência finita. Uma maneira de se fazer isso é adaptando uma sequência longa por uma janela retangular, resultando em:

$$X(k) = \sum_{n=0}^{N-1} x(x)e^{-in\omega k}, \tag{4.27}$$

em que,

$$\omega_k = \frac{2k\pi}{N}, \tag{4.28}$$

onde ω_k representa a frequência da k-ésima senóide [13].

Esta é frequentemente uma aproximação útil do espectro da sequência não modificada. A diferença é uma perda de resolução, que aumenta conforme L aumenta. É comum calcular X(ω) em um número arbitrário de (N) frequências uniformemente espaçadas ao longo de um período (2π), onde L é o omprimento da sequência modificada.

4.5 Transformada Rápida de Fourier

A Transformada rápida de Fourier (do inglês *Fast Fourier Transform* (FFT)) é um algoritmo eficiente para se calcular a DFT e a sua respectiva inversa. As Transformadas rápidas de Fourier são de grande importância em uma vasta gama de aplicações, inclusive a projetada neste trabalho.

O algoritmo é baseado no método de dobramentos sucessivos, onde podemos expressar a transformada de Fourier da seguinte forma [39]:

$$F(u) = \frac{1}{N}\sum_{x=0}^{N-1} f(x)W_N^{ux}, \tag{4.29}$$

em que,

$$W_N^{ux} = e^{\frac{-i2\pi}{N}} \tag{4.30}$$

Perceba que N pode ser escrito como N = 2M, M $\in \mathbb{Z}_+^*$. Desta forma, podemos reescrever a FFT como

$$F(u) = \frac{1}{2M}\sum_{x=0}^{2M-1} f(x)W_{2M}^{ux}. \tag{4.31}$$

O somatório acima pode ser dividido em dois, na seguinte maneira:

$$F(u) = \frac{1}{2}\left[\frac{1}{M}\sum_{x=0}^{M-1} f(2x)W_M^{u(2x)} + \frac{1}{2}\frac{1}{M}\sum_{x=0}^{M-1} f(2x+1)W_{2M}^{u(2x+1)}\right] \tag{4.32}$$

Considerando que $W_{2M}^{2ux} = W_M^{ux}$, nomeamos a primeira soma por

$$F_{par}(u) = \frac{1}{M} \sum_{x=0}^{M-1} f(2x) W_M^{ux} \ , \ u = 0, 1, 2, ..., M-1 \tag{4.33}$$

e a segunda por

$$F_{mpar}(u) = \frac{1}{M} \sum_{x=0}^{M-1} f(2x+1) W_{2M}^{ux} \ , \ u = 0, 1, 2, ..., M-1 \tag{4.34}$$

Podemos reescrever a transformada de Fourier como sendo

$$F(u) = F_{par}(u) + F_{impar}(u) W_{2M}^{u} \tag{4.35}$$

uma vez que $W_M^{u+M} = W_M^u$ e $W_{2M}^{u+M} = -W_{2M}^u$. A recombinação da equação $F_{par}(u)$ com a última, nos fornece

$$F(u+M) = F_{par}(u) - F_{mpar}(u) W_{2M}^{u} \tag{4.36}$$

A partir dessas equações, é possível perceber que uma transformada de N pontos pode ser computada pela divisão da expressão original em duas partes.

No próximo Capítulo, *Metodologia Proposta*, serão descritos de forma detalhada, todos os módulos que compõe o sistema implementado neste trabalho.

Capítulo 5

Metodologia Proposta

Neste Capítulo será apresentada a metodologia de construção do sistema de *Verificação Automática de Assinaturas On-line Utilizando Descritores de Fourier em Janelas de Tamanho Fixo*. A metodologia é baseada no trabalho desenvolvido por Yanikoglu e Kholmatov no artigo [41]. Para isso, os processos de *registro* e *verificação* do usuário serão descritos de forma detalhada nas Seções e Subseções deste Capítulo.

A Seção 5.1 apresenta o mecanismo utilizado para se extrair as características biométricas de um conjunto de assinaturas coletadas no momento do cadastramento do usuário no sistema. Essas assinaturas, chamadas de *assinaturas de referência*, são divididas em segmentos (janelas) de mesmo tamanho, que servirão como recurso para a criação do *template* do usuário, o qual, a grosso modo, sintetiza a biometria média do usuário, que será utilizada na etapa de comparação e classificação da assinatura de teste, submetida no processo de verificação.

Na Seção 5.2, é apresentado o mecanismo utilizado no processo de *verificação* de uma assinatura de teste, que é comparada ao respectivo *template* do usuário (previamente cadastrado no sistema) e classificada de acordo com um critério de decisão, baseado na distância euclidiana entre as características biométricas da assinatura de teste e referência. A Figura 5.1 ilustra o modelo geral do sistema proposto.

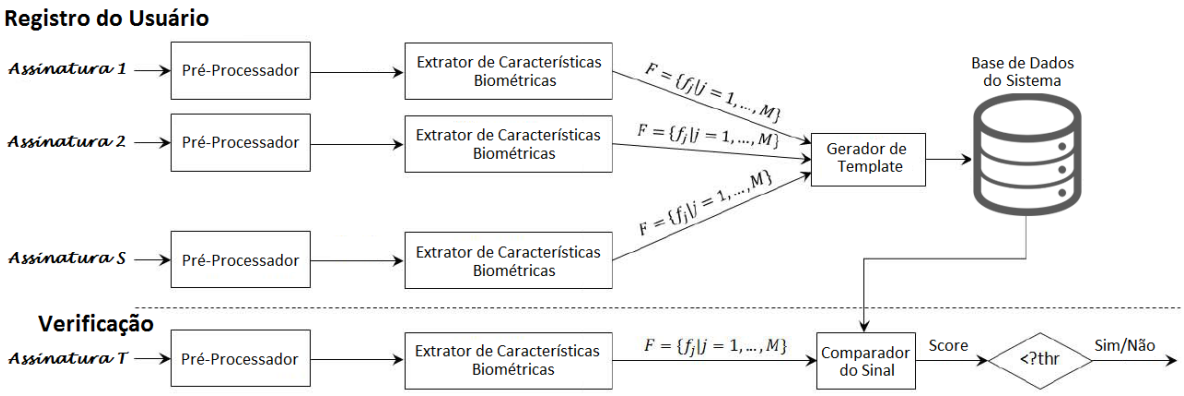

Figura 5.1: Modelo geral do sistema proposto. **F** representa o conjunto de **M** seguimentos, de mesmo tamanho, de uma dada assinatura S submetida ao sistema (adaptada de [30]).

5.1 Registro do Usuário

Como a metodologia proposta objetiva realizar autenticações de assinaturas *on-line*, primeiramente é necessário que o usuário seja cadastrado no sistema, para se associar um identificador ao seu respectivo perfil biométrico, que é chamado de *template do usuário* neste texto. O processo de *Registro de Usuário* utilizado nesta metodologia proposta, é ilustrado no diagrama de blocos da Figura 5.2. Cada bloco será detalhado nas Subseções 5.1.1 à 5.1.4.

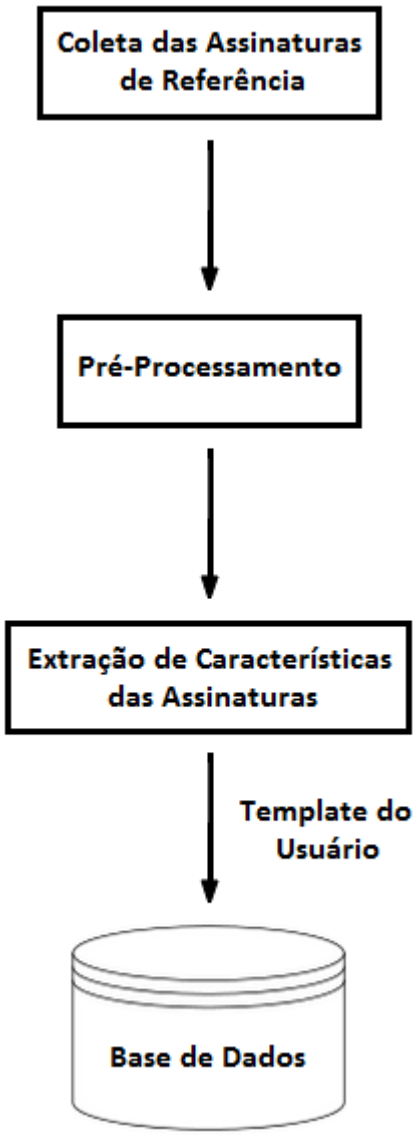

Figura 5.2: Diagrama de blocos do processo de *Registro do Usuário*.

5.1.1 Coleta das Assinaturas de Referência

A metodologia proposta necessita de um dispositivo capaz de amostrar o sinal de uma assinatura, de tal maneira, que seja possível representá-la sob a forma de um vetor tridimensional. As dimensões desse vetor, que serão chamadas indistintamente de componentes da assinatura neste texto, são utilizadas para representar valores das abscissas, ordenadas e pressões da ponta da caneta durante a coleta da assinatura.

Desta forma, uma assinatura S, coletada por um *tablet* sensível ao toque e que possui uma taxa constante de amostragem, pode ser representada como uma sequência temporal, dada por:

$$s[n] = (x[n],\ y[n],\ p[n]), \tag{5.1}$$

em que, $n = 0, 2, ..., N$, é o índice da amostra coletada durante a trajetória da assinatura, $x[n]$ e $y[n]$ representam, respectivamente, sequências de amostras das abscissas e ordenadas do traço da assinatura, e $p[n]$ representa a sequência de valores de pressão que a tela do *tablet* é submetida pela ponta da caneta. Neste Capítulo, $s\,[n]$ representará o sinal de uma assinatura no sistema proposto.

No processo de *Registro do Usuário*, cinco assinaturas de referência são coletadas para se obter seu respectivo *perfil biométrico*, que ficará armazenado na base de dados do sistema para posteriores utilizações no processo de *Verificação*.

5.1.2 Base de Dados do Sistema

Para a implementação deste trabalho, foi utilizada a biblioteca SQLite 3.8.11.1, para armazenar os dados coletados e processados pelo sistema. O SQLite é uma biblioteca em linguagem C que implementa um banco de dados SQL embutido. As tabelas utilizadas pela base de dados do sistema são ilustradas na Figura 5.3:

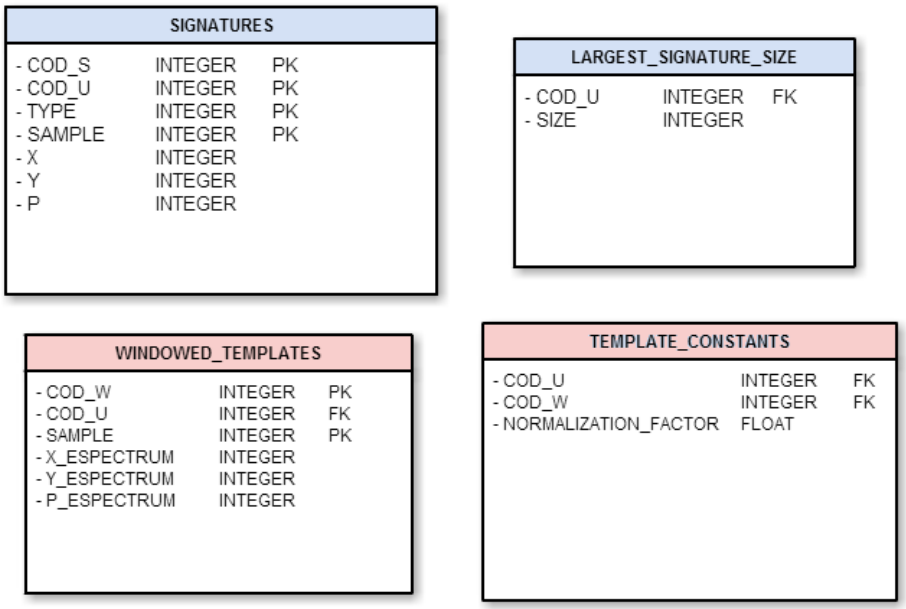

Figura 5.3: Tabelas utilizadas pelo no banco de dados do sistema.

Os campos utilizados por estas tabelas possuem os seguintes significados:

- COD_U: código do usuário;
- COD_S: código da assinatura;
- TYPE: tipo da assinatura (utilizado na etapa de testes do sistema);
- SAMPLE: índice da amostra do sinal;
- X: abscissa da amostra;
- Y: ordenada da amostra;
- P: valor de pressão da amostra;
- SIZE: tamanho da maior assinatura coletada;
- X_ESPECTRUM: coeficiente de Fourier do sinal X;
- Y_ESPECTRUM: coeficiente de Fourier do sinal X;
- P_ESPECTRUM: coeficiente de Fourier do sinal P;
- NORMALIZATION_FACTOR: valor de do coeficiente de normalização da respectiva janela.

5.1.3 Pré-Processamento

A etapa de pré-processamento é comumente considerada em projetos de sistemas de verificação de assinaturas *on-line*. Ela objetiva remover variações dos dados de entrada que são consideradas irrelevantes ou prejudiciais ao desempenho global do sistema, além de formatar o sinal de entrada em um modelo adequado para o tratamento da aplicação. Embora útil, deve-se ser cauteloso na quantidade de operações de pré-processamento os quais os dados de entrada serão submetidos, para que características biométricas importantes não sejam removidas [41].

Neste trabalho, as operações de pré-processamento consideradas incluem: remoção dos tempos de duração de suspensões da ponta da caneta, concatenação de zeros ao final dos vetores componentes da assinatura, janelamento de assinaturas, remoção da média e de ruídos do sinal de entrada de cada janela de uma assinatura. Essas operações são realizadas sobre cada assinatura de referência, e serão apresentadas e detalhadas nesta Subseção.

A Figura 5.4 ilustra as etapas de pré-processamento que as assinaturas de referência são submetidas no momento da inscrição do usuário no sistema.

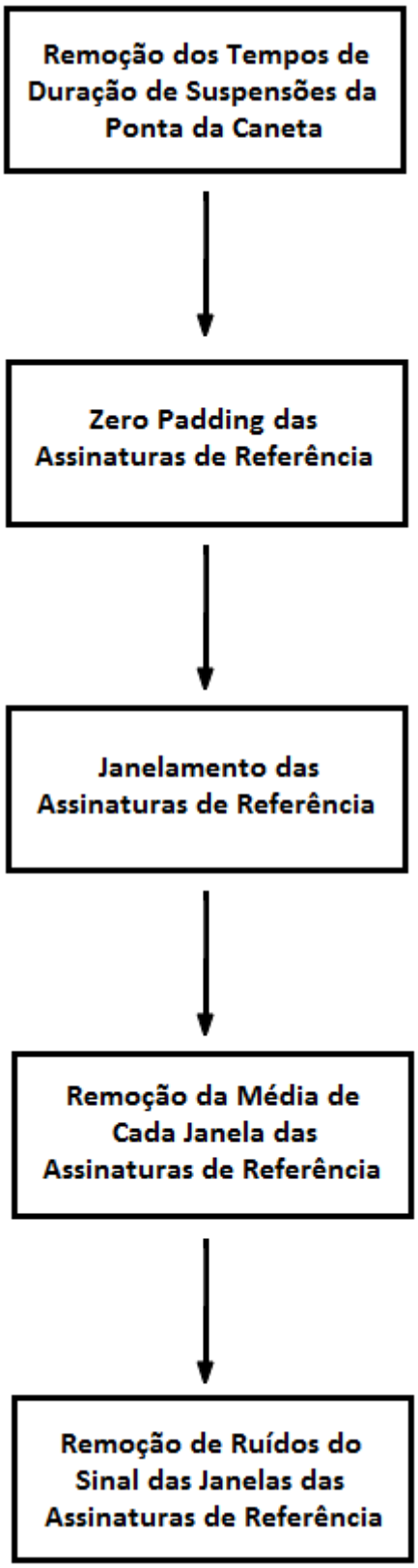

Figura 5.4: Diagrama de blocos da etapa de pré-processamento das assinaturas de referência.

Remoção dos Tempos de Duração de Suspensões da Ponta da Caneta

Sinais captados enquanto a ponta da caneta encontra-se suspensa são retirados da sequência temporal representativa da assinatura, pois, em primeiro momento, não há indícios de informação significativa nesse tipo de sinal que seja útil no processo de verificação.

Para tal fim, os intervalos de tempo em que a caneta não está em contato com o *tablet* são identificados observando-se valores nulos de pressão. Assim, subconjuntos das sequências temporais $x[n]$ e $y[n]$ associados a tais intervalos de tempo, são eliminados da representação da assinatura coletada. As sequências de amostras $r_i[n]$ denotam subconjuntos que devem ser removidos da janela w[n] $\subset S$, e são dados por:

$$r_i[n_i] = (x[n_i],\ y[n_i],\ 0), \tag{5.2}$$

em que $i = 0, 1, 2, ...$ é o índice do i-ésimo subconjunto de amostras em que a ponta da caneta não está em contato com a superfície do *tablet*, e n_i representa o enésimo sinal amostrado pertencente à r_i.

Desta forma, definimos os conjuntos $R = \{r_i[n_i]|i, n \in \mathbb{Z}_+\}$ e $W = \{(X, Y, P)\} \in S$ (janela de S), em que $X = \{x_n|x_n = x[n] \subset s[n]\}$, $Y = \{y_n|y_n = y[n] \subset s[n]\}$ e $P = \{p_n|p_n = p[n] \subset s[n]\}$, quando submetida à etapa de remoção dos tempos de suspensão da caneta, gera-se uma nova janela W_r dada por:

$$W_r = W - R \tag{5.3}$$

Zero Padding

A variação natural do comprimento das assinaturas coletadas, inviabiliza o processamento realizado na etapa descrita na Subseção **??**. Tal problema é resolvido padronizando-se o tamanho das janelas das assinaturas, para um mesmo usuário, tomando-se como referência a assinatura de maior comprimento.

Como descrito na Subseção 5.1.1, cinco assinaturas são tomadas para gerar o perfil biométrico do usuário. Neste momento, o sistema obtém os comprimentos das assinaturas coletadas, identificando o maior comprimento.

A partir deste momento, é verificado se o maior comprimento $s_{largest}$ identificado é múltiplo do comprimento w_{size} (tamanho das janelas do sistema), previamente definido para a aplicação. Se o tamanho $s_{largest}$ for múltiplo de w_{size}, armazena-se $s_{largest}$ na base de dados do sistema, mais precisamente, no campo SIZE da tabela LARGEST_SIGNATURE_SIZE. Caso contrário, concatenam-se zeros (*zero padding*) ao final dos vetores componentes das assinaturas de referência S_r, até se atingir o primeiro múltiplo de w_{size} superior a $s_{largest}$, armazenando tal múltiplo no campo SIZE da tabela LARGEST_SIGNATURE_SIZE. Por exemplo, suponha que o tamanho da janela seja 50 e o tamanho da maior assinatura coletada seja 138. Temos que 138 não é múltiplo de 50, logo, o maior valor de assinatura a ser considerado pelo sistema, neste contexto, será de 150.

Portanto, todas as assinaturas de referência devem ter seus comprimentos equalizados com relação ao comprimento $s_{largest}$, registrado na base de dados do sistema e associado a um dado usuário.

Desta forma, considerando-se as assinaturas $s_i[n]$ e $s_j[n]$ pertencentes ao conjunto de assinaturas utilizadas para gerar o perfil do usuário, com $i \neq j \in \{0, 1, 2, 3, 4\}$, k_i e k_j representando o comprimento das assinaturas $s_i[n]$ e $s_j[n]$, respectivamente, temos:

$$s_i^p[n] = \begin{cases} (x_i[n], y_i[n], p_i[n]), n = 0, 1, 2, ..., k_i - 1 \\ (0, 0, 0), n = k_i, k_i + 1, ..., k_j - 1 \end{cases} \tag{5.4}$$

se $k_i < k_j$, ou

$$s_i[n]' = s_i[n], \tag{5.5}$$

se $k_i = k_j$, em que, k_j é o comprimento da maior assinatura coletada. Logo, $s_i^p[n]$ é o resultado obtido do processo de *zero padding* sob a assinatura $s_i[n]$.

Janelamento do Sinal

Toda assinatura submetida ao sistema, passa por um processo de segmentação do seu sinal $s[n]$. Os segmentos, chamados de *janelas* neste trabalho, devem possuir tamanhos idênticos, pois, este requisito é necessário para processa-los na etapa de classificação da assinatura.

Após a etapa de *zero padding*, as assinaturas de referência são divididas em janelas de mesmo comprimento. Nenhuma janela de uma dada assinatura deve compartilhar dados em comum com outra janela qualquer, ou seja, não há sobreposição de valores entre janelas, pois, cada janela é uma amostra única do sinal coletado da assinatura.

Além disso, cada janela obtida nesta etapa, é submetida a outras fases de pré-processamento, sendo tratadas de maneira independente pelo sistema.

A Figura 5.5 ilustra o processo de janelamento de um sinal das componentes XY do sinal amostrado $s[n]$:

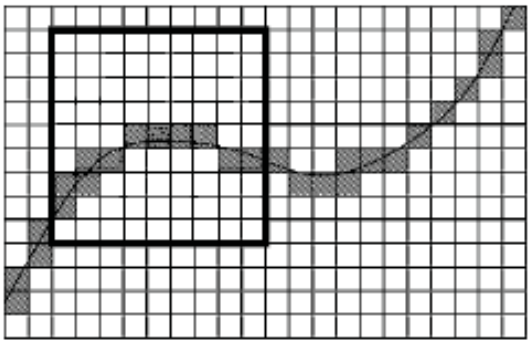

Figura 5.5: Ilustração do processo de janelamento das componentes X e Y de uma assinatura $s[n]$ (adaptada de [7]).

É importante ressaltar, que todo o sinal da assinatura coletada é aproveitado, ou seja, na etapa de janelamento, nenhum subconjunto da assinatura $s[n]$ é desprezado.

Remoção da Média de cada Janela das Assinaturas

Com efeito de normalização de dados, a remoção da média das janelas de uma assinatura, é realizada por meio da diferença entre os vetores componentes de cada janela e suas respectivas médias. O vetor média $m_c[n]$ de um componente $c[n] \in \{x[n], y[n], p[n]\}$ de uma janela $w[n]$, é dado por:

$$m_c[n] = \overline{c}, \tag{5.6}$$

em que,

$$\overline{c} = \frac{\sum_{n=0}^{k-1} c[n]}{k}, \tag{5.7}$$

sendo k o tamanho do vetor c[n]. Desta forma, a janela w_{r_i} resultante da remoção de sua respectiva janela média i de uma assinatura S, é dada por:

$$w_{r_i}[n] = w_i[n] - (m_x[n], m_y[n], m_p[n]), \tag{5.8}$$

em que, $w_i \subset S$ e i é o índice da i-ésima janela da assinatura S.

Remoção de Ruídos do Sinal das Janelas da Assinatura

Visando diminuir a influência de ruídos sob o sinal das janelas de uma assinatura, provenientes dos dispositivos de coleta (*tablet*/caneta), foi utilizado o método dos mínimos quadrados para estimar as flutuações sobre a linha base desse sinal. Dado o sinal de um componente $c[n] \in \{x[n], y[n], p[n]\}$ e de tamanho k, a versão $c_r[n]$ desse sinal com a remoção de flutuações, é dado por [41]:

$$c_r[n] = c[n] - \beta.(t - \bar{t}), \tag{5.9}$$

em que, $t[n]$ representa o tempo na enésima amostra, e

$$\beta = \frac{\sum_{n=0}^{k}(c[n].t[n] - k.\bar{c}[n].\bar{t}[n])}{\sum_{n=0}^{k}(t[n]^2 - k.\bar{t}[n]^2)}. \tag{5.10}$$

5.1.4 Extração de Características das Assinaturas

Nesta Subseção, serão detalhadas as etapas para se extrair as características biométricas de cada assinatura de referência, que serão chamadas, também, de *Descritores de Fourier*. Essas etapas são seguidas logo após a etapa de pré-processamento, descrita na Subseção 5.1.3.

A Figura 5.6 ilustra o diagrama de blocos do processo de extração de características das assinaturas.

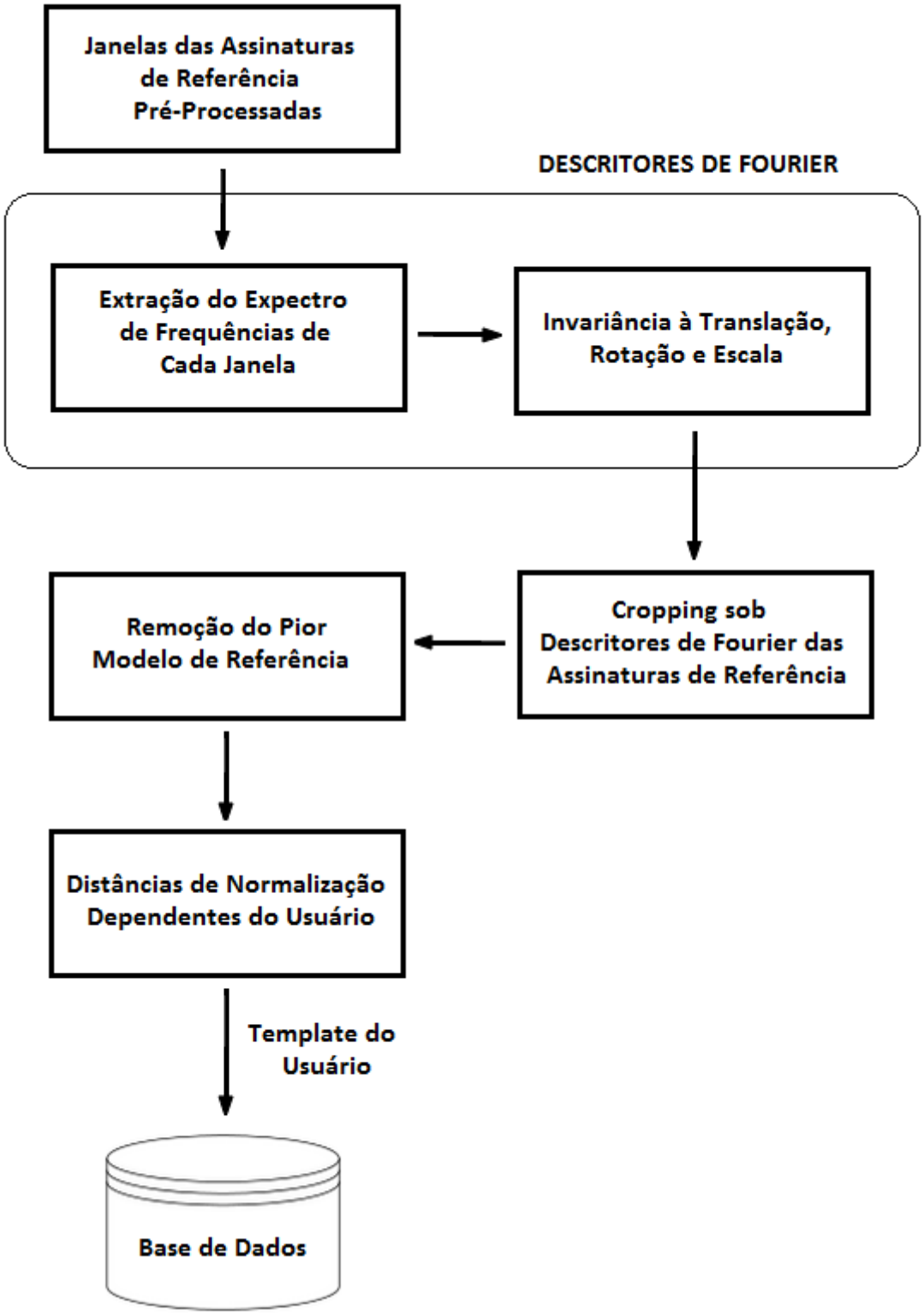

Figura 5.6: Diagrama de blocos da etapa de extração de características das assinaturas de referência.

Descritores de Fourier

Nesta etapa, foi utilizada a FFT para se obter o espectro de frequências de cada janela dos componentes das assinaturas coletadas. Os espectros extraídos são normalizados, obtendo-se o que chamaremos de *Descritores de Fourier*. O processo de normalização objetiva alcançar invariância à translação, rotação e escala da trajetória das janelas da assinatura.

A invariância à translação é obtida com a remoção do termo a_0 dos coeficientes de Fourier. Desta forma, o vetor de espectros $A_c[k]$ de um componente c $\in$ {x, y, p} proveniente de uma janela $w[n]$, é dado por:

$$A_c[k] = [a_1, a_2, ..., a_k - 1] \tag{5.11}$$

em que k é o tamanho da janela $w[n]$ e $a_1, a_2, ..., a_k - 1$ representam os $k-1$ primeiros coeficientes de Fourier.

Já a invariância à rotação é alcançada automaticamente considerando-se somente a magnitude do espectro do sinal de uma dada componente de assinatura.

Finalmente, a invariância à escala do traçado da janela da assinatura é obtida a partir da divisão de cada termo, de um vetor componente particular, por uma constante, que é calculada da seguinte forma:

$$m = \sum_{i=0}^{k-1} |a_i| = \sqrt{a_i.\overline{a_i}}, \tag{5.12}$$

em que k é o tamanho da janela da assinatura; $|a_i|$ é a magnitude dos coeficientes complexos a_i e $\overline{a_i}$ é o complexo conjugado de a_i.

Utilizando o coeficiente m calculado na equação 5.12, compilamos o vetor final de características da respectiva janela janela da assinatura a partir dos Descritores de Fourier (DF) F_k da seguinte forma:

$$F_i = \frac{a_i}{m}, \tag{5.13}$$

em que $i = 1, 2, ..., \frac{k}{2}$, k sendo o tamanho da janela da assinatura. Note que i varia até $\frac{k}{2}$, pois, descartamos metade dos coeficientes de Fourier por conta da simetria do espectro obtido com a FFT.

Cropping sob Descritores de Fourier das Assinaturas de Referência

Após a etapa anterior, parte do DF de cada componente de uma dada janela é desprezado. Isso se faz necessário, para excluir frequências mais altas do sinal de uma janela, pois, tais frequências podem ser provenientes de ruídos adicionados a esse sinal, no momento de coleta da assinatura.

Desta forma, realizam-se cortes (*cropping*), de mesmo tamanho, sobre o DF correspondente a cada compontente da janela tratada. Neste trabalho, o comprimento final considerado para cada DF de uma dada janela, é de tamanho 25.

Essa padronização de comprimento dos *Descritores de Fourier*, facilita a implementação de algoritmos de comparação, pois, não há a necessidade de adaptar tal processo a diferentes tamanhos desses descritores.

Remoção do Pior Modelo de Referência

Por conta da variação natural das assinaturas de referência de um usuário, a assinatura de referência que possui o descritor de Fourier com maior desvio em relação aos descritores das outras referências restantes, é eliminada do conjunto de assinaturas de referência. Para isso, o sistema calcula todas as combinações possíveis da norma Euclidiana entre vetores espectrais das assinaturas de referência. Aquela que obtiver a maior média de distâncias dentre essas assinaturas é descartada.

Distâncias de Normalização Dependentes do Usuário

No processo de verificação, é utilizada a norma euclidiana para se calcular as distâncias correspondentes entre os DF das janelas da assinatura de teste e do *template* do usuário. Tais distâncias, após obtidas, devem ser normalizadas por um fator D_w, associado a tal janela, que é dado por:

$$D_w = \overline{d(r_i, R/r_i)}, \tag{5.14}$$

em que, R/r_i é o conjunto R de assinaturas de referência sem o elemento $r_i, \forall r_i \in R$. Portanto, $d(r_i, R/r_i)$ representa a média das distâncias entre uma dada janela de referência $r_i \in R$ e cada uma das janelas $R - \{r_i\}$, com $i \in \{0, 1, 2, 3, 4\}$.

Armazenamento do Template do Usuário

O *template* do usuário é gerado pela média dos DF das janelas pertencentes às assinaturas remanescentes do processo de remoção do pior modelo de referência. Essa média é calculada simplesmente adicionando-se os DF de cada janela correspondente, das assinaturas de referência, e dividindo tal soma, pelo total de assinaturas de referência, que neste caso é 4, já que a pior assinatura de referência foi removida.

Após essa etapa, o *template* do usuário, que pode ser entendido como um conjunto de janelas cujos vetores são a média dos DF das assinaturas de referência, é armazenado na base de dados da aplicação, mais precisamente, na tabela WINDOWED_TEMPLATES.

5.2 Verificação

No processo de verificação, a assinatura de teste a ser verificada é submetida às mesmas etapas de pré-processamento e extração de características biométricas, realizadas individualmente sobre as assinaturas de referência.

Quando uma assinatura é submetida ao sistema para ser verificada, a dissimilaridade entre seus descritores de Fourier e os das assinaturas de referência do usuário é calculada. Essa dissimilaridade é obtida a partir da norma euclidiana entre tais descritores (janela a janela), que são normalizados utilizando-se estatísticas do conjunto de assinaturas de referência do usuário. A assinatura a ser verificada é autenticada caso essa distância normalizada seja inferior a um limiar previamente definido, caso contrário, a assinatura não é autenticada. Os detalhes desse processo, serão descritos nesta Seção.

A Figura 5.7 ilustra o diagrama de blocos do processo de verificação de uma dada assinatura de teste.

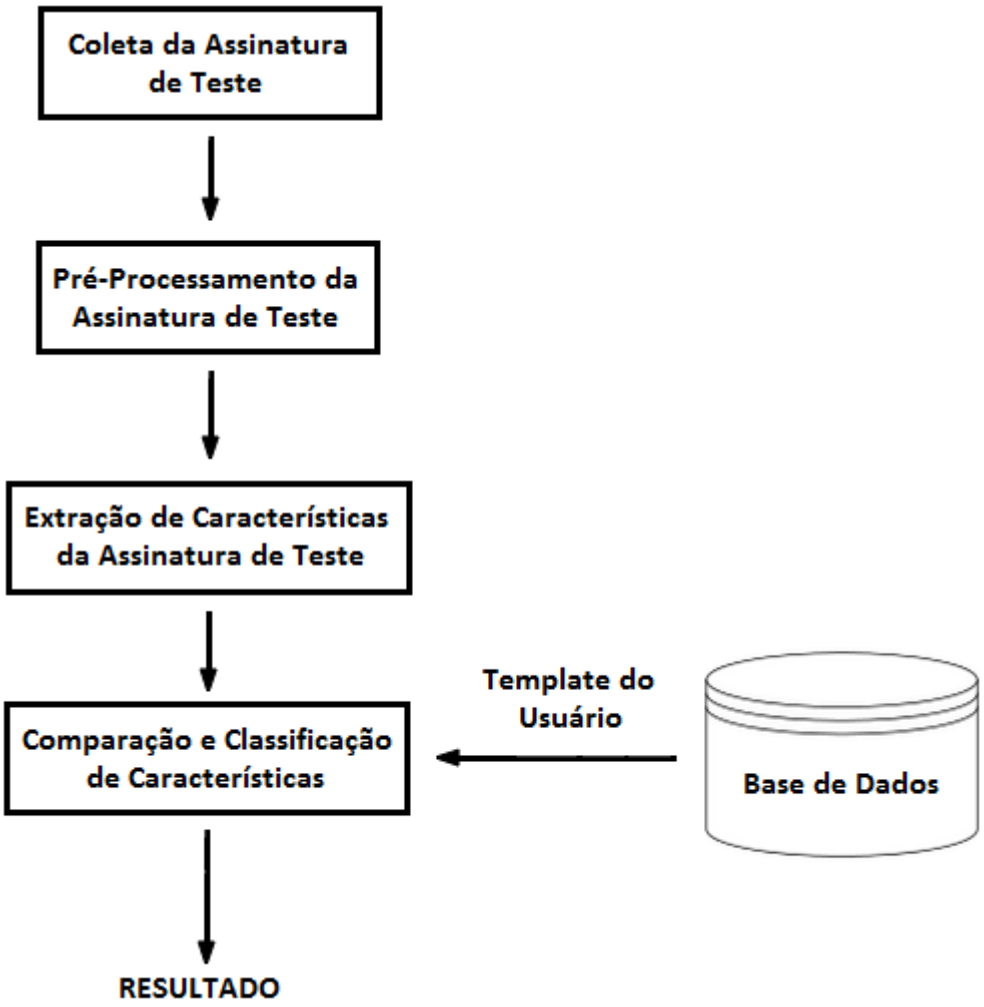

Figura 5.7: Diagrama de blocos do processo de verificação do sistema, para uma dada assinatura de teste.

5.2.1 Coleta da Assinatura de Teste

A assinatura de teste é coletada de maneira análoga à descrita na Subseção 5.1.1.

5.2.2 Pré-Processamento da Assinatura de Teste

Assim como a coleta de dados, a etapa de pré-processamento da assinatura de teste é análoga à descrita na Subseção 5.1.3, com exceção da possibilidade de se realizar um corte ao invés de uma concatenação de zeros ao final da assinatura de teste, tomando-se como base, o maior tamanho de assinatura armazenado na base de dados do sistema, o qual está associado ao número identificador do usuário.

Zero Padding ou Cropping da Assinatura de Teste

O *zero padding* soluciona casos em que o comprimento das assinaturas são inferiores ao comprimento da maior assinatura, considerando-se um dado usuário já cadastrado.

No entanto, casos em que o comprimento da assinatura é superior ao da maior assinatura, é necessário a realização de um *crop* (corte) sob essa assinatura, para se atingir o tamanho padrão definido para o usuário. Desta forma, considerando-se as assinaturas $s_i[n]$ e $s_j[n]$ pertencentes ao conjunto de assinaturas utilizadas para gerar o perfil do usuário, com i, j $\in \{0, 1, 2, 3, 4\}$, k_i e k_j representando o comprimento das assinaturas $s_i[n]$ e $s_j[n]$, respectivamente, temos:

$$s_i^c[n] = (x_i[n], y_i[n], p_i[n]), n = 0, 1, 2, ..., k_j - 1 \tag{5.15}$$

em que, $k_i > k_j$ e k_j é o comprimento da maior assinatura coletada. Logo, $s_i^c[n]$ é o resultado obtido da realização do processo de *cropping* sob a assinatura $s_i[n]$.

5.2.3 Comparação e Classificação de Características

O perfil do usuário, que também podemos chamar de *assinatura final de referência*, é utilizado no cálculo de dissimilaridade entre ele e a assinatura de teste a ser verificada.

A dissimilaridade $d(W_T, R_i)$ é obtida por meio da distância euclidiana entre o conjunto de vetores finais de características W_T das janelas de cada assinatura de teste, e os respectivos e correspondentes vetores $\overline{W_R}$, em que, R denota o conjunto de assinaturas de referência, ou seja, $\overline{W_R}$ representa a média dos vetores de características das assinaturas de referência. Desta forma, temos que:

$$d(W_T, R) = \|W_T - \overline{W_R}\| \tag{5.16}$$

Após essa etapa, tais distâncias são normalizadas pelos fatores D_i 5.14, entre cada janela da assinatura a ser verificada e as janelas correspondentes do respectivo *template* do usuário. Após a realização desses cálculos, adquire-se a média simples das distâncias normalizadas, que será comparada a um valor limiar definido para o sistema. Caso a média seja inferior ao valor limiar, o sistema classifica o sinal de entrada como *autêntico*, caso contrário, como *falsificado*.

No próximo Capítulo, *Testes e Resultados*, serão apresentados os resultados dos testes e simulações do sistema.

Capítulo 6

Testes e Resultados

Neste Capítulo serão descritos como foram realizados os testes que objetivam avaliar o desempenho global do sistema, assim como a apresentação e discussão dos seus respectivos resultados.

Para a realização de testes e medidas de performance, foi utilizada a base de dados de medidas biométricas desenvolvido no projeto MCYT, uma das mais conhecidas entre os pesquisadores de soluções biométricas. Essa base foi desenvolvida com o intuito de auxiliar projetos de sistemas de reconhecimento automático, para avaliação do desempenho de aplicações civis, comerciais ou forenses.

Os testes serão realizados sob diversos cenários distintos de configuração do sistema. Os cenários de teste foram determinados sobre diferentes tipos de etapas de pré-processamento em conjunto com diferentes componentes do sinal de entrada. A Seção 6.2 descreve os protocolos utilizados nos momentos de registro e autenticação de um usuário.

6.1 Aquisição dos Dados

Neste trabalho, foi utizada uma base de dados bimodal de medidas biométricas, desenvolvida a partir da iniciativa do laboratório de pesquisa biométrica da *Universidad Politecnica de Madrid* (UPM), resultando no projeto MCYT. A base de dados MCYT visa auxiliar projetos de sistemas de reconhecimento automático na avaliação do desempenho de aplicações civis, comerciais ou forenses.

6.1.1 Base de Dados MCYT

A base de dados MCYT está organizada em duas partes: *MCYT_Fingerprint subcorpus* e *MCYT_Signature subcorpus*. Os dados foram coletados de 330 pessoas em um consórcio com quatro instituições acadêmicas: UPM, *University of Valladolid* (UVA), *University of the Basque Country* (EHU) e Escola Universitária Politécnica de Mataro (EUPMt) [25].

Em relação ao *MCYT_Signature subcorpus*, foram registradas 16500 amostras de assinaturas, obtidas a partir da coleta de 25 assinaturas genuínas e 25 assinaturas forjadas por falsificadores profissionais, para cada um dos 330 indivíduos que contribuíram para a realização do projeto. As amostras coletadas possuem dados de natureza dinâmica como a

trajetória da assinatura, pressão da caneta, azimute e altitude da caneta, além da imagem da assinatura coletada, que é uma informação de natureza estática [25].

Para a aquisição das assinaturas *online* foi utilizado o *tablet* Wacom Intuos A6 sensível à caneta (Figura 6.1), com a seguinte especificação [25]:

- resolução de 100 linhas/mm;
- precisão de +/- 0,25 mm;
- área de captura de 127 x 97 mm^2;
- altura máxima entre a ponta da caneta e a superfície do *tablet* para detecção do sinal de entrada: 10 mm;
- frequência de captura de 100 Hz;
- posições no eixo x_t: $x[t] \in [0, 12700]$, correspondendo à variação de 0 a 127 mm;
- posições no eixo y_t: $y[t] \in [0, 9700]$, correspondendo à variação de 0 a 97 mm;
- pressão p_t: $p[t] \in [0, 1023]$;
- ângulo do azimute φ_t em relação ao plano da tela do *tablet*: $\varphi[t] \in [0, 3600]$, correspondendo à variação de 0° a 360° (Figura 6.2);
- ângulo da altitude θ_t em relação ao plano da tela do *tablet*: $\theta[t] \in [300, 900]$, correspondendo à variação de 30° a 90° (Figura 6.2);

Figura 6.1: Wacom Intuos A6 [33].

Uma assinatura *online* coletada pelo *tablet* pode ser representada como uma sequência temporal dada por [41] :

$$S[n] = (x[n],\ y[n],\ p[n],\ \varphi[n],\ \theta[n]), \tag{6.1}$$

em que, n = 1, 2, ..., N, é o índice da amostra coletada durante a trajetória da assinatura.

Na implementação deste trabalho, foram utilizadas somente as três primeiras componentes de S[n] (Equação 6.1) para se descrever as assinaturas submetidas pelos usuários

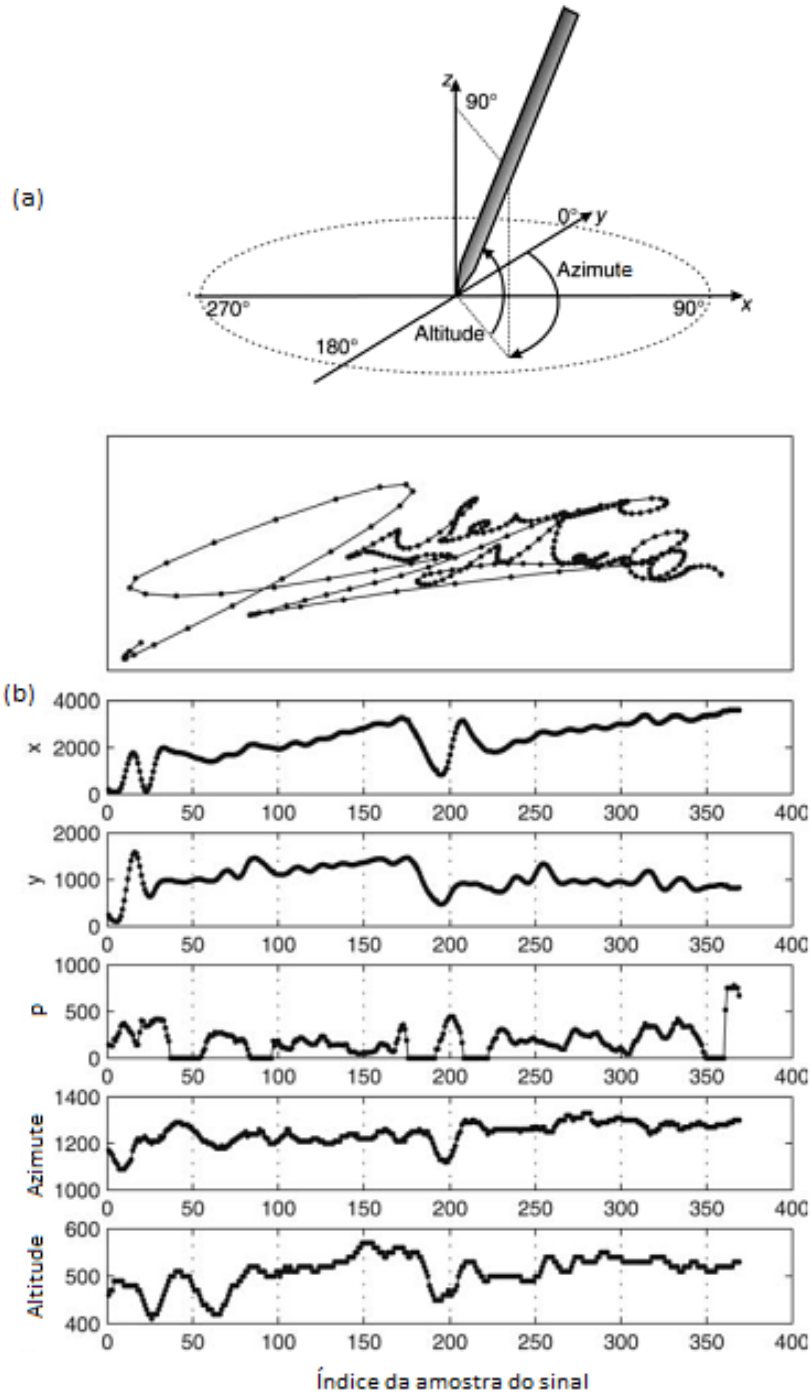

Figura 6.2: **(a)** Representação da posição, azimute altitude da caneta em relação ao plano de escrita do dispositivo de coleta de dados. **(b)** Exemplo de sinais coletados da assinatura (adaptada de [14]).

do sistema, ou seja, foram desprezadas as medidas de azimute $\varphi[t]$ e altitude $\theta[t]$ da caneta. Desta forma, a definição de assinatura que deverá ser assumida neste texto é dada a seguir:

$$s[n] = (x[n],\ y[n],\ p[n]), \tag{6.2}$$

em que n, x[n], y[n] e p[n] mantém os mesmos significados descritos na equação 6.1. Além disso, apesar da contribuição de 330 indivíduos para o projeto MCYT, somente 100 desses permitiram que seus dados biométricos fossem de domínio público. Desta forma, foram utilizados os dados biométricos somente desses 100 usuários.

As assinaturas da base de dados MCYT estão armazenadas em arquivos com formato "fpg". Por questão de conveniência, foi criado o *script* "ExtractXYZParameters.m", executado no Matlab R2014a, para extrair e converter os dados do formato "fpg"para o formato "csv", desprezando os dados sobre medidas do azimute e altitude da caneta. Desta forma, foram criados 5000 arquivos no formato "csv", compostos por biometrias de 25 assinaturas genuínas e 25 falsificadas, para cada um dos 100 usuários. Esses arquivos criados compõe o universo de amostras possíveis a serem tratadas pelo sistema em questão.

Os nomes dos arquivos foram definidos de maneira que os dados biométricos fiquem associados ao devido usuário. Para isso, cada nome de arquivo é composto por três partes:

1. um número que serve como identificador único do usuário;
2. uma letra para descrever a classificação do tipo de assinatura, que pode ser genuína (v) ou forjada (f);
3. um número para identificar a amostra da assinatura coletada.

Por exemplo, os dados de um arquivo com o nome "0018v03.csv"indicam que a amostra 3 de uma assinatura genuína está associada ao usuário 18, enquanto um arquivo com o nome "0098f24.csv"indica que a amostra 24 de uma assinatura falsificada está associada ao usuário 98.

As assinaturas também foram persistidas na base de dados "*SystemDatabase.db*", criada utilizado-se a biblioteca SQLite SQLite 3.8.11.1. Apesar de permitir maior flexibilidade para a implementação do sistema proposto, a utilização das assinaturas contidas na base de dados SystemDatabase.db diminuiu a performance do sistema, o qual utiliza como fonte de entrada somente as assinaturas armazenadas nos arquivos .csv. Desta forma, as assinaturas armazenadas em SystemDatabase.db foram utililizadas somente para fins de análise por meio da ferramenta *SQLite Browser*, já que a mesma oferece uma interface mais amigável para consultas sob as assinaturas do que a leitura de arquivo por aquivo .csv.

6.2 Protocolos de Simulação

Esta Seção descreve os protocolos utilizados nos momentos de registro e autenticação de um usuário.

6.2.1 Simulação do Cadastramento de Usuários

A simulação do cadastramento de um usuário, se dá pela coleta de suas 5 primeiras assinaturas, ou seja, para cada usuário **U**, são coletadas as assinaturas **Uv00**, **Uv01**, **Uv02**, **Uv03** e **Uv04**, do conjunto V de assinaturas genuínas com elementos UvS, em que $U = \{0, 1, 2, ..., 99\}$ e $S = \{0, 1, 2, ..., 24\}$. Essas assinaturas serão submetidas às etapas descritas no Capítulo 5, referentes ao cadastramento de usuários. O *template* gerado pelo sistema para cada usuário registrado, é armazenado na base de dados *SystemDatabase.db*, além do tamanho de assinatura a ser considerado como padrão para cada verificação e os fatores de normalização dependentes do usuário.

6.2.2 Simulação de Verificações de Usuários

O conjunto de assinaturas utilizadas na simulação do processo de verificação de um dado usuário **U** é definido por:

$$V \cup F, \tag{6.3}$$

em que,

$$V = \{Uv05, Uv06, ..., Uv24\} \tag{6.4}$$

e

$$F = \{Uf00, Uf01, ..., Uf24\}. \tag{6.5}$$

Cada assinatura $s \in V \cup F$ será comparada ao template do usuário armazenado na base de dados do sistema. A cardinalidade do conjunto $V \cup F$ é 4500.

6.3 Experimentos Realizados

Para avaliar a performance do sistema, foi criado o método *performances(cod_cfg, firstSignerId, lastSignerId)*, no arquivo *main.cpp*. Os parâmetros *firstSignerId* e *lastSignerId* servem para selecionar o intervalo fechado de usuários a serem utilizados no procedimento de teste. O parâmetro *cod_cfg* é passado para definir o conjunto de parâmetros de configuração que o sistema deve considerar na execução do teste. Além disso, foi criada a base de dados *ResultsDatabase.db* que registra diversos resultados no processo de verificação que serão apresentados nas Tabelas 6.3, à 6.6.

A performance do sistema é baseada no valor da taxa de EER, obtida por meio da média entre as taxas falso negativo e falso positivo mais próximas entre si. A análise da proximidade de tais taxas foi possível por meio da variação dos limiares do sistema (de 0,01 em 0,01), para uma dada configuração de teste, obtendo-se as FRR e FAR em cada experimento.

O sistema foi submetido a testes sob diferentes combinações de parâmetros de configuração, os quais estão registrados na tabela *CONFIGURATIONS* da base de dados *ResultsDatabase.db*. Todas as possíveis configurações registradas em *CONFIGURATIONS* (Tabela 6.2) foram testadas utilizando-se o conjunto $V \cup F$, ou seja, para cada configuração, foram testadas 4500 assinaturas, dentre genuínas e falsificadas.

A Tabela 6.1 servirá como referência para a consulta dos significados dos campos das tabelas utilizadas neste Capítulo.

Tabela 6.1: Significados dos campos das tabelas contidas no Capítulo 6.

CAMPO	**DESCRIÇÃO**
AVG_ERR	Contém o erro médio para uma dada configuração de teste
CFG	Contém os códigos das configurações de teste
CMP	Componentes da assinatura ($XY \longleftrightarrow 2$ e $XYP \longleftrightarrow 3$)
EER	*Equal Error Rate*
FN	Falso Negativo
FP	Falso Positivo
SIZE_SPC	Largura do espectro de frequências
SIZE_W	Tamanho da janela assinatura
TEST_SIG	Quantidade de assinturas testadas
THR	*Threshold* (limiar)

Tabela 6.2: Parâmetros de configuração utilizados em testes do sistema.

CFG	**SIZE_W**	**SIZE_SPC**	**CMP**	**TEST_SIG**
0	50	25	2	4500
1	50	25	3	4500
2	75	25	2	4500
3	75	25	3	4500
4	100	25	2	4500
5	100	25	3	4500
6	125	25	2	4500
7	125	25	3	4500
8	150	25	2	4500
9	150	25	3	4500

Tabela 6.3: Melhores configurações para o sistema, utilizando somente os componentes XY e diferentes tamanhos de janela. Lista organizada em ordem crescente da EER

SIZE_W	SIZE_SPC	CMP	THR	FN (%)	FP (%)	EER (%)
150	25	2	1,61	19,95	19,48	19,69
100	25	2	1,71	19,80	19,64	19,71
075	25	2	1,69	20,35	20,16	20,24
125	25	2	1,72	20,10	20,60	20,38
050	25	2	1,65	24,55	24,88	24,73

Tabela 6.4: Melhores configurações para o sistema, utilizando somente os componentes XYP e diferentes tamanhos de janela. Lista organizada em ordem crescente da EER

SIZE_W	SIZE_SPC	CMP	THR	FN (%)	FP (%)	EER (%)
150	25	3	1,23	17,20	17,08	17,13
100	25	3	1,31	18,35	18,88	18,64
075	25	3	1,30	18,85	19,20	19,04
125	25	3	1,30	19,20	19,72	19,49
050	25	3	0,00	00,00	00,00	00,00

A partir da observação das Tabelas 6.3 e 6.4, as melhores performances obtidas em sistemas que utilizaram somente os componentes XY e aqueles que utilizaram XYP foram de 19,69 % e 17,13 %, respectivamente. Isso mostra que os dados relativos à pressão, permitiram uma pequena melhoria da performance global do sistema. A Figura 6.3 ilustra o comportamento das FRR e FAR, para o sistema configurado com os parâmetros do teste de melhor desempenho utilizando somente as componentes XY da assinatura.

É importante observar, que ambas as configurações de testes, no que se refere ao número de componentes da assinatura utilizados nos experimentos (somente XY ou XYP), obtiveram a mesma sequência de tamanhos de janelas relacionados à melhor performance. Isso sugere uma correlação entre a metodologia utilizada e um tamanho ótimo de janela.

Além disso, é possível perceber, também, que janelas de tamanho relativamente pequeno tendem a deteriorar a performance do sistema, já que, pelas tabelas 6.3 e 6.4, a diminuição do tamanho da janela acarreta em uma diminuição do desempenho do sistema, de maneira geral.

Já as tabelas 6.5 e 6.6, apresentam os dez melhores resultados, no que se refere à taxa média de erro AVG_ERR, usando somente XY ou XYP, respectivamente, com a variação de 0,1 entre limiares. Esses resultados, permitem analisar a performance do sistema sob uma perspectiva alternativa à adotada utilizando-se a EER.

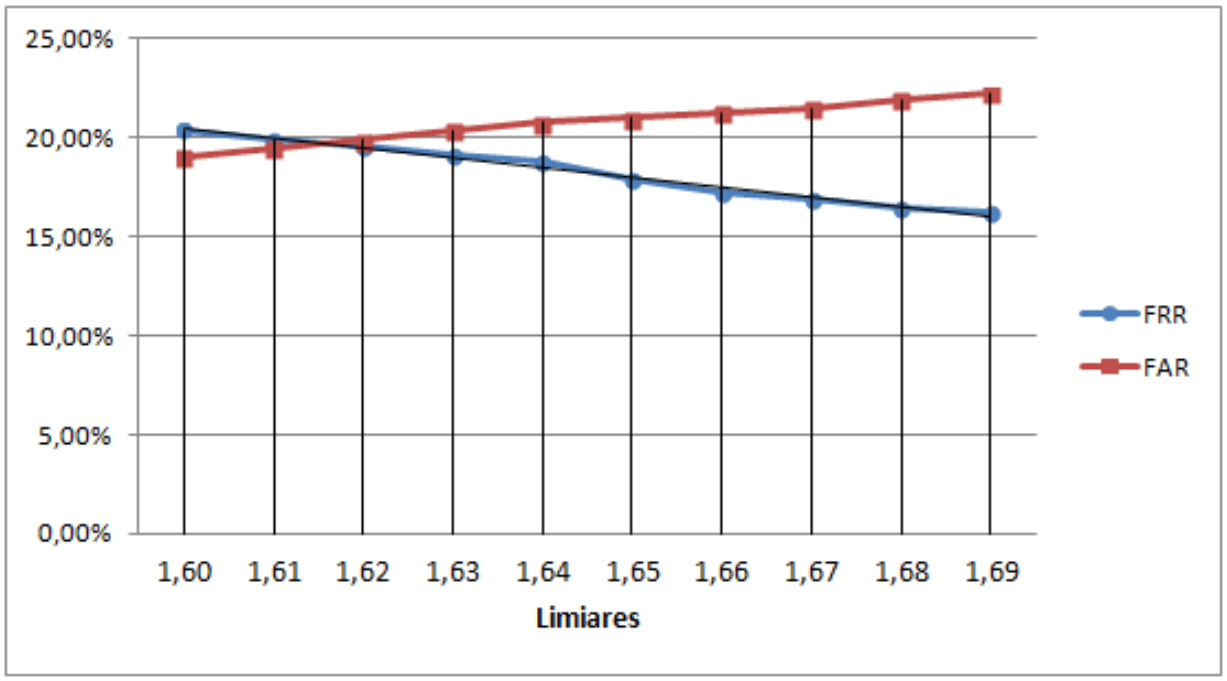

Figura 6.3: Gráfico FRR x FAR obtido a partir de um teste com a seguinte configuração: SIZE_W = 150 e CMP = 2.

Tabela 6.5: Lista das dez melhores configurações para o sistema utilizando somente os componentes XY da assinatura, em ordem crescente do *AVG_ERR*.

SIZE_W	**SIZE_SPC**	**CMP**	**THR**	**FN (%)**	**FP (%)**	**AVG_ERR (%)**
100	25	2	1,5	29,00	10,48	18,71
100	25	2	1,6	23,85	14,96	18,91
150	25	2	1,6	20,40	19,04	19,64
075	25	2	1,6	24,45	16,04	19,78
075	25	2	1,5	30,00	12,12	20,07
125	25	2	1,6	25,45	15,88	20,13
150	25	2	1,5	26,50	15,80	20,56
125	25	2	1,5	30,30	12,88	20,62
100	25	2	1,4	36,60	8,00	20,71
075	25	2	1,4	36,75	8,44	21,02

Tabela 6.6: Lista das dez melhores configurações para o sistema utilizando os componentes XYP da assinatura, em ordem crescente do *AVG_ERR*.

SIZE_W	**SIZE_SPC**	**CMP**	**THR**	**FN (%)**	**FP (%)**	**AVG_ERR (%)**
150	25	3	1,3	13,55	20,80	17,58
100	25	3	1,3	18,85	18,28	18,53
075	25	3	1,3	18,85	19,20	19,04
150	25	3	1,4	10,15	26,84	19,42
125	25	3	1,3	19,20	19,72	19,49
100	25	3	1,4	15,35	24,92	20,67
075	25	3	1,4	14,00	26,20	20,78
125	25	3	1,4	15,20	25,68	21,02
150	25	3	1,5	8,10	33,16	22,02
100	25	3	1,5	12,75	30,56	22,64

A performance geral dessa aplicação não superou a obtida daquela proposta por Yanikoglu e Kholmatov em [41], o qual obteve as EER = 15,58 %, FRR = 15,25 % e FAR = 15,84 %, utilizando somente a forma da assinatura, ou seja, XY, e as EER = 15,71 %, FRR = 15,65 % e FAR = 15,76 %, utilizando XYP, quando submetida ao mesmo cenário de testes definidos na Seção 6.2.

Apesar disso, é importante salientar que o sistema obteve resultados relativamente próximos ao do sistema em que foi baseado. Todavia, a técnica abordada necessita ser aprimorada para se obter uma melhor performance global.

No Capítulo seguinte, *Conclusão*, conclui-se este trabalho apresentando uma síntese geral de todo o texto e resultados obtidos.

Capítulo 7

Conclusão

Apesar da verificação de assinaturas não ser um dos métodos biométricos mais seguros, ainda é o mais utilizado na autenticação de pessoas em contextos formais. Desta forma, o futuro de tecnologias de verificação automática de assinaturas se mostra promissor. A assinatura é um tipo de característica biométrica comportamental a qual varia relativamente por conta da falta de precisão humana em reproduzi-la. Essa essa variância impõe uma certa dificuldade na implementação de sistemas biométricos baseados em reconhecimento de indivíduos. Quando utilizam computadores, esses sistemas digitalizam e processam os sinais de uma assinatura coletada, buscando extrair características que sirvam para verificar ou identificar um indivíduo em particular. Inúmeras técnicas podem e são utilizadas por sistemas digitais que realizam a tarefa reconhecimento de indivíduos, baseando-se em algoritmos de natureza estatística e/ou relacionados à inteligência artificial. Uma das técnicas mais utilizadas por sistemas biométricos, está a extração do espectro de frequências de um sinal, por intermédio da transformada rápida de Fourier, para se obter algum padrão que identifique a unicidade de uma pessoa.

Neste trabalho, foi proposta uma metodologia de reconhecimento automático de assinaturas *on-line*, a qual realiza a comparação entre características biométricas de janelas correspondentes da assinatura de teste e do *template* do usuário, sendo que, a extração das características biométricas de cada janela baseia-se no trablho de Yanikoglu e Kholmatov, proposto em [41].

Na etapa de inscrição de um usuário no sistema, um conjunto de assinaturas é coletado para serem processadas e formarem o *template* ou perfil do usuário, que será utilizado na etapa de verificação de um sinal de entrada. No sistema, as assinaturas e suas respectivas características são armazenadas em forma de vetores. Para a confecção do perfil biométrico da assinatura do usuário, primeiramente calcula-se o comprimento da maior assinatura do conjunto de amostras de referência. Esse comprimento servirá para padronizar o tamanho de todas as assinaturas submetidas pelo usuário (inclusive as outras amostras de referência), sendo realizado o *zero padding* (concatenação de zeros ao final do sinal) em assinaturas de tamanho inferior, e o *cropping* (corte) de assinaturas de tamanho superior à assinatura de maior comprimento.

Após essa etapa de padronização de comprimentos, cada assinatura é dividida em seguimentos de mesmo tamanho, que chamados de *janelas* da assinatura. O tamanho do segmento, ou seja, da janela, é definido globalmente para todo o sistema e é utilizado na segmentação de todo sinal de entrada. Após o janelamento das assinaturas, cada janela

passará por etapas de pré-processamento e extração do espectro de frequências do seu respectivo sinal, obtido pela FFT. Em seguida, exclui-se o sinal que possui maior desvio com relação ao conjunto de assinaturas de referência.

Quando uma assinatura de teste é submetida à verificação, são repetidos os passos supracitados de pré-processamento e extração de características biométricas sob a assinatura. Em seguida, na etapa de classificação do sinal, calcula-se a norma euclidiana normalizada entre cada janela da assinatura a ser verificada e as janelas do respectivo *template* do usuário. Após a realização desses cálculos, para se classificar uma assinatura como *autêntica* ou *falsificada*, o sistema obtém a média das distâncias dos descritores de Fourier entre as respectivas janelas do sinal de entrada e do *template* do usuário. Após obtida, essa média é comparada a um limiar previamente definido para o sistema. O sinal da assinatura é considerado autêntico se a média obtida for inferior ao limiar estipulado, caso contrário, o sinal é classificado como falsificado.

Para se verificar a performance deste sistema, foi utilzada a base de dados MCYT, desenvolvido em um projeto iniciado pela UPM. As performances foram medidas por meio do cálculo da EER para cada configuração que o sistema foi submetido no processo de testes, utilizando um conjunto fixo de 4500 assinaturas, divididas em 2000 genuínas e 2500 forjadas. As performances foram avaliadas em dois cenários diferentes, onde são considerados números distintos de componentes no processo de verificação das assinaturas. Os resultados obtidos nesta metodologia se aproximam relativamente dos resultados obtidos no trabalho proposto em [41], utilizando-se somente as cinco primeiras assinaturas de cada usuário para a criação do seu respectivo perfil biométrico. Porém, a performance global do sistema foi inferior ao do trabalho proposto em [41], o qual obteve EER = 15,51 % em sistemas que utilizaram somente os componentes XY, e EER = 15,73 % para sistemas que utilizaram os componentes XYP.

O sistema obteve sua melhor performance no cenário em que utilizou os componentes XYP das assinaturas, obtendo uma EER = 17,13 %, configurado com os seguintes parâmetros: janelas de tamanho iguais a 150, limiar de 1,23 e largura do espectro de frequências igual a 25. Quando utilizado somente os componentes XY, houve uma pequena redução na performance do sistema, atingindo a EER = 19,69 %, utilizando a seguinte configuração: janelas de comprimento iguais a 150, limiar de 1,61 e largura do espectro de frequências igual a 25.

Apesar da performance sistema proposto ser inferior ao desenvolvido em [41], os resultados foram considerados como satisfatórios, uma vez que, obteve um desempenho semelhante ao trabalho em que foi baseado. Além disso, a técnica utilizada apresenta uma nova abordagem para a análise das características locais de um sinal biométrico.

Portanto, com o objetivo de se melhorar os resultados dessa abordagem, a qual utiliza a FFT como método principal para extração de características biométricas do sinal de uma janela, devem ser estudadas e combinadas outras técnicas de verificação de assinaturas, como também, testar outras métricas para a comparação das amostras e analisar as possíveis diferenças de performance em conjuntos de assinaturas classificadas pelo tamanho.

Referências

[1] Fine Art America. Bertillon card, June 2015. vii, 7

[2] Fórum Biometria. Verificação (1:1) versus identificação (1:n), June 2015. 10

[3] biometrics.derawi.com. Decision error tradeoff (det). Disponível em: http://biometrics.derawi.com/wp-content/uploads/2011/01/det_roc.png. Acessado em: 31 de julho de 2015. vii, 16

[4] Wei-Lun Chao. Face recognition. 2010. 3, 13

[5] F. Galton. *Personal identification and description.* Nature, 28 de junho de 1888. 7

[6] Peter Gregory and Michael A. Simon. *Biometric For Dummies.* For Dummies, 2008. vii, 2, 6, 11, 12, 13

[7] Frederike Dorothea Griess. Project report: On-line signature verification. In *Project Report: On-line Signature Verification*, Michigan, MI, US, 2000. Michigan State University - Departament of Computer Science and Engeneering. vii, 1, 2, 10, 35

[8] H.Faulds. *On the skin furrows of the hand.* Nature, 28 de outubro de 1880. 7

[9] Dicionário Informal. Biometria. Disponível em: http://www.dicionarioinformal.com.br/biometria/. Acessado em: 16 de junho de 2015. 6

[10] National Law Enforcement Museum Insider. Bertillon system of criminal identification, June 2015. 6, 7

[11] A. Jain, L. Hong, and S Pankanti. *Biometric Identification.* Communications of the ACM, 2000. 8, 12, 13

[12] Anil K. Jain, Patric Flynn, and Arun A. Ross. *Hand Book of Biometrics.* Springer US, 1 edition, 2008. vii, 2, 8, 9, 11, 12, 13, 14, 15

[13] John W. Leis. *Digital Signal Processing Using MATLAB for Students and Researchers.* John Wiley & Sons, Inc., 2011. 21, 25, 26, 27

[14] Stan Z. Li. *Encyclopedia of Biometrics.* Springer Publishing Company, Incorporated, 1st edition, 2009. viii, 14, 15, 44

[15] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar. *Handbook of Fingerprint Recognition.* Springer-Verlag, 2003. 11

[16] mathworld.wolfram.com. Fourier series. Disponível em: http://mathworld.wolfram.com/FourierSeries.html. Acessado em: 31 de julho de 2015. vii, 24

[17] Stephen Mayhew. History of biometrics, June 2015. 7

[18] Dicionário Michaelis. Biometria. Disponível em: http://michaelis.uol.com.br/moderno/portugues/index.php?lingua=portugues-portugues&palavra=biometria. Acessado em: 16 de junho de 2015. 6

[19] J.M.F. Moura. What is signal processing? [president's message]. *Signal Processing Magazine, IEEE*, 26(6):6–6, Nov 2009. 19

[20] V.S. Nalwa. Automatic on-line signature verification. *Proceedings of the IEEE*, 85(2):215–239, Feb 1997. 13

[21] New York State Division of Criminal Justice Services. The bertillon system. Disponível em: http://www.criminaljustice.ny.gov/ojis/history/bert_sys.htm. Acessado em: 17 de junho de 2015. 7

[22] NSTC Subcommittee on Biometrics. Glossary, June 2015. 10

[23] Alan V. Oppenheim, Alan S. Willsky, and S. Hamid Nawab. *Signals &Amp; Systems (2Nd Ed.)*. Prentice-Hall, Inc., Upper Saddle River, NJ, USA, 1996. 18, 19, 21, 24, 25

[24] Sophocles J. Orfanidis. *Introduction to Signal Processing*. Prentice-Hall, Inc., Upper Saddle River, NJ, USA, 1995. 18, 20

[25] J. Ortega-Garcia, J. Fierrez-Aguilar, D. Simon, J. Gonzalez, M. Faundez-Zanuy, V. Espinosa, A. Satue, I. Hernaez, J.-J. Igarza, C. Vivaracho, D. Escudero, and Q.-I. Moro. Mcyt baseline corpus: a bimodal biometric database. *Vision, Image and Signal Processing, IEE Proceedings* -, 150(6):395–401, Dec 2003. 42, 43

[26] Paolo Prandoni and Martin Vertteli. *Signal Processing for Communications*. EPFL Press, 6000 Broken Sound Parkway,NW, Suite 300 Boca Raton, FL, USA, 2008. 19, 21

[27] Zhong-Hua Quan, De-Shuang Huang, Xiao lei Xia, M.R. Lyu, and Tat-Ming Lok. Spectrum analysis based onwindows with variable widths for online signature verification. In *Pattern Recognition, 2006. ICPR 2006. 18th International Conference on*, volume 2, pages 1122–1125, 2006. 4

[28] Nalini K. Ratha, Andrew W. Senior, and Ruud M. Bolle. Automated biometrics. In *Proceedings of the Second International Conference on Advances in Pattern Recognition*, ICAPR '01, pages 445–474, London, UK, UK, 2001. Springer-Verlag. 12

[29] Kenneth Revett. *Behavioral Biometrics: A Remote Access Approach*. Wiley Publishing, 1st edition, 2008. 13, 14

[30] Napa Sae-Bae and N. Memon. Online signature verification on mobile devices. *Information Forensics and Security, IEEE Transactions on*, 9(6):933–947, June 2014. vii, 4, 29

[31] Cesar Roberto Santos. *Análise de Assinaturas Manuscritas Baseada nos Princípios da Grafoscopia*. Pontifícia Universidade Católica do Paraná, 2004. vii, 2

[32] Dag Stranneby and William Walker. *Digital Signal Processing and Applications (Second Edition)*. Newnes, Oxford, 2004. 20

[33] techradar. Wacom intuos a6, Acessado em: 24 de junho de 2015. vii, 43

[34] James L. Wayman. Fundamentals of biometric authentication technologies. *National Biometric Test Center*, pages 1–19, 1999. 6

[35] J.L. Wayman, A. Jain, D. Maltoni, and D. Maio. *Biometric Systems*. Springer London, 2005. 6, 7, 8, 10

[36] Wikibook. Signal and systems. Disponível em: https://en.wikibooks.org/wiki/Signals_and_Systems. Acessado em: 22 de julho de 2015. 17, 21, 23

[37] Wikipédia. Processamento de sinais. Disponível em: https://pt.wikipedia.org/wiki/Processamento_de_sinal. Acessado em: 22 de julho de 2015. 19

[38] Wikipédia. Série de fourier. Disponível em: https://pt.wikipedia.org/wiki/S%C3%A9rie_de_Fourier. Acessado em: 27 de julho de 2015. 21, 22

[39] wikipedia. Transformada rápida de fourier. Disponível em: https://pt.wikipedia.org/wiki/Transformada_r%C3%A1pida_de_Fourier. Acessado em: 15 de julho de 2015. 27

[40] Wikipedia. Biometrics, June 2015. 10

[41] Berrin Yanikoglu and Alisher Kholmatov. Online signature verification using fourier descriptors. *EURASIP J. Adv. Signal Process*, 2009:12:1–12:1, January 2009. 3, 4, 5, 13, 29, 32, 36, 43, 50, 51, 52

[42] D. Zhang, Wai-Kin Kong, J. You, and M. Wong. Online palmprint identification. *Pattern Analysis and Machine Intelligence, IEEE Transactions on*, 25(9):1041–1050, Sept 2003. 12

[43] David D. Zhang. *Automated Biometrics*. Springer US, 2000. vii, 6, 11, 12, 13, 14, 15