Capítulo 6

Proteção de Sistemas Biométricos

Marco Antonio Torrez Rojas (IFC), Charles Christian Miers (UDESC), Marcos Antonio Simplício Jr (POLI-USP), Luis Henrique de Almeida Fernandes (POLI-USP), Rafael Yamada de Oliveira (POLI-USP), Gabriela Guilherme de Andrade (IFC), Isaak Gomes de Araújo (IFC), Sara de Almeida Sehnem (IFC), Vinicius Dacio da Silva (IFC)

Abstract

The protection of biometric information is a growing concern due to the pivotal role of biometrics in today's identification and authentication mechanisms. This chapter contextualizes the subject, covering key concepts, models, procedures and technologies related to the construction of reliable biometric systems (and, hence, required for ensuring the security of systems that rely on biometric data). We address the fundamentals of biometrics, including the characteristics used for personal identification and the techniques for capturing and analyzing biometric data. Furthermore, we discuss the importance of protecting biometric information along its lifecycle, considering privacy, security, revocability, and potential vulnerability concerns. This review establishes a solid foundation for understanding the challenges and requirements in this constantly evolving field.

Resumo

A proteção de informações biométricas é uma preocupação crescente, em especial devido ao papel central da biometria nos mecanismos atuais de identificação e autenticação. Este capítulo contextualiza o assunto, abordando os principais conceitos, modelos, procedimentos e tecnologias relacionados à construção de sistemas biométricos robustos (e, portanto, necessárias para garantir a segurança dos sistemas que dependem de dados biométricos). O documento aborda conceitos fundamentais sobre biometria, incluindo as características utilizadas para identificação pessoal e as técnicas de captura e análise de dados biométricos. Além disso, discute-se a importância de proteger informações biométricas ao longo de todo o seu ciclo de vida, considerando questões de privacidade, segurança, revogabilidade e possíveis vulnerabilidades. Esta revisão estabelece uma base sólida para a compreensão dos desafios e requisitos neste campo em constante evolução.

6.1. Introdução

A biometria desempenha um papel fundamental em várias áreas da nossa sociedade moderna, desde o acesso a sistemas de controle de segurança até a autenticação em aplicações *online*. Sistemas biométricos se fundamentam na utilização de características físicas ou comportamentais aproximadamente exclusivas de um indivíduo para identificá-lo ou autenticá-lo. No primeiro caso, da identificação, as características biométricas do indivíduo são comparadas com todos os registros em um banco de dados em busca de uma correspondência próxima o suficiente, permitindo ao sistema dizer a qual usuário a leitura biométrica pertence (e, por exemplo, autorizá-lo a acessar um local protegido). Já no segundo caso, da autenticação, é comum que o usuário primeiro se identifique, por exemplo escolhendo seu nome de usuário em uma lista, ou apresentando um identificador em um teclado numérico; em seguida, a leitura biométrica capturada é comparada apenas com o indivíduo associado ao identificador apresentado, de modo que a autenticação tem sucesso apenas em caso de elevada correspondência. Em ambos os tipos de aplicação, a biometria surge como uma abordagem promissora para solucionar a crescente necessidade de soluções com maior usabilidade para os processos de identificação e autenticação, sem degradar sua segurança e confiabilidade. A biometria engloba uma ampla gama de aplicações práticas. Por exemplo, no controle de acesso físico, sistemas biométricos substituem ou complementam métodos tradicionais, como chaves ou cartões de identificação, oferecendo uma autenticação bastante segura e confiável [Li and Jain, 2015]. Ao dispensar uma boa memória ou o cuidado com dispositivos físicos nesses cenários, a boa usabilidade trazida por sistemas biométricos pode trazer ganhos de produtividade ao simplificar e agilizar processos administrativos, economizando tempo e recursos [Jain et al., 1996]. Já em dispositivos como *smartphones* e caixas eletrônicos, a autenticação biométrica, como reconhecimento facial ou leitura de impressões digitais, proporciona uma forma rápida e conveniente de desbloqueio e acesso, em particular para usuários que têm dificuldade em lembrar de senhas complexas. Além disso, a autenticação biométrica é comumente aplicada como fator adicional em transações financeiras, fornecendo maior segurança e reduzindo riscos de fraudes [Matos, 2000].

Este documento tem por objetivo contextualizar o uso de biometria em sistemas modernos, abordando os principais tipos conceitos, modelos, procedimentos e tecnologias relacionados à construção de sistemas biométricos robustos. Para isso, a Seção 6.2 apresenta uma breve revisão dos principais conceitos sobre biometria, os principais tipos e características, e exemplos típicos de aplicação em diversos setores. Também uma introdução a norma ISO/IEC 24745:2022 que aborda aspectos relacionados à proteção de dados biométricos. Na Seção 6.3 é introduzido o conceito de sistemas biométricos e os seus principais subsistemas, e respectivas funcionalidades no processamento dos dados biométricos. Também é apresentado o ciclo de vida de tratamento dos dados biométricos, bem como exemplos de aplicação dos sistemas biométricos. Na Seção 6.4 são apresentado os requisitos de segurança recomendados nos sistemas biométricos, em especial os requisitos de renovação e revogação de *templates* biométricos. Também são apresentadas e analisadas as principais ameaças relacionadas ao ciclo de vida de tratamento dos dados biométricos. Finalmente, são apresentados os mecanismos que possibilitam prover proteção dos dados biométricos. Na Seção 6.5 é apresentado a classificação dos sistemas biométricos com base no local em que os dados de referência e identidade biométricos

dos indivíduos são armazenados e comparados. Também são apresentados os modelos de aplicação dos dados biométricos e os modelos de segurança relacionados. Na Seção 6.6 são apresentadas as considerações finais sobre os principais pontos abordados no minicurso. Também são discutidos demandas e oportunidades futuras de pesquisa com relação a segurança e privacidade de dados biométricos.

6.2. Características Biométricas

A base da identificação de usuários em sistemas biométricos são as chamadas *características biométricas*. Essencialmente, elas são formadas por atributos singulares e distintos de cada indivíduo, podendo então ser usadas como padrão para validação de cada usuário do sistema. Essas características podem ser divididas em duas categorias principais: físicas, ou seja, mensuráveis diretamente dos usuários e pouco variáveis (e.g., impressão digital e íris); e comportamentais, baseadas na análise de padrões apresentados pelos usuários (e.g., modo de caminhar, ou forma de assinar manualmente um documento) [Li and Jain, 2015]. Cabe destacar que diferentes características biométricas possuem benefícios e limitações distintas. Por exemplo, características físicas como a impressão digital e a íris apresentam alta exclusividade; porém, elas podem ser mais difíceis de capturar em alguns contextos (e.g., em ambientes nos quais é obrigatório o uso de equipamentos de segurança para proteger mãos e olhos), ou mais fáceis de burlar em outros (e.g., captura de digitais de alvo a partir de superfícies por ele tocadas). Por outro lado, características comportamentais como a assinatura manual e a voz podem ser menos exclusivas, mas mais fáceis de serem coletadas e aceitas pelos usuários.

Essa avaliação comparativa é essencial para a seleção da biometria mais adequada a cada aplicação específica, garantindo segurança, usabilidade e eficiência nos sistemas biométricos utilizados em diferentes áreas, como segurança de dispositivos, controle de acesso e autenticação de transações. É importante observar que, além das características biométricas físicas (anatômicas) e comportamentais (baseadas em ações ou padrões de comportamento), existem algumas características biométricas adicionais que podem ser utilizadas para identificação ou autenticação, embora sejam menos comuns. Algumas destas incluem: características químicas (envolvem a análise de características químicas únicas no corpo humano, como o uso de análise de composição química da pele, saliva ou suor); características do cérebro (reconhecimento biométrico baseado em padrões cerebrais, incluindo a análise de padrões de atividade cerebral ou conectividade funcional); entre outras. A Figura 6.1 ilustra uma classificação de algumas das principais tecnologias e características biométricas utilizadas atualmente.

6.2.1. Características Físicas

As características físicas são aquelas que podem ser medidas diretamente do corpo humano, constituindo atributos aproximadamente únicos e mensuráveis associados a cada indivíduo. Alguns exemplos de características físicas utilizadas na biometria são:

- **Impressões Digitais:** As impressões digitais são padrões distintivos formados por cristas e vales que constituem a superfície dos dedos. Através da análise dessas características, é possível criar modelos únicos para cada indivíduo, permitindo sua identificação precisa [Maltoni et al., 2009]. O processo envolve a aquisição de imagens de alta reso-

Figura 6.1: Classificação das principais tecnologias biométricas [Oliveira Filho, 2014].

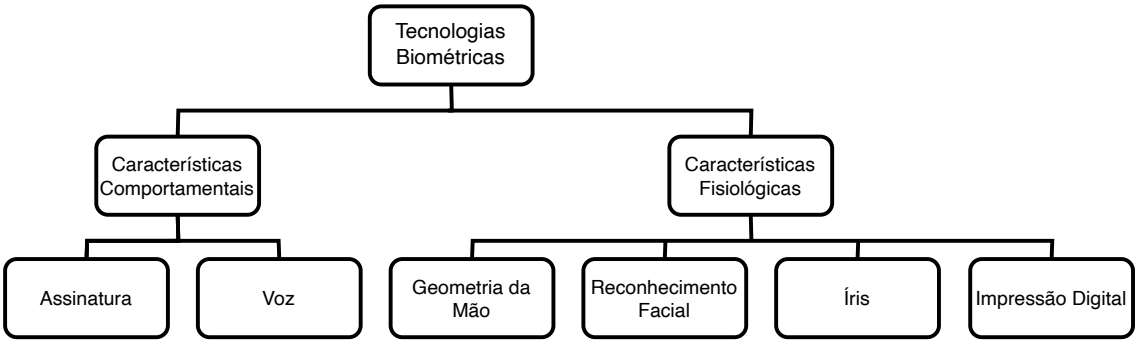
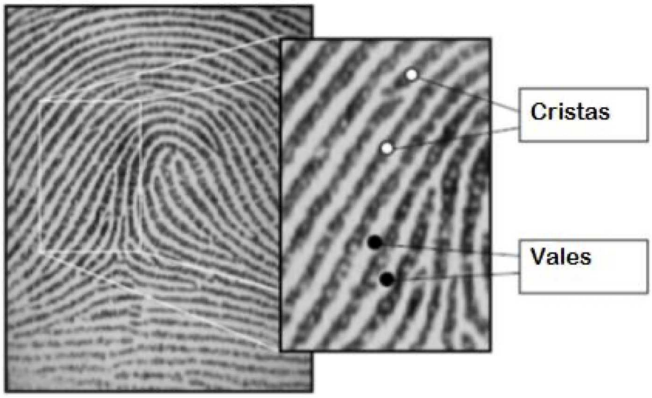


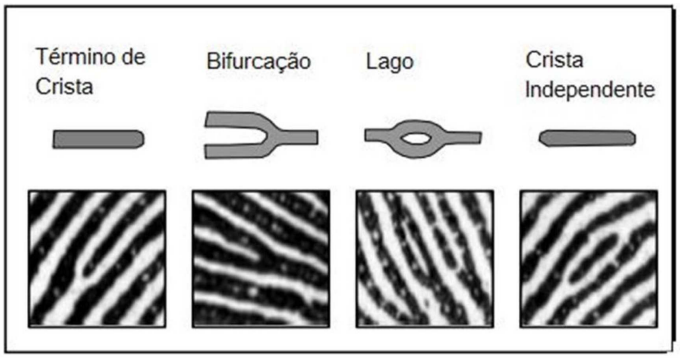
Figura 6.2: Cristas e vales em uma impressão digital [Faria, 2014].



lução das impressões digitais, seguido de pré-processamento para melhorar a qualidade e realçar as características essenciais (Direção das Cristas e Padrões de Arranjo). A extração de características das impressões digitais envolve a identificação de pontos de interesse, como bifurcações e terminações, que são utilizados para criar um modelo ou *template* da impressão. Esses modelos são então armazenados e comparados com outras impressões digitais para efetuar a autenticação ou identificação de usuários [Maltoni et al., 2009]. A Figura 6.2 ilustra os padrões de cristas e vales que se encontram na identificação de impressões digitais. A Figura 6.3 ilustra os detalhes identificados em impressões digitais que são empregados nas capturas para a análise comparativa de impressões digitais.

- **Reconhecimento Facial:** O reconhecimento facial envolve a análise das características faciais de uma pessoa, como a forma do rosto, posição dos olhos, nariz e boca. Com base nas características extraídas, um *template* ou representação matemática do rosto é criado, capturando suas informações essenciais. Essa característica é comumente utilizada em sistemas de segurança e controle de acesso. A verificação da biometria é feita então a partir da semelhança desse *template* e da imagem do rosto capturada diretamente do indivíduo interagindo com o sistema, levando à liberação ou negação de acesso [Ratha et al., 2001a].
- **Geometria da Mão:** A geometria da mão analisa a estrutura e as proporções da mão de um indivíduo, incluindo o tamanho dos dedos, formato da palma e posição das

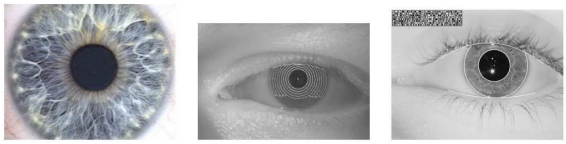
Figura 6.3: Tipos de minúcias encontradas em uma impressão digital [Faria, 2014].



articulações.

- **Reconhecimento de Íris e Retina:** O reconhecimento de íris e retina analisa as características únicas presentes nos olhos de um indivíduo. A íris é a parte colorida do olho, enquanto a retina é a camada interna sensível à luz. Essas características são altamente distintivas de cada indivíduo. A Figura 6.4 ilustra a imagem da íris adquirida sob condições ideais (esquerda). É mostrada a fase de aplicação do algoritmo de extração de características (centro), e a íris com seu código de íris associado (direita).

Figura 6.4: Processo de captura e processamento do reconhecimento íris/retina. Fonte: [Costa et al., 2006].



6.2.2. Características Comportamentais

As características comportamentais referem-se aos padrões de comportamento de um indivíduo. Essas características são mais difíceis de serem copiadas ou forjadas, pois estão relacionadas à forma como uma pessoa age ou se comporta. Alguns exemplos de características comportamentais utilizadas na biometria são [Li and Jain, 2015]:

- **Voz:** A análise da voz envolve a identificação de características distintivas, como a frequência, o tom e o padrão de fala. Existem também sistemas baseados em desafio-resposta, em que o usuário deve ler uma frase específica escolhida dinamicamente como parte do processo de verificação biométrica.
- **Assinatura:** A análise da assinatura envolve a identificação dos traços únicos presentes na maneira como uma pessoa assina seu nome. Essa característica é amplamente utilizada em autenticação em documentos e transações.
- **Forma de Digitação:** A forma de digitação analisa os padrões de pressão aplicada às teclas, velocidade entre teclas distintas, e duração do pressionamento durante a

digitação [Araújo et al., 2005]. Essa característica pode ser utilizada em sistemas de autenticação em computadores e dispositivos móveis.

- **Termograma:** A biometria termográfica, também conhecida como termograma ou termografia, é uma técnica não invasiva e sem contato para medir e registrar a temperatura do corpo humano ou de outros objetos. Essa tecnologia é baseada na captura e análise da radiação infravermelha emitida por corpos e objetos que emitem calor. A termografia é amplamente utilizada em diversas aplicações, incluindo medicina, indústria, segurança física e vigilância, e até mesmo na conservação do meio ambiente, encontrando também alguma aplicação em sistemas biométricos [Cross and Smith, 1995].

Existem diferentes critérios que podem ser considerados relevantes para a adoção de um tipo específico de característica biométrica em sistemas de segurança. Critérios comumente encontrados na literatura são [Jain et al., 1996]: universalidade, que indica o quão comum é a presença dessa característica na população alvo do sistema (e.g., assinaturas manuais podem ser poucos difundidas entre usuários analfabetos); exclusividade, ou a capacidade de ser única para cada indivíduo; permanência, que mede a estabilidade da característica biométrica ao longo do tempo, considerando fatores ambientais adversos (e.g., o uso de produtos de limpeza abrasivos pode apagar impressões digitais) ou naturais (e.g., envelhecimento); coletabilidade, que se refere à facilidade e conveniência na coleta dos dados biométricos (e.g., a necessidade de treinamento específico para uso do coletor biométrico afeta negativamente esta métrica); desempenho, em termos de precisão e confiabilidade na identificação; aceitabilidade, que tem relação com grau de aceitação e conforto dos usuários quanto à sua utilização (e.g., tecnologias que usam leitores próximos aos olhos costumam ser mais invasivas do que as baseadas em câmeras comuns, distantes do indivíduo); e facilidade de circunvenção, considerando tentativas de falsificar informações biométricas ou burlar o sistema sem a conivência do usuário.

Embora não haja um consenso na literatura, a evolução em termos de tecnológica de *hardware* e *software* pode afetar de forma distinta a aquisição de cada característica biométrica, a Tabela 6.1 apresenta um comparativo entre tecnologias contemporâneas [Balakrishnan et al., 2021] e tecnologias clássicas [Jain et al., 1996] das principais características biométricas aqui discutidas, com base nesses critérios. Cumpre notar, entretanto, que cada aplicação específica costuma necessitar de uma análise mais detalhada do que essa avaliação comparativa ampla, considerando as particularidades do cenário alvo. Por exemplo, embora a tabela considere que voz seja de coleta mais difícil do que face, essa facilidade pode facilmente se inverter em ambientes médicos em que são usados equipamentos de proteção facial e máscara. Como outro exemplo, atualmente a facilidade de circunvenção de autenticação por face em sistemas remotos tem sido fortemente influenciada por técnicas de inteligência artificial (o chamado "deep fake" [Wojewidka, 2020]). Entretanto, em sistemas em que a biometria é coletada por sensores localmente, técnicas de circunvenção como o uso de máscaras 3D teriam que passar por diversos sensores voltados a verificar a presença de um usuário humano em frente à câmera (conceito conhecido como *liveness*, ou "prova de vida") [Hernandez-Ortega et al., 2023]; exemplos incluem o uso de múltiplas câmeras, para captura do rosto de diferentes ângulos, e sensores de calor.

É relevante também ressaltar que a utilização de características comportamentais, em conjunto com características físicas, costuma ser interessante para aprimorar ainda mais a segurança e a precisão dos sistemas biométricos. A combinação inteligente dessas abordagens permite o desenvolvimento de sistemas multimodais, que utilizam múltiplas características para verificar a identidade de um indivíduo. Em particular, o uso de características comportamentais é útil em cenários nos quais a captura de características físicas pode ser desafiadora ou indesejada [Li and Jain, 2015]. Por exemplo, em sistemas de autenticação remota, o reconhecimento de voz ou a análise da forma de digitação podem ser preferíveis em comparação com a coleta de impressões digitais ou outros dados biométricos físicos. À medida que a biometria se torna mais integrada no cotidiano dos usuários, é fundamental considerar a privacidade e a proteção dos dados biométricos, garantindo o uso responsável e ético dessas tecnologias para o benefício de todos.

Tabela 6.1: Comparativo entre as abordagens clássica e contemporânea de biometria

Biometrias	**Universalidade**	**Exclusividade**	**Permanência**	**Coletabilidade**	**Desempenho**	**Aceitabilidade**	**Circunvenção**
Face	alta	baixo	média	alta	baixo	alta	alta/baixo
Impressão Digital	média	alta	alta	média	alta	média	alta/média
Geometria da Mão	média	média	média	alta	média	média	média
Veias das mãos	média	média	média	média	média	média	alta
Iris	alta/média	alta	alta	média	alta	baixo	alta/baixo
Retina	alta	alta	média	baixo	alta	baixo	alta
Assinatura	baixo	baixo	baixo	alta	baixo	alta	alta/baixo
Voz	média	baixo	baixo	média	baixo	alta	alta/baixo
Termograma	alta	alta	baixo	alta	média	alta	alta

Na Tabela 6.1 podemos notar que existem colunas com um único valor e colunas com dois valores. As colunas que possuem um único valor informam que a avaliação efetuada por [Balakrishnan et al., 2021] e [Jain et al., 1996] são a mesma. Nas colunas que possuem dois valores, o primeiro valor é referente a avaliação de [Jain et al., 1996], e o segundo valor é referente a avaliação de [Balakrishnan et al., 2021].

6.2.3. Métodos de Captura e Análise de Dados Biométricos

A captura de dados biométricos é um processo fundamental para realizar a identificação e autenticação biométrica. Os métodos, técnicas e dispositivos de captura podem variar dependendo da característica biométrica.

Os sensores ópticos são comumente utilizados na captura de características como impressões digitais, reconhecimento facial, íris e retina. Esses sensores capturam imagens detalhadas das características biométricas e as convertem em dados digitais [Oliveira Filho, 2014]. Processo similar acontece com câmeras de alta resolução, que costumam ser amplamente utilizadas para capturar imagens faciais, geometria da mão e outros traços físicos. Por meio de algoritmos específicos, é possível extrair as informações relevantes e criar modelos biométricos aproximadamente exclusivos para cada indivíduo.

No caso da captura de voz, são utilizados microfones. As amostras de som capturadas são analisadas por meio de algoritmos de reconhecimento de voz, que identificam padrões e características distintivas para autenticação biométrica.

Já para assinaturas manuais de usuários, é comum o uso de canetas digitais. Os sensores embutidos na caneta registram os movimentos e a pressão exercida durante a escrita, gerando uma representação digital precisa da assinatura, semelhante a técnica

já citada de formas de digitação. Outra alternativa consiste no uso de mesas digitalizadoras. Combinadas ou não com canetas digitais, esses dispositivos permitem que os usuários escrevam suas assinaturas diretamente na superfície digital, capturando características biométricas relevantes (e.g., velocidade e trajetória do movimento) em tempo real [Oliveira Filho, 2014].

6.2.4. Aplicações da biometria

A biometria tem encontrado uma amplitude de aplicações em diferentes setores, em particular devido à conveniência de seu uso em tarefas de identificação e autenticação de indivíduos, com base em características únicas do corpo humano. Algumas das principais áreas em que a biometria é amplamente utilizada incluem [Jain et al., 1999]

- **Identificação pessoal:** A aplicação mais comum da biometria é na identificação pessoal. As impressões digitais, o reconhecimento facial, a íris, a voz e a geometria da mão são alguns dos atributos biométricos utilizados para estabelecer a identidade de uma pessoa de maneira única e confiável. Isso tem sido aplicado em *smartphones*, *tablets* e *laptops* para autenticação de usuário, substituindo senhas e PINs.
- **Controle de acesso:** A biometria é frequentemente utilizada em sistemas de controle de acesso para garantir a segurança em locais restritos. Impressões digitais e reconhecimento facial são os métodos mais comuns nesse contexto. Estes são usados em aeroportos, prédios corporativos, laboratórios de pesquisa e outras instalações nas quais a identificação precisa é crucial para a entrada ser autorizada.
- **Aplicações forenses:** A biometria desempenha um papel importante na investigação criminal e na aplicação da lei. As impressões digitais são usadas para comparar e identificar suspeitos, enquanto a análise de voz pode ser útil para fins de reconhecimento de voz e identificação de locutor. Além disso, o reconhecimento facial é utilizado para confrontar imagens de vigilância e auxiliar na identificação de suspeitos.
- **Saúde e cuidados médicos:** A biometria tem sido aplicada na área da saúde para garantir a segurança do paciente, acessar registros médicos eletrônicos e controlar o acesso a áreas restritas, como salas de cirurgia e laboratórios. Além disso, sistemas biométricos são utilizados para monitorar sinais vitais, como frequência cardíaca e padrões de respiração, fornecendo informações precisas para diagnósticos e tratamentos.
- **Serviços financeiros:** A biometria está sendo cada vez mais utilizada nos serviços financeiros para aumentar a segurança das transações. As impressões digitais, reconhecimento facial e voz são usados para autenticação de identidade em caixas eletrônicos, pagamentos móveis e autenticação de transações *online*, substituindo senhas e códigos de acesso que podem ser comprometidos.
- **Educação:** A biometria também possui aplicações na área educacional, principalmente em instituições de ensino e exames. Os sistemas biométricos podem ser utilizados para registro de presença de alunos, controle de acesso a áreas restritas e garantir a integridade dos exames, evitando fraudes e substituições de identidade.

Essas são apenas algumas das muitas aplicações da biometria, revelando o seu amplo potencial em garantir a segurança, facilitar processos de identificação e melhorar a eficiência em várias áreas. Com o contínuo desenvolvimento de tecnologias biométricas

e aprimoramento dos algoritmos, se espera que a biometria desempenhe um papel ainda mais significativo no futuro, transformando a forma como se autentica e identifica.

6.2.5. ISO/IEC 24745:2022

A ISO/IEC 24745:2022 [ISO/IEC 24745, 2022] é uma versão atualizada e aprimorada da ISO/IEC 24745:2011 e aborda a necessidade de mecanismos de autenticação seguros para aplicações fornecidas pela Internet, como serviços bancários *online* e atendimento médico remoto por exemplo. Com o aumento da dependência da Internet, a autenticação adequada entre os usuários e os serviços se torna cada vez mais crítica. A norma aborda especificamente o uso de técnicas biométricas como um mecanismo de autenticação confiável, servindo como base para o levantamentos realizados durante o processo de revisão sistemática sobre biometria, segurança e sistemas.

A ISO/IEC 24745:2022 possui diversos aspectos relevantes, mas em função da limitação de páginas do minicursos, destacam-se [ISO/IEC 24745, 2022]:

- **Autenticação biométrica:** A norma reconhece a autenticação biométrica como uma abordagem confiável para verificar a identidade de um indivíduo. Isso envolve o uso de características comportamentais e fisiológicas, como impressões digitais, padrões de voz, imagens da íris e imagens faciais para reconhecimento automatizado.
- **Compromisso entre privacidade e segurança:** A autenticação biométrica levanta preocupações sobre a privacidade dos dados biométricos dos indivíduos. Embora a vinculação precisa entre o indivíduo e a credencial biométrica forneça uma forte garantia de autenticação, também apresenta desafios em relação à proteção dos dados biométricos e à prevenção de seu uso indevido.
- **Proteção de dados biométricos:** A norma aborda a proteção dos dados biométricos em relação aos requisitos de confidencialidade, integridade e renovabilidade/revogabilidade durante o armazenamento e a transferência. Isso inclui a vinculação segura entre uma referência biométrica (BR) e uma referência de identidade (IR), além de fornecer diretrizes para o gerenciamento e o processamento seguros e em conformidade com a privacidade dos dados biométricos.
- **Modelos de aplicação de sistemas biométricos:** São descritos diferentes cenários de aplicação de sistemas biométricos, incluindo o armazenamento e a comparação de referências biométricas. Além disso, inclui uma análise de ameaças e as contramedidas inerentes aos modelos de aplicação de sistemas biométricos.
- **Privacidade do indivíduo:** Fornece orientações sobre a proteção da privacidade do indivíduo durante o processamento de informações biométricas. Isso inclui garantir que as informações biométricas sejam processadas de maneira segura e em conformidade com as regulamentações de privacidade aplicáveis.

Em síntese, este capítulo proporciona uma visão abrangente das características biométricas, suas aplicações e o processo de captura e análise de dados. Explora-se a diversidade de usos da biometria, desde a identificação pessoal até aplicações forenses, saúde, serviços financeiros e educação. Com isso compreende-se a importância da avaliação criteriosa das características biométricas em termos de suas propriedades exclusivas, confiabilidade e aceitabilidade pelos usuários. Além disso, enfatiza-se a necessidade de considerar a privacidade dos dados biométricos em todas as etapas. A Seção 6.3 aprofunda as abordagens sobre Sistemas Biométricos, na qual são examinadas as diferentes

abordagens, tecnologias e desafios associados a esses sistemas, ampliando o entendimento sobre como a biometria é implementada para garantir identificação e autenticação precisas e seguras.

6.3. Sistemas biométricos

A presente seção aborda os principais aspectos dos sistemas biométricos e seu funcionamento, bem como seus subsistemas e como estes se relacionam de acordo com a ISO/IEC 24745 [ISO/IEC 24745, 2022].

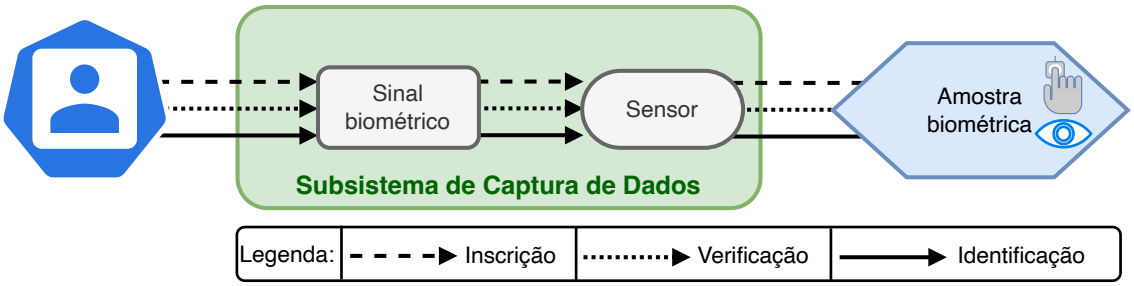
6.3.1. Sistemas e subsistemas biométricos

A biometria associada às tecnologias computacionais é conhecida como sistemas biométricos. Os sistema biométricos são empregados para realizar o reconhecimento por meio de características físicas ou comportamentais, que sucintamente se referem a um conjunto de diversas etapas de um processo com a finalidade de identificação e autenticação de indivíduos [Marcondes, 2019]. De um modo geral, um sistema biométrico tem como principal função vincular, atendendo requisitos de segurança, uma referência de identidade (IR) com uma referência biométrica (BR) de acordo com a aplicação em que está inserido. Os conceitos de IR e BR podem ser definidos, respectivamente, como um atributo não biométrico capaz de identificar exclusivamente um indivíduo dentro de um domínio específico e uma ou mais amostras ou modelos biométricos pertencentes a um titular dentro do sistema biométrico [ISO/IEC 24745, 2022]. A escolha de uma IR dependerá do contexto de uso da aplicação, por exemplos: número do Registro Civil (RG), número de matrícula/inscrição associada ao domínio (instituição de ensino, companhia, clube, etc.) e número de passaporte. Já a BR é a representação de uma característica biométrica, e.g., uma imagem facial armazenada digitalmente em um passaporte ou um modelo de minúcias de impressão digital em uma carteira de identidade. Além disso, ao processar amostras biométricas por algoritmos, as características são convertidas para representações matemáticas que também são consideradas referências biométricas.

Existe uma sequência de processos para vinculação de uma IR a uma BR e sua utilização dentro do sistema biométrico. Cada um destes processos é realizado por um subsistema, que são partes menores e independentes dentro do sistema biométrico principal. Estes subsistemas tem funções específicas que se relacionam sequencialmente para atingir o objetivo principal de cadastrar, identificar e verificar a identidade de um individuo, sendo estas a captura de dados, processamento de sinal, armazenamento, comparação e decisão. Vários subsistemas podem ser incluídos adequando à necessidade da aplicação, mas, conforme referencia a norma, os cinco principais subsistemas são:

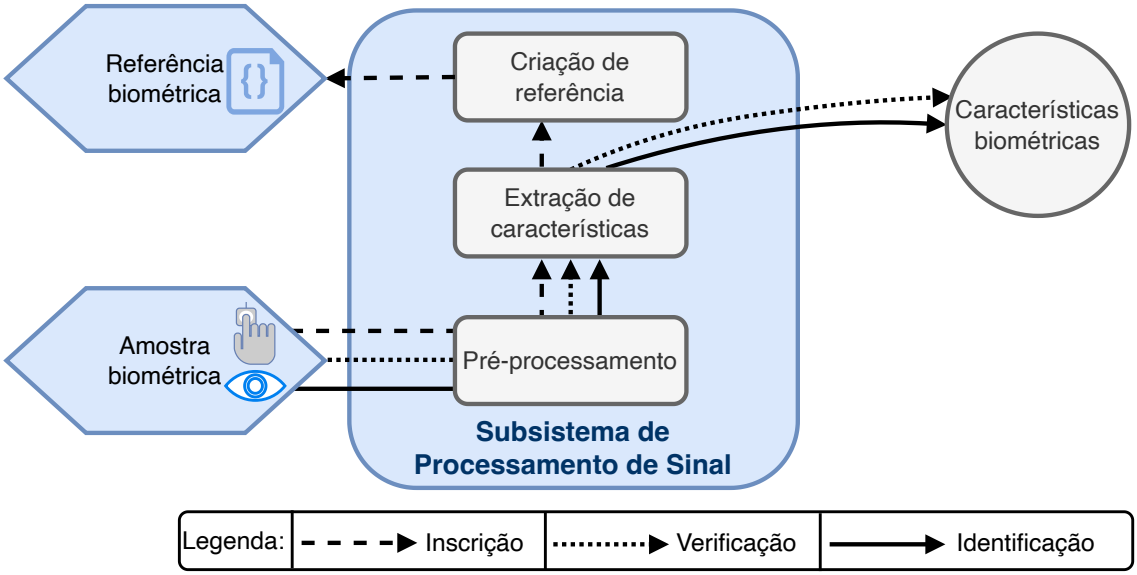
- **Captura de Dados:** É o conjunto de elementos que contém dispositivos ou sensores para coletar sinais de uma característica biométrica e convertê-los em um formato adequado para ser utilizado. A Figura 6.5 ilustra quando o usuário insere a sua biometria e o sinal biométrico é capturado por um sensor que converte para uma amostra biométrica que é enviada ao próximo subsistema. O Subsistema de Captura de Dados depende do tipo de biometria utilizada e afeta todo o desempenho do sistema a partir da qualidade da amostra obtida e do sensor ou dispositivo de coleta.

Figura 6.5: Subsistema de Captura de Dados.



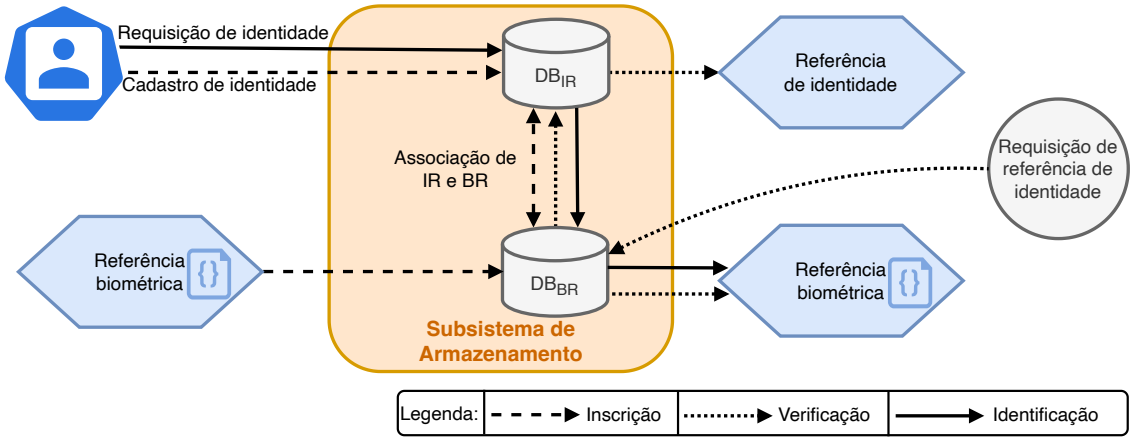
- **Processamento de Sinal:** Esta etapa é responsável por aprimorar a biometria bruta extraindo um conjunto de recursos possíveis de serem comparados com outras amostras biométricas previamente registradas em um Subsistema de Armazenamento. A Figura 6.6 indica que primeiramente é feito um pré-processamento no qual o sistema realiza correções, ajustes e remoção de ruídos para melhorar a qualidade da amostra obtida. Após isso, o sistema extrai características distintivas dependendo do tipo de biometria utilizada e, baseado nas propriedades extraídas, pode enviar diretamente ao sistema de comparação (processo de identificação ou verificação) ou criar uma referência biométrica para ser armazenada (processo de inscrição).

Figura 6.6: Subsistema de Processamento de Sinal.



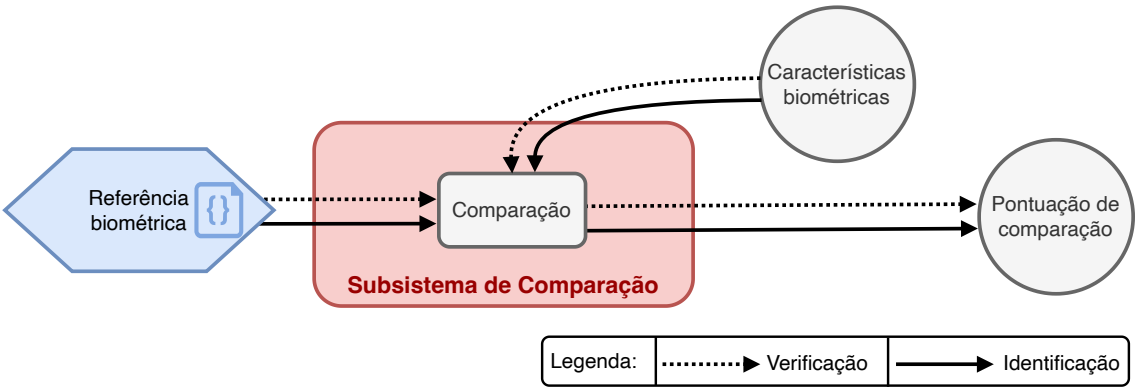
- **Armazenamento de Dados:** São bancos de dados que armazenam e vinculam as BRs e IR. A Figura 6.7 ilustra o processo em que um banco de dados recebe a referência de identidade do usuário e a referência biométrica processada pelo Subsistema de Processamento de Sinal. Assim, pode atender requisições externas, como por exemplo fornecer uma BR armazenada para comparação ou uma IR para o processo de identificação, e.g., os bancos de dados geralmente são separados por questões de segurança e privacidade.

Figura 6.7: Subsistema de Armazenamento.



- **Comparação:** É nesse subsistema que é determinada a similaridade entre as características biométricas capturadas e as referências biométricas armazenadas previamente no Subsistema de Armazenamento conforme a Figura 6.8. Em um processo de verificação, é utilizada a comparação 1:1, na qual a característica biométrica é comparada com uma BR armazenada pertencente a um titular único e produz uma pontuação para comparação. Já em em um processo de identificação, a pontuação é baseada em uma comparação 1:N entre a característica obtida e um conjunto de BRs armazenadas pertencentes a mais de um titular.

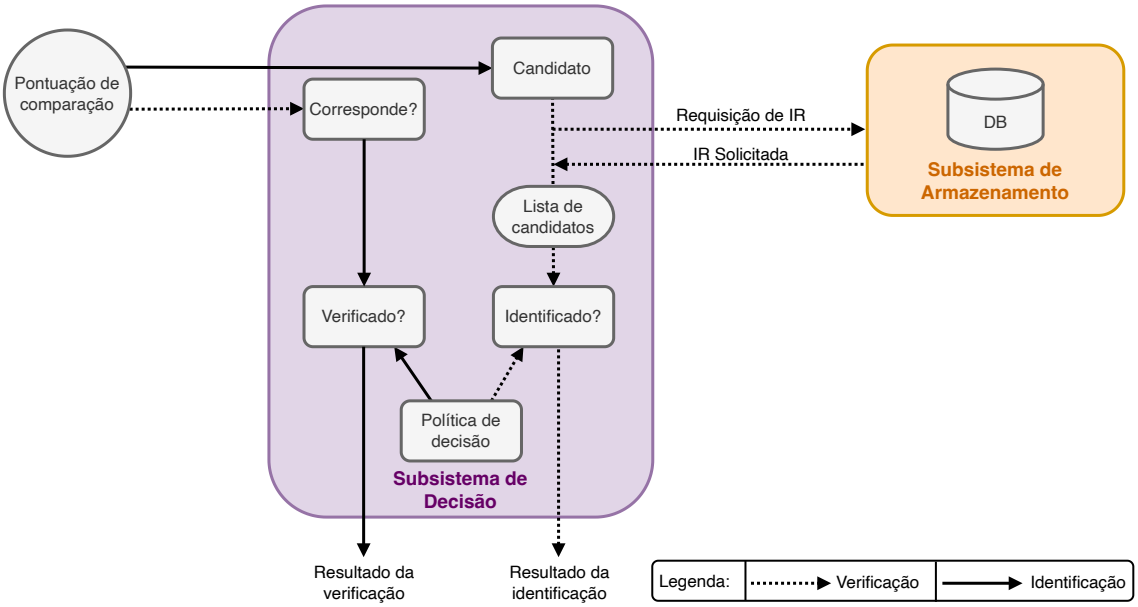
Figura 6.8: Subsistema de Comparação.



- **Decisão:** É o momento em que o subsistema determina se a amostra capturada é similar o suficiente com a referência armazenada para que ambas tenham a mesma fonte. O subsistema tem como entrada a pontuação obtida no Subsistema de Comparação e a saída é decisão tomada, que se difere nos dois processos de verificação e identificação exemplificados na Figura 6.9. Na verificação, é averiguado se a pontuação obtida é suficiente para corresponder ao usuário cadastrado e, baseado na política de decisão, o sistema retorna a aceitação ou rejeição do titular dos dados biométricos. Na identificação, o sistema determina, pela pontuação obtida, se o usuário é um candidato ou não.

Para isso, solicita ao banco de dados a(s) IR(s) associada(s) à(s) BR(s) candidata(s) e pode retornar uma identidade ou uma lista de candidatos, também baseado na política de decisão aplicada.

Figura 6.9: Subsistema de Decisão.



Além dos cinco principais subsistemas, outros podem ser incluídos conforme a necessidade. Estes podem ser relacionados às medidas de segurança, privacidade, formatação de dados, adaptação de referência (quando se deseja minimizar fatores externos que podem afetar a taxa de reconhecimento ou para atualizar referências que podem ser alteradas por efeitos de envelhecimento, por exemplo), entre outros.

6.3.2. Ciclo de vida das informações em sistemas biométricos

O ciclo de vida de informações biométricas se refere ao conjunto de etapas que um dado é submetido desde a sua coleta, uso e descarte adequados. O gerenciamento da privacidade durante todo esse processo é relevante e deve estar em conformidade com as regulamentações e leis de proteção de dados. Esta subseção aborda requisitos e diretrizes para garantir a privacidade das informações biométricas bem como as etapas do ciclo de vida em que esses dados são submetidos.

6.3.2.1. Requisitos e diretrizes

Dados biométricos são informações pessoalmente identificáveis (PII), i.e., que estes podem estar direta ou indiretamente vinculados ao titular a quem se referem e podem permitir identificá-lo. Sendo assim, para tratar as questões relacionadas à privacidade e proteção de dados pessoais em sistemas de tecnologia da informação, incluindo os sistemas que utilizam as tecnologias biométricas, recomenda-se que a norma internacional [ISO/IEC

29100, 2011] seja aplicada. Para garantir a proteção contra ameaças à privacidade na utilização de dados biométricos, são estabelecidos três requisitos e diretrizes de privacidade:

- **Irreversibilidade:** Um dos principais objetivos da [ISO/IEC 29100, 2011] é garantir a transparência em relação às práticas de coleta e uso de dados pessoais. Isso significa que os dados biométricos não devem ser utilizados para qualquer finalidade diferente da originalmente pretendida. Para isso, estes devem ser processados por transformações irreversíveis antes do armazenamento, evitando que seja possível a recuperação dos traços biométricos que originaram a BR. Uma das maneiras de alcançar esse objetivo é através da aplicação de uma função de transformação inversível, ou unidirecional, como a cartesiana e polar.
- **Desvinculabilidade:** Ao capturar dados biométricos, o sistema deve evitar que informações biométricas sejam correlacionadas entre bancos de dados de uma mesma aplicação ou de aplicações distintas. No caso de uma mesma aplicação, se o modelo biométrico do usuário for revogado, a mesma biometria deve ser capaz de gerar um novo modelo diferente do antigo. Já em aplicações distintas, a desvinculabilidade deve garantir que não haja relação entre dois modelos da mesma biometria, evitando a comparação cruzada entre bancos de dados.
- **Confidencialidade:** A segurança de dados também deve ser assegurada segundo a [ISO/IEC 29100, 2011]. Sendo assim, um sistema biométrico deve ter confidencialidade para proteger BRs contra o acesso não autorizado de entidades. Uma das principais medidas para evitar esse risco à privacidade é separar o armazenamento e utilizar servidores protegidos com controle de acesso, e utilizar criptografias específicas durante a transmissão e o armazenamento dos dados biométricos.

6.3.3. Privacidade do ciclo de vida

O ciclo de vida engloba todas as etapas em que um dado biométrico entra no sistema até o seu desuso, sendo estes: coleta, transferência, uso, armazenamento, retenção, arquivamento e *backup* de dados e descarte. De acordo com a [ISO/IEC 24745, 2022], os requisitos de privacidade que devem ser cumpridos em cada uma das etapas são:

- **Coleta:** O consentimento do sujeito ao tomar posse de seus dados biométricos é de extrema importância nessa etapa. Não obstante, mesmo que a organização tenha a permissão, esta deve apenas extrair a quantidade mínima de informações biométricas necessárias para a finalidade pretendida. O usuário deve ser informado sobre a finalidade da coleta e por quanto tempo seus dados vão ser retidos, quais as alternativas caso o mesmo não queira ou não possa ser cadastrado, o tipo e a quantidade de informações biométricas capturadas, como estas serão processadas no sistema biométrico e informações de identificação sobre o responsável, e a organização que vão gerir seus dados.
- **Transferência:** Esta etapa diz respeito a transferências de informação biométrica entre a organização e um terceiro. Para garantir a privacidade nesse processo, além do consentimento explícito ou implícito no serviço solicitado pelo sujeito, deve-se fornecer a ele informações como: quem irá recebê-las, qual o conteúdo e a quantidade que será transferida, qual entidade irá efetuar a transmissão, a finalidade e o período de retenção dos dados.

- **Uso:** Ao entrar em um sistema biométrico, os dados podem ser acessados, processados ou modificados para a finalidade específica do sistema. Sendo assim, o titular deve estar ciente e dar permissão para esta utilização. Na condição da organização ter a intenção de utilizar as informações para outros fins diferente dos especificados, novamente deve informar a descrição da nova finalidade e o período da retenção de dados, tendo a aceitação do usuário e evitando o desvio de função ou a utilização para obter dados relacionados à saúde ou genética do mesmo.
- **Armazenamento:** Como um Subsistema de Armazenamento pode ser distribuído, para garantir a confidencialidade e a integridade dos dados, pode ser necessário que as informações sejam identificadas como PII confidenciais. As organizações devem manter as informações física ou logicamente separadas de outras PIIs do titular para reduzir o impacto na privacidade do titular.
- **Retenção:** Se refere ao período em que os dados biométricos serão mantidos no sistema até o descarte. Para evitar que gere riscos tanto à organização quanto à informação biométrica, é necessário retê-las apenas pelo tempo necessário. Além disso, para não haver problemas durante auditorias, é importante garantir justificativas concretas para manter esses dados.
- **Arquivamento e *backup* de dados:** Esta etapa é responsável por contribuir na garantia de disponibilidade e integridade dos dados biométricos ao longo do tempo. O arquivamento serve para armazenar informações que não estão mais em uso ativo para preservação permanente ou a longo prazo. A criação de cópias de segurança dos dados biométricos em intervalos regulares pelo *backup*, assim como o arquivamento, deve atender políticas de segurança e privacidade mantendo controle de acesso aos dados.
- **Descarte:** Após fazer uma coleta de dados biométricos, caso o objetivo tenha sido atingido, o período de retenção dos dados tenha sido expirado ou o titular conteste o consentimento na coleta ou uso das informações biométricas, a organização ou terceiros que a possuem devem descartá-las de forma segura. Isso serve até mesmo para armazenamento distribuído e dados de *backup*.

6.3.4. Principais processos dos sistemas biométricos

Para efetivar o reconhecimento de uma pessoa, um sistema biométrico é composto por três processos principais:

- **Inscrição:** É realizado o cadastro de dados por meio dos sensores do Subsistema de Captura de Dados que envia a amostra biométrica para o Subsistema de Processamento de Sinal. É nesse momento em que os dados são processados e convertidos para um formato que o sistema entenda e finalmente são extraídas as referências biométricas para serem armazenadas e utilizadas para comparação futuramente [T. R. Jacqueline, 2012]. Além disso, durante a inscrição também é necessário que o usuário apresente sua IR para a associação com a BR cadastrada. Esse processo é finalizado no Subsistema de Armazenamento, onde o tipo de aplicação vai definir como e onde serão guardadas as informações.
- **Verificação:** A verificação se inicia da mesma forma que a inscrição, capturando os dados biométricos e processando-os para comparação com modelos armazenados. Porém, em vez de seguir para o banco de dados, as informações vão para o Subsistema de

Comparação, e, com base na pontuação de similaridade entre estas e a referência cadastrada no processo de inscrição, o Subsistema de Decisão determinará se pertencem ao mesmo indivíduo.
- **Identificação:** O processo de identificação é muito similar ao de verificação. Entretanto, ao chegar no Subsistema de Comparação, o sistema calcula a similaridade entre a amostra obtida e outras referências armazenadas. Assim, o Subsistema de Decisão retorna se existe pelo menos um ou mais correspondentes as informações biométricas fornecidas.

A verificação e a identificação realizam a autenticação e dependem dos dados armazenados na inscrição. A principal diferença entre estas é a forma de comparação e decisão. Na identificação, o usuário apresenta sua biometria e o Subsistema de Comparação determina a similaridade entre esta e um conjunto de BRs de mais de um titular já cadastrados, retornando as pontuações de comparação entre estas. Logo, o objetivo da identificação é obter uma identidade ou uma lista de candidatos em uma busca 1:N de acordo com a pontuação de comparação e com a política de decisão. Já na verificação, além da biometria, o indivíduo deve informar sua IR para que o sistema faça uma busca específica (1:1) e verifique se os dados informados pertencem a fonte que reivindicou. A decisão desse processo também depende da pontuação de comparação e da política de decisão do sistema.

6.3.5. Aplicações dos sistemas biométricos

Existem diversos sistemas que utilizam a biometria para trazer mais segurança e conveniência para o usuário. Esta seção elenca alguns exemplos de uso de biometria nos quais os *templates* biométricos necessitam ser tratados adequadamente.

6.3.5.1. Urnas eletrônicas

O sistema de votação eletrônico brasileiro tem por objetivo garantir segurança e transparência no processo eleitoral. Com a evolução desse sistema, foram realizados aprimoramentos para resolver problemas relacionados à segurança e privacidade do eleitor, entre estes, em 2006, a incorporação da identificação biométrica [Schauren, 2016].

O cadastro da biometria é um processo que envolve a coleta das informações biométricas dos eleitores, como suas impressões digitais, para criar um registro único e seguro. Ao apresentar um documento oficial com foto, é feita a coleta de IR baseada na carteira de identidade, carteira de motorista ou passaporte. A coleta da amostra biométrica é feita por meio de um *scanner* biométrico (normalmente dos dedos indicador e polegar das duas mãos). Para evitar duplicidade, as impressões digitais e fotos coletadas dos eleitores são comparadas, uma a uma, com as outras armazenadas no Cadastro Eleitoral por meio do Sistema Automatizado de Identificação Biométrica (ABIS) [Tribunal Superior Eleitoral, 2023]. Em seguida, os dados são processados e armazenados em um banco de dados da Justiça Eleitoral de forma segura e cifrada.

No dia da eleição, acontece a identificação do eleitor. Ao se apresentar à Mesa Receptora de Votos, o indivíduo apresenta novamente o documento com foto e insere

os dados biométricos para liberação da urna. Ao inserir a digital no leitor disposto no Terminal do Mesário, o sistema faz até quatro tentativas de reconhecimento das digitais. Durante o período de votação, a urna eletrônica não tem contato com nenhuma rede de computadores. Portanto, todas e somente as informações dos eleitores da seção em específico são inseridas previamente e contem um lacre, que quando removido a torna inutilizável [Tribunal Reginal Eleitoral, 2023]. Por se tratar de um processo de identificação, o sistema busca uma correspondência única da impressão digital apresentada pelo eleitor em relação a todas as impressões digitais cadastradas no banco de dados eleitoral, garantindo assim que apenas os eleitores autorizados votem e que não haja duplicação de votos.

6.3.5.2. Controle de acesso

O controle de acesso pode ser aplicado em diversos cenários e utilizando diversos tipos de biometria. Recentemente, divulgou-se o caso de uma torcedora de um time brasileiro que foi fatalmente atingida por estilhaços de uma garrafa de vidro antes de uma partida de futebol. O clube mandante da partida havia instalado um sistema de reconhecimento facial que auxiliou na identificação do responsável por atirar a garrafa.

Nessa aplicação, o cadastro é feito pelo site do clube no qual o usuário informa seus dados pessoais e, caso esteja acessando de um computador, recebe um *QR Code* para acesso a câmera do celular para cadastro da face. Caso já esteja no celular, a câmera apenas abre para o registro da biometria facial [Palmeiras, 2023].

A política de privacidade disponibilizada no site oficial do clube dispõe dos tratamentos realizados nos dados pessoais, como por exemplo garantir a criptografia, acesso somente a pessoas autorizadas, incluindo o torcedor titular, e a não divulgação dos mesmos exceto por determinação judicial [Palmeiras, 2021]. No dia do evento esportivo, os torcedores devem passar por catracas com câmeras que devem identificá-los. Uma luz verde é emitida caso a imagem facial captada seja a mesma do torcedor que adquiriu o ingresso para a respectiva seção. O site não disponibiliza detalhes do processamento de dados e do armazenamento realizado pela aplicação.

6.3.5.3. Autenticação por voz

A detecção por alto-falante ou *speaker*, pode ser utilizada em diversos serviços e aplicativos. A Instituição de Engenharia e Tecnologia e Wiley [Mtibaa et al., 2021] publicou uma abordagem em que essa tecnologia é aplicada de forma segura.

Na fase de inscrição dessa aplicação não é definido qual dispositivo realiza a captura, mas cita sua utilização em *smartphones*, que utilizam seu próprio microfone para essa função. No processamento de dados são utilizados recursos *Mel-frequency cepstral coefficients*s (MFCCs) para converter o sinal de áudio de fala em uma representação mais compacta e adequada para análise. Ainda nessa fase, um *token* é gerado e utilizado para embaralhar a amostra obtida antes do armazenamento. Na aplicação, o armazenamento é distribuído de acordo com o Modelo G da [ISO/IEC 24745, 2022], no qual os dados são

registrados parcialmente em um *token* (informado pelo usuário durante a fase de verificação) e em um servidor.

Durante a fase de verificação, a captura de dados é feita da mesma forma da inscrição e são aplicadas transformações para proteger a amostra obtida. O sistema faz a comparação baseado em cálculos da distância de Hamming e a decisão é tomada com base em um limite predefinido, ambas acontecem no lado do servidor, que nunca tem acesso a voz e a referência biométrica do titular. Assim, são garantidos os requisitos de segurança do ciclo de vida das informações no sistema. A irreversibilidade é alcançada por meio das transformações aplicadas que tornam as referências computacionalmente inviáveis de obterem a original. A pontuação obtida em um arcabouço que avalia a desvinculabilidade em sistemas de proteção de modelo biométrico aponta que a abordagem é totalmente desvinculada, pois não foi possível identificar se dois vetores protegidos inscritos em aplicações diferentes pertencem a mesma pessoa.

Existem muitos outros tipos de aplicações de sistemas biométricos que se adéquam conforme a necessidade de autenticar indivíduos. Cada uma destas aplicações têm processos e subprocessos bem definidos e comuns umas as outras, bem como requisitos para manter a privacidade em cada etapa do ciclo de vida das informações utilizadas.

6.4. Segurança de sistemas biométricos

A rápida evolução da tecnologia biométrica trouxe consigo um amplo espectro de aplicações, desde autenticação pessoal até controles de acesso. No entanto, essa crescente adoção também apresenta desafios cruciais, sendo a segurança um destes. À medida que sistemas biométricos utilizam dados brutos, como a captura de impressões digitais, a questão da proteção dos modelos biométricos torna-se crucial. Essa evolução não está isenta de desafios, especialmente quando se trata da segurança dos dados sensíveis envolvidos [Patel et al., 2015a].

Um dos riscos emergentes nos sistemas biométricos é o comprometimento dos modelos biométricos, no qual um modelo comprometido de um indivíduo pode ser usado indevidamente para acessar as informações de outro. Esse cenário é conhecido como correspondência cruzada entre bancos de dados. Nesse contexto, surge a necessidade premente de implementar requisitos rigorosos para garantir a confidencialidade, integridade e disponibilidade dos dados biométricos.

A fim de enfrentar esses desafios, a ISO/IEC 24745:2022 estabelece uma estrutura sólida de requisitos para sistemas biométricos. Esses requisitos são cruciais para mitigar os riscos associados ao comprometimento de modelos biométricos e garantir a operação segura e eficaz dos sistemas. No entanto, além das normas, a discussão sobre requisitos adicionais que vão além da segurança pura e simples surge como um tópico relevante, buscando uma proteção abrangente contra uma gama de ameaças potenciais e proporcionar uma proteção abrangente aos dados sensíveis.

Este trabalho também aborda a segurança durante a transmissão de dados biométricos, explorando estratégias para proteger a confidencialidade e a integridade dos dados à medida que são transferidos entre diferentes subsistemas. Este processo é particularmente crucial devido à crescente complexidade e variação geográfica desses sistemas.

Nesse contexto, busca-se explorar a importância dos requisitos em sistemas biométricos, considerando tanto as diretrizes estabelecidas por normas quanto os requisitos adicionais propostos por especialistas na área. Além disso, é examinado como esses requisitos se traduzem em medidas práticas para garantir a integridade dos modelos biométricos, prevenir o uso indevido e assegurar a proteção das informações dos indivíduos. Ao reunir as preocupações de segurança e as orientações normativas, visa-se fornecer uma compreensão abrangente dos elementos essenciais para construir sistemas biométricos robustos e seguros.

6.4.1. Requisitos de segurança dos sistemas biométricos

Para garantir a segurança adequada de sistemas biométricos a [ISO/IEC 24745, 2022] é bem direta e sugere o cumprimento de quatro requisitos básicos:

- Confidencialidade: refere-se à propriedade que protege as informações contra acesso ou divulgação não autorizados. Nos sistemas biométricos, as BRs são geralmente armazenadas em bancos de dados específicos. Durante as etapas de inscrição e identificação, por exemplo, os dados biométricos são transmitidos entre as entidades envolvidas para comparação. Caso haja uma interceptação, acesso por entidades não autorizadas ou mesmo vazamento do banco de dados, a identidade dos indivíduos não será revelada. Portanto, a confidencialidade deve assegurar que uma referência biométrica obtida fora do sistema, como resultado de um vazamento, não possa ser associada a nenhum indivíduo. Para garantir a confidencialidade dos dados biométricos armazenados, é necessário utilizar algoritmos de criptografia.
- Integridade: a integridade garante que um dado dentro do sistema biométrico é confiável. Esta propriedade é fundamental para o devido funcionamento do sistema. Está presente principalmente nas etapas de coleta dos dados. No processo de autenticação a integridade do processo está diretamente relacionada a confiabilidade da amostra, se uma BR não for confiável a autenticação também não será. As BRs não confiáveis podem ocorrer devido aos seguintes motivos:
  - Corrupção acidental devido a mau funcionamento de hardware ou software;
  - Modificação acidental ou intencional de um BR de "boa-fé"por uma entidade autorizada (i.e., inscrito não autorizado ou proprietário do sistema), sem intervenção de um invasor; e
  - Modificação (incluindo substituição) de um BR de um inscrito autorizado por um invasor. A integridade pode ser garantida utilizando técnicas de criptografia combinadas com outras técnicas, como o uso de *smart cards*, técnicas de código de autenticação de mensagem (MAC), marcação de tempo, etc.
- Renovabilidade e revogabilidade: As BRs desempenham um papel fundamental nos sistemas biométricos. Sua segurança e privacidade são de extrema preocupação, uma vez que uma variedade de ameaças pode comprometer uma amostra contendo uma BR. Em caso de vazamento de dados, as perdas podem ser catastróficas, uma vez que a biometria de um indivíduo ficará exposta. É importante ressaltar que a biometria é algo que não pode ser alterado, o que intensifica a necessidade de proteção contra acesso não autorizado e comprometimento de dados pessoais. Para enfrentar esse desafio, a revogação das referências biométricas comprometidas se mostra indispensável.

A renovabilidade é proporcionada pelo processo de diversificação, o qual consiste na criação de múltiplas referências biométricas independentes entre si, a partir de uma ou mais amostras biométricas transformadas de um mesmo indivíduo. Essa abordagem não apenas preserva a privacidade do indivíduo, mas também garante a segurança das informações do proprietário, ao criar representações únicas e não diretamente relacionadas entre si. Por outro lado, a revogação de uma BR envolve o cancelamento do modelo comprometido. Nesse processo, todas as permissões são revogadas e uma nova BR é emitida pelo sistema. O novo modelo apresenta uma representação biométrica totalmente distinta e sem qualquer relação com a anterior. É importante ressaltar que esse novo modelo não deve corresponder a nenhuma outra referência comprometida. A revogação pode ser acionada por diversas razões, como a ocorrência de violações de segurança ou a validade por um período de tempo específico. Em todos esses casos, a revogação preserva a segurança do sistema e a privacidade do indivíduo, evitando potenciais usos indevidos de modelos biométricos comprometidos.

- Disponibilidade: é a garantia de acesso contínuo a informações por pessoas autorizadas. As medidas de segurança, como defesa contra ataques *Distributed Denial-of-Service* / negação de serviço distribuída (DDoS) e *backups* regulares, são essenciais. Redundância de hardware também mantém a disponibilidade, permitindo troca imediata em caso de falha, assegurando acesso seguro e confiável às informações.

Esses requisitos desempenham um papel fundamental na gestão de dados sensíveis, incluindo os biométricos. No entanto, é importante notar que os elementos de confidencialidade, integridade e disponibilidade não se limitam apenas aos sistemas biométricos. Na verdade, esses são comuns em diversos tipos de sistemas que lidam com informações sensíveis. Portanto, a presença desses três requisitos não é exclusiva dos sistemas biométricos, mas sim uma característica compartilhada por muitos sistemas que tratam de dados delicados [Li and Jain, 2009]. Apesar da norma [ISO/IEC 24745, 2022] sugerir estes requisitos, outros autores como Nafea [Nafea et al., 2016] sugerem que um sistema biométrico com alto nível de proteção deve atender aos seguintes requisitos:

- Segurança: A privacidade e a integridade dos dados biométricos devem ser extremamente difíceis de serem violadas através de meios computacionais. Isso envolve a implementação de medidas de segurança robustas para proteger os dados biométricos contra acesso não autorizado e uso indevido.
- Diversidade: A diversidade implica que a probabilidade de correspondência cruzada entre diferentes bancos de dados biométricos seja minimizada. Ou seja, os dados de um indivíduo em um sistema biométrico não devem ser relacionados com os dados em outro sistema.
- Revogabilidade: A capacidade de revogar um modelo biométrico comprometido é essencial. Se um modelo biométrico for comprometido, deve ser possível cancelá-lo e gerar um novo modelo para substituí-lo.
- Desempenho: A implementação de medidas de proteção não deve prejudicar o desempenho do sistema biométrico como um todo. É importante que as medidas de segurança adicionais não tenham um impacto negativo nas operações do sistema, garantindo um funcionamento eficiente e eficaz.

6.4.2. Ameaças e contramedidas de segurança dos sistemas biométricos

A segurança em sistemas biométricos é de extrema importância, uma vez que lida com informações altamente sensíveis, ou seja, as características biométricas únicas dos indivíduos. Como em qualquer sistema, existem ameaças que podem comprometer o seu funcionamento, principalmente nos subsistemas responsáveis pela captura e transmissão dos dados biométricos. Além dos requisitos de privacidade no ciclo de vida (Subseção 6.3.3) também existem ameaças potenciais que devem ser evitadas entre os subsistemas. Embora seja impossível evitar completamente todas as ameaças, é fundamental adotar medidas rigorosas para mitigá-las e proteger a integridade e confidencialidade dessas informações sensíveis [ISO/IEC 24745, 2022].

Algumas das ameaças potenciais enfrentadas pelos sistemas biométricos incluem: (i) ataques de falsificação, no qual uma pessoa malintencionada tenta imitar a biometria de outro indivíduo para obter acesso indevido; (ii) ataques de *Denial-of-Service* / negação de serviço (DoS) , que visam sobrecarregar o sistema, impedindo-o de responder às solicitações legítimas de autenticação; e (iii) ataques de interceptação, nos quais os dados biométricos são capturados durante a transmissão e utilizados indevidamente. Analisando o ciclo de vida (Subseção 6.3.3) estas ameaças podem ocorrer nas etapas de coleta e transferência.

Para lidar com essas ameaças, é essencial implementar protocolos de segurança no *template* ou modelo biométrico [Jain and Kant, 2015]. Isso inclui o uso de algoritmos de criptografia para proteger os dados biométricos armazenados e transmitidos. Além disso, é fundamental ter mecanismos de detecção de ataques e tentativas de falsificação, como análise de padrões anômalos ou uso de características biométricas multifatoriais, que envolvem a utilização de mais de uma característica biométrica, como face e impressão digital ou impressão digital e escrita, por exemplo.

A necessidade de proteger os modelos biométricos tem se tornado cada vez mais evidente, o que implica evitar o armazenamento desses dados exatamente como são obtidos dos usuários. Uma estratégia recomendada para proteger o modelo biométrico é a utilização de dados auxiliares para transformar os dados biométricos de referência em um novo formato. Nesse sentido, [Kaur and Khanna, 2016] apontam alguns pontos cruciais a serem considerados:

- Falsificação de identidade/roubo de identidade: caso os dados biométricos de alguém sejam perdidos, estes correm o risco de serem explorados por indivíduos mal-intencionados para obter acesso não autorizado a contas e serviços, e.g., um invasor poderia extrair secretamente impressões digitais latentes de um usuário, possibilitando a reconstrução de sua identidade física ou digital.
- Sensibilidade: Além de serem utilizados para identificação única, os dados biométricos contêm informações pessoais e confidenciais, como histórico médico e condições físicas.
- Vinculabilidade (*Linkability*): O compartilhamento crescente de dados biométricos pode levar ao rastreamento e localização de usuários em diferentes bancos de dados, permitindo a correlação de seus perfis. Esse cruzamento de informações para determinar a relação entre os modelos de referência armazenados deve ser evitado.

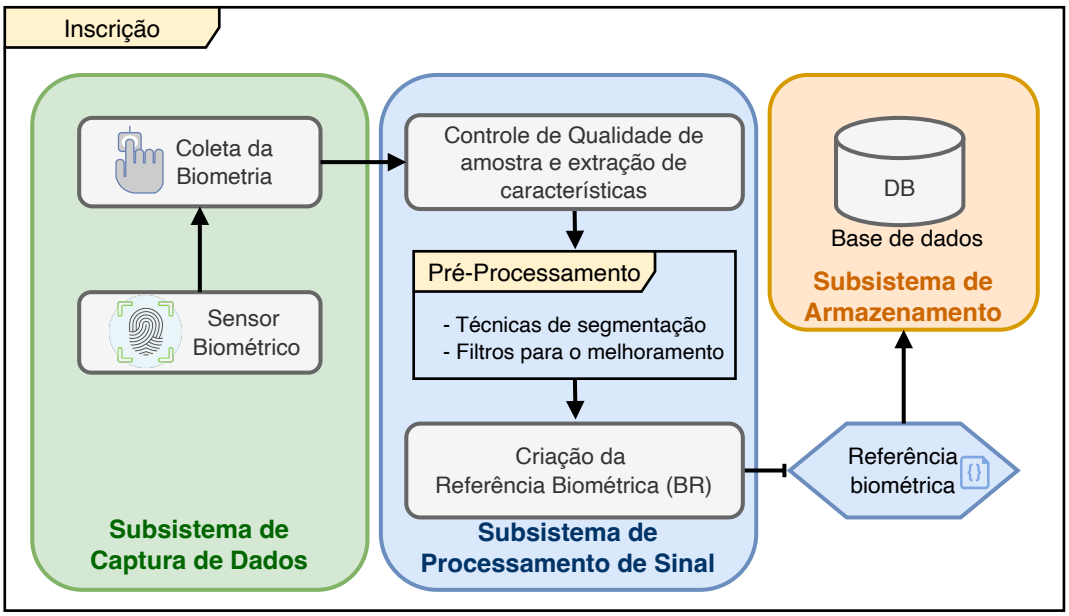
6.4.3. Funcionamento dos sistemas biométricos

Segundo [Jain and Kant, 2015] um sistema biométrico possui ao menos quatro partes: (i) sensor biométrico para a captura de dados; (ii) extrator de características; (iii) armazenamento em uma base de dados; e (iv) comparação para os processos de verificação e identificação. Já para o processo de inscrição envolve a captura de dados, extração de características e armazenamento.

6.4.3.1. Processo de Inscrição

O processo de inscrição de um novo usuário é a etapa inicial, no qual os dados biométricos do individuo são coletados e armazenados para possibilitar identificação futura no sistema. Este processo engloba o uso de três subsistemas: Captura de dados, Processamento de sinal e Armazenamento. O modelo representa o ciclo desta etapa pode ser visualizado na Figura 6.10.

Figura 6.10: Processo de inscrição de um sistema biométrico.



Para dar início a coleta dos dados biométricos pelo Subsistema de Captura de Dados (Figura 6.10), utiliza-se um sensor ou leitor biométrico para capturar as características únicas do indivíduo e após a coleta é enviado para o subsistema de processamento de sinal. Esse primeiro passo é essencial para obter os dados necessários para a identificação biométrica. Em seguida, os dados coletados passam por um processo de pré-processamento no subsistema de processamento de sinal, no qual a qualidade da amostra é avaliada. Essa qualidade está diretamente relacionada à eficiência e precisão do leitor biométrico utilizado e à forma como o dado biométrico foi fornecido pelo indivíduo. Caso a qualidade da amostra seja baixa, existem técnicas disponíveis para melhorá-la, e.g., podem ser aplicadas técnicas de segmentação ou filtros para aprimorar os pontos com ruídos, garantindo que a informação biométrica seja mais clara e precisa [Faria, 2014, Jain et al., 1999].

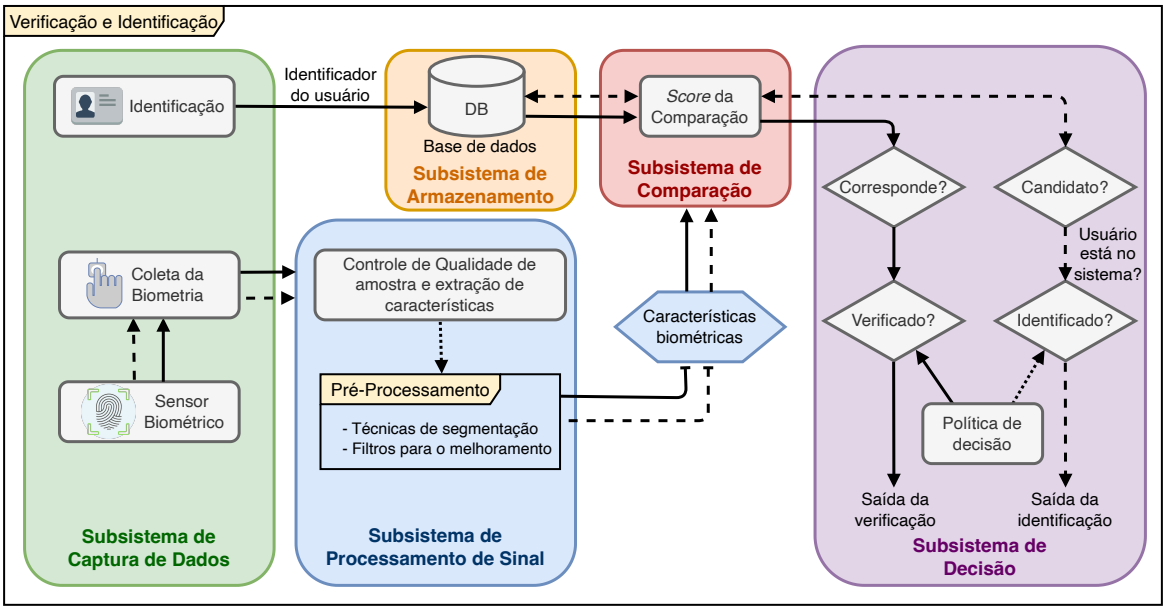
Após o pré-processamento, é gerada uma representação digital dos dados biométricos capturados, a referência biométrica BR. Esta referência é uma forma compacta

de armazenar as informações biométricas, e será usada para comparação e correspondência durante os processos de autenticação e identificação. Como pode-se verificar na Figura 6.10 no Subsistema de Processamento de Sinal nos módulos de controle de qualidade de amostra, pré-processamento e criação de referência biométrica (BR). A última etapa do processo de inscrição ocorre no Subsistema de Armazenamento como visto na Figura 6.10. Após a coleta e o tratamento da amostra biométrica, é crucial proceder ao armazenamento seguro das informações em um banco de dados que é realizado no Subsistema de Armazenamento. Nessa etapa, são aplicadas técnicas avançadas de proteção dos dados, como *fuzzy vault* [Juels and Sudan, 2006] que permite armazenar informações biométricas em um "cofre"seguro, o algoritmo transforma a informação biométrica em um conjunto de pontos em um espaço tridimensional que durante a comparação busca os pontos que estão mais próximos da chave criptográfica, permitindo que o usuário seja autenticado, isto garante que as características únicas dos indivíduos sejam preservadas com total segurança [Faria, 2014]. Essas medidas visam proteger os dados biométricos dos usuários contra acessos não autorizados, garantindo a confidencialidade e a integridade das informações [Faria, 2014].

6.4.3.2. Processo de Verificação e Identificação

Os sistemas biométricos são empregados na autenticação de indivíduos, sendo as operações principais são executadas de verificação e identificação [Bolle et al., 2013]. O processo de identificação e verificação são duas etapas cruciais em sistemas biométricos. A identificação busca encontrar uma pessoa em um banco de dados comparando suas características únicas com várias entradas. Já a verificação compara a amostra de uma pessoa com um modelo previamente fornecido para confirmar sua identidade. A Figura 6.11 ilustra a interação dos módulos envolvidos.

Figura 6.11: Funcionamento da verificação e identificação de um sistema biométrico.



A verificação é um processo em que o usuário apresenta uma credencial, como um código de identificação ou um cartão de acesso, juntamente com uma amostra biométrica, como uma impressão digital ou uma varredura facial. Essa etapa ocorre no Subsistema de Captura de Dados. A amostra coletada é então direcionada ao Subsistema de Processamento de Sinal para tratamento e controle de qualidade. A Figura 6.11 ilustra a interação nos Subsistemas de Captura de Dados e Processamento de Sinal. Após o tratamento, a amostra é encaminhada ao Subsistema de Comparação, o qual confronta a amostra com os dados biométricos armazenados no banco de dados, gerando uma pontuação de similaridade. Essa pontuação representa o grau de semelhança entre a amostra fornecida e a amostra armazenada. O processo de comparação segue o modelo 1:1, também conhecido como busca fechada, uma vez que o sistema procura um único registro específico para verificar a autenticidade do usuário que forneceu a amostra biométrica. O Subsistema de Decisão avalia se o usuário está presente na base de dados e se corresponde a um candidato válido. Com base nas políticas de decisão, o sistema produz a saída correspondente. Por outro lado, a identificação é um processo mais abrangente, em que o usuário fornece apenas uma amostra biométrica sem a necessidade de apresentar uma credencial. Após ser processada pelo Subsistema de Processamento de Sinal, a amostra é utilizada para realizar uma busca no banco de dados contendo múltiplos registros biométricos. Essa busca segue o modelo 1:N, ou busca aberta, no qual o sistema explora várias entradas para identificar o usuário desconhecido [Costa et al., 2006, ISO/IEC 24745, 2022]. O sistema compara a amostra com os registros biométricos existentes, gerando uma pontuação de comparação. Se uma correspondência suficientemente próxima for encontrada, o sistema identifica a presença do usuário no sistema. Com base nas políticas de decisão, o sistema retorna o resultado da verificação [Costa et al., 2006, ISO/IEC 24745, 2022]. A Figura 6.11 indica essa constante troca de informações entre os Subsistemas de Armazenamento e Comparação para executar a Identificação.

6.4.4. Principais Ameaças e Contramedidas

A análise e compreensão das principais ameaças e a implementação de contramedidas eficazes são elementos essenciais para a garantia da segurança de sistemas biométricos que lidam com informações sensíveis. Neste contexto, explorar as principais ameaças e estratégias para mitigá-las desempenha um papel crítico na sua proteção à privacidade. Os ataques podem ocorrer em várias áreas do sistema. A [ISO/IEC 24745, 2022] classifica esses ataques de acordo com os diferentes subsistemas ou etapas do sistema nos quais estão suscetíveis a ocorrer. Nesse sentido, é importante destacar os principais ataques identificados em nossa pesquisa. A análise da literatura pesquisada revelou que os subsistemas mais impactados por ataques foram a Captura de Dados e o Armazenamento. Isso evidencia uma preocupação mais acentuada dos pesquisadores com esses módulos específicos.

A segurança dos sistemas biométricos é fundamental na era da tecnologia digital, mas enfrenta desafios devido a uma variedade de ataques. Esses ataques buscam explorar vulnerabilidades nos processos de autenticação e identificação, comprometendo a integridade e a privacidade dos dados biométricos. Desde ataques de força bruta até manipulação de dados durante o processamento, a compreensão dessas ameaças é vital para desenvolver estratégias eficazes de proteção. Nesta perspectiva, são descritos os principais ataques

que os sistemas biométricos enfrentam e como funcionam:

- Ataque de Força Bruta: é um ataque no qual o invasor tenta entrar no sistema com diversas entradas de dados possíveis. Em sistemas biométricos pode ser aplicado inserindo sequências de características biométricas até que alguma consiga adentrar no sistema.
- Pessoa no Meio (MitM): ocorre quando um invasor intercepta os dados transmitidos em um meio de comunicação, podendo visualizar, modificar ou roubar os dados.
- Correspondência Cruzada (CrossRef): o ataque de correspondência cruzada ocorre em sistemas biométricos quando um adversário tenta identificar se um mesmo indivíduo está inscrito em dois ou mais sistemas independentes. Nesse tipo de ataque, o adversário tem acesso a modelos protegidos (*templates*) de diferentes sistemas e tenta verificar se esses modelos pertencem ao mesmo indivíduo, comprometendo assim a privacidade e segurança dos dados biométricos [Kelkboom et al., 2011].
- Ataque de Apresentação (Falsificação de Sensor): também conhecidos como ataques de *spoofing* ou apresentação falsa. Nesse tipo de ataque, um elemento biométrico falso, como um dedo sintético ou uma representação facial artificial, é exibido ao sensor por um indivíduo não autorizado, visando contornar os sistemas de identificação. Além disso, o agente mal-intencionado pode causar danos físicos ao sistema de reconhecimento ou inundá-lo com solicitações de acesso fraudulentas. É muito vulnerável já que o atacante não necessita de um conhecimento prévio para executar [Jain and Kant, 2015].
- Captura/reprodução de Sinais: Ao coletar dados biométricos em estado bruto, o sensor os encaminha por um canal de comunicação ao módulo de extração de recursos para pré-processamento. Este canal, localizado entre o sensor e o módulo de processamento de sinal, corre o risco de ser interceptado, permitindo o roubo e armazenamento dos dados biométricos. Posteriormente, esses dados armazenados podem ser reproduzidos no módulo de extração de recursos para burlar o sensor [Jain and Kant, 2015].
- Manipulação não autorizada de dados durante o processamento: Após coletar os dados biométricos brutos, o sensor os encaminha ao módulo de extração de características. No entanto, um invasor pode manipular esse processo, forçando o módulo de extração a gerar valores de características selecionados pelo intruso, em vez de utilizar os valores de características originados dos dados autênticos coletados pelo sensor [Jain and Kant, 2015].
- Manipulação das pontuações de comparação: O sensor é alvo de um ataque visando gerar a pontuação mais elevada escolhida pelo impostor, a fim de contornar o sistema de autenticação biométrica, independentemente dos valores provenientes do conjunto original de recursos de entrada [ISO/IEC 24745, 2022].
- Banco de dados comprometido: Isso acontece quando um impostor compromete a segurança do banco de dados ao inserir novos modelos, alterar modelos existentes ou remover modelos já presentes.
- Ataque de escalada: Os ataques de escalada envolvem um aplicativo que encaminha modelos de minúcias criados de forma sintética para o mecanismo de comparação. Com base na pontuação resultante da comparação, o aplicativo altera os modelos de maneira aleatória repetidamente até que o limite de decisão seja ultrapassado [Martinez-Diaz et al., 2006].

- DDoS: Um atacante emprega múltiplas máquinas para conduzir o ataque. Essas máquinas, conhecidas como *bots*, são selecionadas devido à sua vulnerabilidade. O atacante instala software nas máquinas *bots*, visando executar um ataque DDoS contra o alvo, resultando na indisponibilidade desejada desse alvo [Conrads, 2019].
- Manipulação de *Threshold*: Um intruso pode manipular o resultado informado pelo módulo de comparação. Nesse tipo de ataque, o impostor tem a capacidade de modificar a pontuação de correspondência que é enviada pelo canal de comunicação entre o módulo de comparação e o dispositivo de aplicação. Isso é feito com o objetivo de alterar a pontuação original e, por consequência, a decisão original (aceitar ou rejeitar) do módulo de comparação [Jain and Kant, 2015].

A Tabela 6.2 apresenta as principais ameaças que estão sujeitos os subsistemas, seguido das contramedidas para mitigá-las. Os conceitos de referência biométrica (BR) e referência de identidade (IR) estão na seção 6.3.1, os conceitos de referências biométricas renováveis (RBR) estão na seção 6.4.6 e podem ser consultados para esclarecer o conteúdo da tabela.

Tabela 6.2: Diferentes subsistemas biométricos seguidos das principais ameaças que podem sofrer e contramedidas que devem ser aplicadas.

Ameaças nos Subsistemas Biométricos		
Subsistemas	Ameaças	Contramedidas
Captura de Dados	Falsificação de sensor Captura/reprodução de sinais do sensor	Detecção de ataque de apresentação. Biometria multimodal Desafio/Resposta Dispositivo de captura de criptografia de hardware
Processamento de Sinal	Manipulação não autorizada de dados durante o processamento	Uso de algoritmo confiável
Comparação	Manipulação das pontuações de comparação	Servidor e/ou cliente seguro OCC confiável
Armazenamento	Banco de dados comprometido Substituição não autorizada de BR/IR Modificação não autorizada de BR/IR Exclusão não autorizada de BR/IR Ataque DDoS	Referências biométricas revogáveis e renováveis Separação dos Dados Controle de acesso ao banco de dados Sinal BR/RBR/IR Cifrar BR/RBR/IR Planejamento de contingência adequado e procedimentos de recuperação
Decisão	Ataque de escalada DDoS Manipulação de *Threshold*	Canal seguro Ocultar score de comparação Rede/Canal seguro Controle de acesso a configuração de *Threshold* Proteção do valor de *Threshold*

De acordo com que recomenda a [ISO/IEC 24745, 2022], a principal medida para

prevenir ataques é empregar um algoritmo confiável para cifrar os dados biométricos. Os recursos de modelos biométricos renováveis reforçam ainda mais a segurança. Além disso, existem outras contramedidas que podem ser adotadas:

- Detecção de Ataques de Apresentação: Uma contra medida para este ataque é a detecção dos sinais vitais, como pressão sanguínea e temperatura.
- Biometria Multimodal: envolve o uso de mais de um tipo de traço biométrico, como impressão digital e reconhecimento facial, para autenticar a identidade de um indivíduo. Isso aumenta a segurança e a confiabilidade do processo de autenticação.
- Desafio-resposta: é um método de autenticação que envolve o sistema emissor apresentando um desafio ao usuário, que deve responder corretamente para comprovar sua identidade. A resposta é geralmente baseada em um conhecimento prévio compartilhado entre o sistema e o usuário.
- Uso de algoritmo confiável: é fundamental para assegurar a segurança, pois esses algoritmos passam por testes rigorosos e suas vulnerabilidades são identificadas e abordadas. Isso contribui para uma proteção mais eficaz contra ameaças.
- Servidor e/ou cliente seguro: é essencial para proteger os dados e as comunicações. Isso envolve medidas como autenticação forte, criptografia e prevenção contra acessos não autorizados, garantindo a integridade e confidencialidade dos dados.
- Separação dos Dados: consiste em isolar informações em compartimentos diferentes para garantir a segurança. Isso ajuda a evitar vazamentos acidentais ou intencionais, minimizando o risco de que um acesso não autorizado a um conjunto de dados comprometa outros.
- Ocultar score de comparação: envolve não revelar a pontuação resultante da comparação biométrica para proteger a segurança e privacidade, dificultando ataques baseados na análise dessas pontuações.
- Controle de acesso a configuração de *threshold*: refere-se a gerenciar com rigor o acesso e ajuste do limiar de comparação utilizado em sistemas biométricos. O *threshold* determina a aceitação ou rejeição de uma correspondência biométrica com base na pontuação resultante da comparação de características.

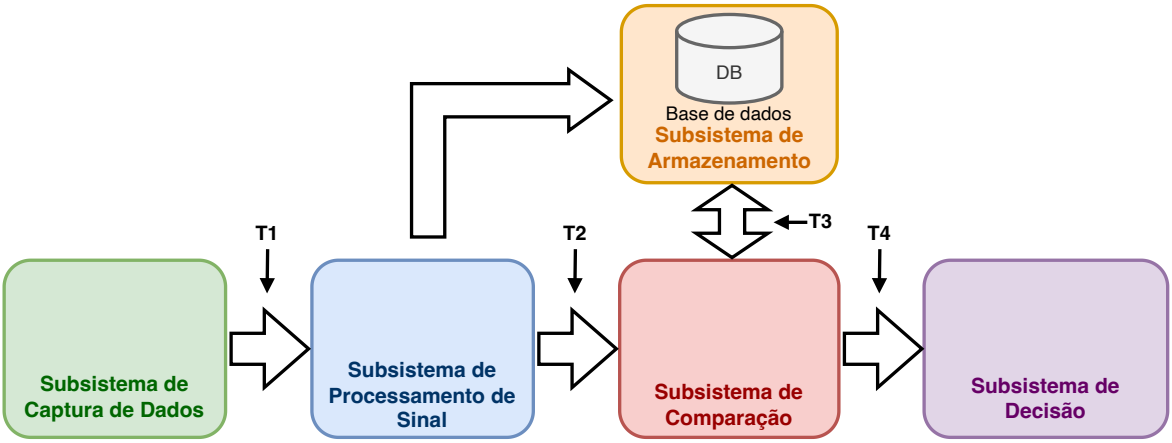
6.4.5. Ataques Durante a Transmissão

Nas fases que englobam a transferência de dados biométricos entre diferentes subsistemas, existe um considerável risco para a integridade desses dados, especialmente em sistemas distribuídos. Isso ocorre porque os dados são transferidos entre várias partes do sistema, as quais estão localizadas geograficamente em diferentes locais devido à natureza distribuída do sistema.

Como descreve [Faria, 2014], um sistema biométrico é constituído de uma infraestrutura composta de vários módulos de software e hardware interligados, envolvendo captura, extração de características, banco de dados de amostras, combinador e módulo de decisão, é entendível que possa haver brechas em pontos desta infraestrutura que comprometem a sua segurança. Estas brechas podem ser citadas como sabotagem e sobrecarga, na qual a sabotagem se refere a danos físicos cometidos contra os componentes da infraestrutura.

A Figura 6.12 exemplifica os principais pontos da Tabela 6.2 e indica os dados transmitidos, principais ameaças / contramedidas, bem como a transmissão dos dados entre os subsistemas.

Figura 6.12: Principais pontos e momentos de ataques ao subsistemas.



Diversos ataques podem ocorrer nos meios de transmissão entre os subsistemas. Seus principais alvos são identificados na Figura 6.12, sendo representadas pelos itens: T1 - Subsistema de Captura de Dados e Processamento de Sinal; T2 - Subsistemas de Processamento de Sinal e Comparação; T3 - Subsistema de Comparação e Armazenamento; e T4 - Subsistema de Comparação e o de Decisão. A Tabela 6.3 descreve os dados transmitidos, principais ameaças e contramedidas.

Tabela 6.3: Ameças e contramedidas entre os subsistemas.

Ameaças entre os subsistemas			
Canais de Comunicação	Dados	Ameaças	Contramedidas
Captura de Dados - Processamento de sinal (T1) Processamento de Sinal e Comparação (T2)	Amostra biométrica e traço	Espionagem *Replay* Força Bruta	Canal seguro/Cifrado. Desafio/Resposta. Política de tempo Limite.
Armazenamento - Comparação (T3)	Referência Biométrica	Espionagem *Replay* Pessoa no meio/MitM Escalada	Canal seguro/Cifrado. Desafio/Resposta. Canal seguro/Cifrado. Verificação de integridade dos dados biométricos com assinatura digital ou MAC. Canal seguro.
Comparação - Decisão (T4)	*Score* de comparação	Manipulação de pontuação de comparação	Canal seguro.

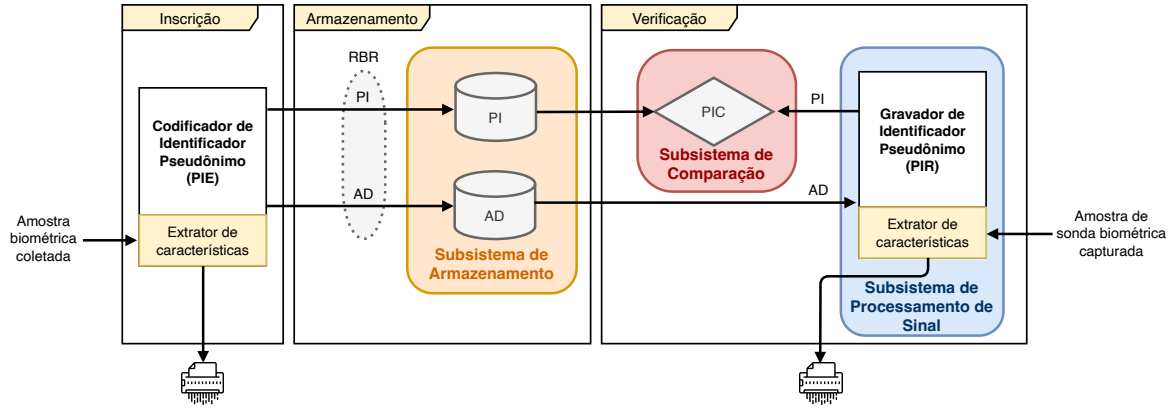
É inegável que todos os subsistemas possuem ameaças potenciais. No entanto, o essencial na segurança reside na capacidade de antecipar essas ameaças e concentrar

esforços na proteção dos pontos mais suscetíveis aos ataques. Deste modo, a Tabela 6.3 informa os canais de comunicação que podem apresentar riscos, bem como os dados que podem comprometidos, seguido das possíveis ameaças e contramedidas que podem ser tomadas para mitigá-las.

6.4.6. Tipos de referências biométricas renováveis e revogáveis

A biometria renovável ocorre com a aplicação dos conceitos de renovabilidade e revogabilidade nas referências biométricas, este conceito é chamado de referências biométricas renováveis (RBR). O processo de criação de RBRs envolve o processo de diversificação que geram múltiplas referências irreversíveis e não vinculáveis a partir das mesmas características biométricas que podem ser usadas para renovar um RBR ou fornecer referências independentes em diferentes aplicações. Seu uso é uma importante contramedida contra ataques que possam comprometer a identidade de um indivíduo no sistema. Essa prática pode ser vista na aplicação de técnicas como a biometria cancelável [ISO/IEC 24745, 2022]. A arquitetura para a criação de uma RBR é ilustrada na Figura 6.13.

Figura 6.13: Tipos de referências biométricas renováveis e revogáveis.



A biometria renovável ocorre basicamente com a aplicação dos conceitos de renovabilidade e revogabilidade nas referências biométricas. Sua utilização é uma importante contramedida a ataques que possam comprometer a identidade de um indivíduo dentro do sistema. As RBRs consistem em dois elementos de dados essenciais: um Identificador Pseudônimo (PI) e os Dados de Recursos Biométricos Correspondentes (AD). Ambos são gerados durante o processo de inscrição e são armazenados porque são necessários para realizar processos de verificação ou identificação biométrica. Caso seja necessária a renovação de uma RBR para um determinado indivíduo, um novo PI correspondente será gerado, acompanhado por um novo conjunto de AD e uma amostra biométrica recentemente capturada, usando o mesmo processo de criação de RBR. As novas informações de PI e AD são então entregues ao sujeito ou prestador de serviços responsável, enquanto as informações de PI e AD anteriores são revogadas e descartadas. Durante a inscrição, um estágio de extração de recursos biométricos é conduzido para gerar dados a partir da amostra biométrica coletada. Em seguida, um codificador de identificador pseudônimo (PIE) é empregado para criar a RBR, composta pelo PI e AD correspondentes [ISO/IEC 24745, 2022].

Uma vez que a RBR é criada, a amostra biométrica original e os dados de recursos

extraídos podem ser devidamente descartados, proporcionando maior segurança e privacidade. O RBR resultante é armazenado em um meio adequado de armazenamento, como um cartão inteligente ou um banco de dados eletrônico. Vale ressaltar que o PI e AD podem ser separados fisicamente ou logicamente, reforçando ainda mais a proteção dos dados biométricos e a confidencialidade do processo [ISO/IEC 24745, 2022].

De acordo com [Kaur and Khanna, 2016] um esquema biométrico cancelável deve cumprir quatro objetivos:

1. Diversidade: muitos modelos canceláveis podem ser gerados a partir da mesma biometria para aplicações diferentes.

2. Renovabilidade/ Revogabilidade: revogação direta e reemissão caso o modelo esteja comprometido.

3. Não inversibilidade: Para evitar a falsificação, não deve ser possível obter informações sobre recurso biométrico original do modelo transformado.

4. Desempenho: O reconhecimento realizado com o modelo transformado não deve prejudicar o desempenho do sistema. Este também deve possuir compatibilidade com versões anteriores.

6.4.7. Biometria Cancelável

A biometria cancelável visa garantir a segurança e a privacidade dos modelos biométricos. Essa técnica consiste em aplicar distorções intencionais e repetíveis nos sinais biométricos, com base em transformações específicas que possibilitam a comparação dos modelos biométricos no domínio transformado. Essa transformação torna os modelos biométricos permanentemente protegidos, tornando difícil ou impossível a recuperação dos dados biométricos brutos a partir dos modelos. Em vez de armazenar os dados biométricos originais, a biometria cancelável mantém os dados do modelo transformado, garantindo assim a confidencialidade dos usuários. A obtenção dos modelos transformados é realizada através da aplicação de uma função de transformação não reversível especialmente projetada para esse propósito.

Essa transformação pode ser aplicada tanto no domínio original quanto no domínio do recurso biométrico. Um dos principais benefícios é a sua capacidade de fornecer revogabilidade. Isso significa que, caso a biometria de um indivíduo seja comprometida, esta pode ser facilmente recriada utilizando uma nova transformação. Dessa forma, a segurança do sistema é mantida mesmo em casos de comprometimento. Outro benefício importante é a preservação da privacidade. A transformação torna computacionalmente difícil recuperar a biometria original a partir dos dados transformados, garantindo a confidencialidade dos dados biométricos dos usuários [ISO/IEC 24745, 2022] [Gomez-Barrero et al., 2016].

Essa abordagem proporciona uma camada adicional de segurança, pois mesmo que os modelos biométricos sejam comprometidos, não será possível reconstruir as informações biométricas originais, protegendo assim a identidade dos usuários e preservando sua privacidade [Yang et al., 2022].

Deste modo, a biometria cancelável evita problemas de correspondência cruzada entre diferentes bancos de dados. Cada aplicativo utiliza uma transformação diferente, impedindo a comparação direta entre as informações armazenadas em diferentes sistemas. Além disso, essa abordagem não degrada a precisão dos algoritmos de correspondência. As características estatísticas dos recursos biométricos são aproximadamente mantidas após a transformação, o que possibilita o uso de algoritmos de correspondência existentes. Comparada à criptografia biométrica, na qual uma chave criptográfica é combinada com o modelo biométrico, a biometria cancelável oferece uma camada adicional de segurança. Enquanto a criptografia biométrica depende totalmente do sigilo da chave secreta, a biometria cancelável garante a desvinculação e a capacidade de revogar ou renovar os modelos transformados [Kaur and Khanna, 2016] [Patel et al., 2015b].

6.4.8. Segurança dos registros de dados biométricos

Os sistemas biométricos precisam armazenar dois tipos de referências: referências biométricas ou biométricas renováveis [ISO/IEC 24745, 2022] (BR ou RBR, geradas pelos sistemas de captura de biometria) e referências de identidade (IR, nomes de usuários, números únicos ou qualquer dado que identifique unicamente um indivíduo dentro do sistema). Com estas identidades, o sistema pode associar uma ou mais biometria (BR) a um indivíduo. Além disso, pode-se armazenar estas referências (IR e BR) na mesma base de dados ou em base de dados separadas.

6.4.8.1. Base de dados única

A forma como as referências BR e IR são armazenadas permite determinar quais requisitos de segurança o sistema atende. É possível armazenar uma referência de quatro maneiras:

- Inalterada: não oferece nenhum tipo de segurança, nem integridade, nem confidencialidade são satisfeitos.
- Cifrada: pode-se cifrar uma única referência (BR ou IR) ou ambas. Desta forma, a referência cifrada satisfaz confidencialidade e, dependendo da cifra utilizada, integridade fraca.
- Autenticada: autenticando uma ou ambas as referências, é garantido que o sistema satisfaz o requisito de integridade para a referência autenticada.
- Autenticada-cifrada: autenticando e cifrando alguma das referências, garante a integridade e confidencialidade para a referência em questão.

É possível também empregar esses métodos de armazenamento em RBR, fazendo isso, são satisfeitos tanto os requisitos supralistados quanto o requisito de *renewability/-revocability*. Com estas possibilidades, são possíveis dezenove tipos de cenários, que atendem total ou parcialmente os requisitos de segurança descritos (Subseção 6.4.1). A Tabela 6.4 delinea os cenários possíveis para proteção das BRs ou IRs. Cada um destes cenários garante diferentes requisitos de segurança para determinadas referências.

Tabela 6.4: Possíveis cenários de proteção das identidades e os requisitos de segurança satisfeitos.

Cenário	Confidencialidade		Integridade		*Renewability*	Irreversibilidade	Confidencialidade	Armazenamento da IR	Armazenamento da BR
	IR	BR	IR	BR					
1								IR	nda
2		X		0		0		IR	enc
3				X				IR	aut
4		X		X		0		IR	aut-enc
5	X		0					enc IR	nda
6			X					aut IR	nda BR
7	X		X					aut-enc IR	nda BR
8	X	X	0	0		0	0	enc IR	enc BR
9			X	X				aut IR	aut BR
10	X	X	X	X		0	0	aut-enc IR	aut-enc BR
11	X	X	0	X		0	0	enc IR	aut-enc BR
12		X	X	X		0		aut IR	aut-enc BR
13	X	X	X	0		0	0	aut-enc IR	enc BR
14	X		X	X				aut-enc IR	aut BR
15					X	X		IR	RBR
16		0	X	X	X	X		aut IR	aut div. RBR
17	X	X	X	X	X	X	0	aut-enc IR	aut-enc div. RBR
18	X	X	0	0	X	X	0	enc IR	enc RBR
19		X	X	X	X	X		aut IR	aut-enc, div. RBR

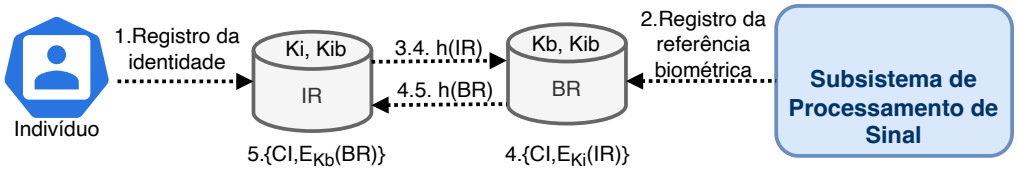
enc - cifrado
aut - autenticado
aut-enc - autenticado e cifrado
X - satisfeito
0 - parcialmente satisfeito

6.4.8.2. Caso de bases de dados separadas

Utilizar bases de dados separadas para o armazenamento da BR e IR é, em geral, considerado uma boa prática de segurança [ISO/IEC 24745, 2022]. Separando estes dados, o vazamento dos dados de um servidor não necessariamente compromete a identidade e acesso à conta de um usuário. No entanto, para que esta separação seja o mais efetiva possível, é ideal que a separação seja tanto física (servidores diferentes em localizações diferentes) e de operadores (as bases devem ser administradas por operadores diferentes com chaves criptográficas diferentes para qualquer proteção que esteja sendo utilizada). Com isto, para se utilizar bases separadas para o armazenamento das referências, surgem alguns problemas relacionados à segurança da comunicação entre estas bases. É preciso definir como conectar a BR e IR (ou PI e AD em caso de uma RBR) para autenticação, e também, como fazer isso de forma segura. Em geral, esta funcionalidade é provida por um *identificador comum* (CI).

O CI deve ser formado a partir das duas (ou mais) referências sendo conectadas para que todas as bases sejam capazes de identificar e autenticar o usuário. Uma forma de implementar um CI é utilizando algum tipo de MAC formado por ambas as referências para formar um único identificador CI. Um diagrama de uma implementação similar ([ISO/IEC 24745, 2022]) é apresentado na Figura 6.14.

Figura 6.14: Exemplo de possível implementação de esquema de proteção utilizando bases de dados separadas para IR e BR.



O diagrama na Figura 6.14 mostra o fluxo das referências entre bases, especificamente para o registro de uma BR. Este tráfego garante que tanto a base com IR quanto com a BR tenham o CI e possam autenticar o usuário caso necessário. De forma similar ao uso de somente uma base de dados, a forma de armazenamento do das referências determinam quais requisitos de segurança serão satisfeitos pelo sistema. A Tabela 6.5[1] A seguir, assim como na Tabela 6.4.

Tabela 6.5: Possíveis cenários de proteção das identidades e os requisitos de segurança satisfeitos por cada um em um cenário de armazenamento das referências em diferentes bases de dados. Fonte: Adaptado de [ISO/IEC 24745, 2022].

Cenário	Confidencialidade		Integridade		*Renewability BR*	Irreversibilidade	Confidencialidade	Armazenamento da IR	Armazenamento da BR
	IR	BR	IR	BR					
1								IR	nda
2		X		0		0		IR	enc
3				X				IR	aut
4		X		X		0		IR	aut-enc
5	X		0					enc IR	nda
6			X					aut IR	nda BR
7	X		X					aut-enc IR	nda BR
8	X	X	0	0		0	0	enc IR	enc BR
9			X	X				aut IR	aut BR
10	X	X	X	X		0	0	aut-enc IR	aut-enc BR
11	X	X	0	X		0	0	enc IR	aut-enc BR
12		X	X	X		0		aut IR	aut-enc BR
13	X	X	X	0		0	0	aut-enc IR	enc BR
14	X		X	X				aut-enc IR	aut BR
15		0			X	X		IR, PI	AD
16		0	X	X	X	X		aut IR, aut PI	aut AD
17	X	X	X	X	X	X	0	aut-enc IR, aut-enc PI	aut-enc AD
18	X	X	0	0	X	X	0	enc IR, enc PI	enc AD
19	X	X	X	X	X	X		aut IR, aut-enc PI	aut-enc AD

enc - cifrado
aut - autenticado
aut-enc - autenticado e cifrado
X - satisfeito
0 - parcialmente satisfeito

6.4.9. Mecanismos para proteção dos dados biométricos

Nesta seção são apresentados os principais mecanismos que buscam efetuar a proteção dos dados biométricos. Estes mecanismos apresentam diversas abordagens que buscam esta proteção, as duas principais técnicas são os criptossistemas biométricos e a biometria cancelável.

6.4.9.1. Criptossistemas biométricos

Uma das principais maneiras de proteger *templates* biométricos é com técnicas denominadas Criptossistemas Biométricos [Rathgeb and Uhl, 2011]. Estes sistemas funcionam de forma similar a sistemas de criptografia tradicionais, mas precisam acomodar algumas características específicas a dados biométricos, e.g., a imprecisão que a leitura de dados biométricos apresenta, pela própria natureza não-fixa dos dados.

Fuzzy Commitment Esta técnica se baseia na ideia de *"fuzzy logic"* [Zadeh, 1965]. Em oposição a sistemas de criptografia comuns, que requerem uma chave precisa para de-

[1] Em todos os casos, o CI é armazenado em ambas as bases, juntamente com o IR (ou PI) e BR (ou AD).

cifrar os dados cifrados, os sistemas "*fuzzy*"aceitam chaves suficientemente similares à original [Juels and Wattenberg, 1999]. Por exemplo, cifrando algum dado D com a chave "SBSEG", em um sistema tradicional só se consegue decifrar este dado com a chave exata. Porém, um sistema criptográfico *fuzzy* teórico pode aceitar até uma letra errada, como na chave "SBSIG". Esta tolerância, em primeira análise, parece introduzir uma falha de segurança. Contudo, como sistemas biométricos sempre apresentam ruído na leitura da biometria, a tolerância do *fuzzy commitment* permite consistentemente identificar um usuário, mesmo que o leitor não apresente a biometria idêntica à apresentada no cadastro. Para se obter este comportamento, [Juels and Wattenberg, 1999] utilizam códigos de correção de erros (ECC). Ao salvar uma BR na fase de cadastro, é criado também uma chave K que será combinada com BR (com, por exemplo, uma função de *hash*) criando *helper data* (HD)). Com HD, ao tentar se autenticar, tem-se uma BR' "corrompida" pelo ruído introduzido na coleta. Agora, usando um ECC, é tentado recuperar a chave K original utilizando HD e BR'. Se o ruído não for superior à capacidade de correção do ECC, será obtida a chave original K e autenticando o usuário com esta. Caso fosse apresentado uma biometria completamente diferente ou extremamente distorcida, não se tem a chave exata K ao final. Dessa forma, é recusada a autenticação do usuário.

Fuzzy Vault Com o *Fuzzy Vault* [Juels and Sudan, 2006], se pretende obter a mesma "*fuzzynes*"que o *fuzzy commitment*. Para isso, é criado a ideia de um *vault* ou "cofre"que armazena as minúcias da biometria armazenada. É construído o cofre primeiro, projetando as minúcias coletadas em um polinômio escolhido aleatoriamente a adicionando pontos "falsos"ao cofre para que as minúcias não possam ser recuperadas, somente com acesso ao cofre. Com estes dados armazenados, ao realizar autenticação, é disposto um conjunto de minúcias que, caso se sobreponham o suficiente com as minúcias cadastradas, serão o suficiente para reconstruir o polinômio original e confirmar a identidade do usuário. Biometrias não compatíveis ou muito corrompidas não se sobrepõe o suficiente às minúcias originais, e geram um polinômio diferente do cadastrado.

Bio Hashing Esta técnica consiste em aplicar diversas transformações à BR ([Jin et al., 2004] usa transformadas em ondaletas e Fourier-Mill juntamente com outros tratamentos) para gerar um vetor de recursos. Pode-se então combinar este vetor com um número aleatório para gerar o *hash* biométrico. Na autenticação, pode-se aplicar o *hash* na biometria proposta e compará-lo com o *hash* da biometria original cadastrada, permitindo ou não a autenticação. O benefício de utilizar o *bio-hash* em oposição à biometria original, é a segurança que se ganha caso o *hash* seja vazado. Sem o número aleatório usado no cadastro, é praticamente impossível obter a BR original a partir do *hash*, mantendo a identidade do usuário em caso de vazamento.

Criptografia homomórfica Pode-se dizer que um algoritmo criptográfico é homomórfico se um ou mais tipo de operações, ao serem aplicados nos dados cifrados, são também aplicados nos dados originais [Armknecht et al., 2015]. Isso permite trabalhar com os dados cifrados, mantendo privacidade, sem ter a necessidade de decifrar os dados para realizar cálculos com eles. Com esta capacidade, em sistemas biométricos, é possível

trabalhar com uma BR cifrada, e calcular métricas de similaridade entre *templates* (como similaridade de cossenos [Gomez-Barrero et al., 2017]). Assim, atua-se somente no domínio dos dados cifrados, minimiza-se a necessidade de armazenar os *templates* as claras.

6.4.9.2. Técnicas de biometria cancelável

As técnicas de Biometria Cancelável, assim como Criptosistemas Biométricos, tem o propósito de proteger os *templates* e referências biométricas. Porém, este tipo de técnica, tenta mitigar principalmente o perigo de um vazamento do dado biométrico. As Características biométricas são, em geral, permanentes para um indivíduo. Por isso, caso uma BR desprotegida seja vazada, a biometria dos usuários afetados pode ser considerada comprometida para o resto de sua vida [Ratha et al., 2001b]. Para características como digitais, pode-se simplesmente utilizar outros dedos, mas, por exemplo, rostos não podem serem facilmente alterados. Essa situação acontece em contraste a sistemas de autenticação baseados em senhas (*keywords*), que podem, a qualquer momento, serem revogadas e alteradas caso sejam comprometidas. Por isso, é necessário este tipo de revogabilidade ou "cancelabilidade"para os *templates*. Assim, caso as BRs sejam comprometidas, é possível, do mesmo modo que as senhas, simplesmente revogá-las, e o usuário continua utilizando a mesma biometria sem medo de o *template* vazado ser utilizado por terceiros.

Bio Convolving Para se utilizar esta técnica, é preciso que a BRs possa ser representada por um conjunto de sequências [Maiorana et al., 2010, Patel et al., 2015a]. Para transformar a biometria original, esta é dividida em n sequências de tamanho d, sendo d é o um número aleatório chamado de chave. Com estas n sequências, se obtém o *template* transformado e realizando a convolução entre cada uma das sequências. Este *template* ainda representa a biometria, entretanto é possível gerar vários *templates* diferentes alterando somente d. Desta forma, então tem-se a possibilidade de revogar um *template* comprometido e criar um novo a partir da biometria original.

Random projections Este método [Khan et al., 2015] consiste em projetar a BR em um "espaço aleatório". Neste espaço, cada valor é escolhido aleatoriamente e, ainda mais, deve preservar a distância entre dois pontos no *template* original. Caso o segundo requisito não seja satisfeito, a projeção não poderá ser utilizada como uma "*proxy*"da biometria original.

Transformações não inversíveis As transformações deste tipo [Pabitha and Latha, 2013] [Rathgeb and Uhl, 2011] são um dos métodos mais simples para criação de *templates* biométricos canceláveis. O objetivo desta técnica é aplicar uma ou mais transformações não inversíveis na BR original, no ato do cadastro. Como a transformação é não inversível, um atacante, ou até mesmo o agente armazenando a BR transformada, não consegue obter a biometria original com base no *template* transformado. Para realizar autenticação, basta aplicar as mesmas transformações à BR sendo testada e compará-la com o *template* transformado original. Dessa forma, no caso de um vazamento de dados, o *template* transformado pode ser revogado sem dano ao usuário. Para criar uma nova BR, basta realizar

a transformação novamente utilizando outras transformações ou parâmetros diferentes da primeira transformação.

Filtros Bloom Um Filtro Bloom [Bloom, 1970] é uma estrutura de dados que pretende armazenar a possível existência ou não de um elemento nesta estrutura. Em outras palavras, dado um elemento *n*, deseja-se saber se este está presente na base de dados. O Filtro Bloom pode dizer que *n* possivelmente está na base ou que não há possibilidade de *n* estar na base. Durante este processo, a base nunca guarda *n* em si, mas simplesmente se *n* está, ou não, cadastrado na base. Em geral, Filtros Bloom funcionam utilizando várias funções de *hash* diferentes [Rathgeb et al., 2014]. Ao cadastrar uma BR na base, é calculado todos os *hashes* da BR. O resultado deste cálculo resulta em uma série de posições em um *bit-array* que serão definidos como 1. Na autenticação, é feito o mesmo processo para a BR sob teste. Se nenhuma das posições no *array* é 1, sabe-se com certeza que a BR testada não está cadastrada na base. Caso um ou mais bit seja 1, sabe-se somente que "é possível"que a BR tenha sido cadastrada, mas não se pode ter certeza. Para minimizar esta incerteza, utiliza-se um número maior de funções de *hash* para evitar que uma BR não cadastrada tenha bits selecionados.

6.5. Modelos de aplicação e segurança de sistemas biométricos

Ao projetar um sistema biométrico deve-se analisar as condições e o meio em que o sistema será implementado, nesse sentido, existem diferentes tipos de modelos que servem para as mais diversas aplicações de segurança. Nessa seção serão discutidos os diferentes tipos de modelos de sistemas biométricos e suas aplicações tendo como base a norma [ISO/IEC 24745, 2022].

6.5.1. Modelos de aplicação de sistemas biométricos

De acordo com a norma [ISO/IEC 24745, 2022], de forma geral, um sistema biométrico pode ser classificado considerando o local no qual as BR e as IR são armazenadas e comparadas. No que diz a respeito de segurança, cada modelo possui seus benefícios e problemas em termos de transmissão, processamento de dados e armazenamento. Conceitualmente, vários diferentes tipos de modelos são possíveis, mas neste minicurso são abordados apenas aqueles com aplicações reais que são discutidas na norma [ISO/IEC 24745, 2022]. Assim, onze diferentes tipos de modelos que vão de A a K como expostos na Tabela 6.6.

Tabela 6.6: Modelos de aplicação de sistemas biométricos.

		Armazenamento			
		Servidor	Cliente	*Token*	Distribuída
Comparação	Servidor	A		B	G
	Cliente	C	D	E	H
	Token			F	
	Distribuída	I		J	K

As plataformas em que os dados podem ser armazenados e comparados são:

- Servidor: É basicamente um computador conectado remotamente ao cliente por meio de uma rede.
- Cliente: A característica principal de um cliente é a de garantir os serviços de *front-end* a um sistema biométrico, além de ser responsável de se comunicar com o servidor e com o *token*. Logo, o cliente é a plataforma que faz a comunicação do usuário com o servidor e com o *token*. Nesse sentido, o cliente pode ser os computadores pessoais, celulares e seus equivalentes. Observa-se que muitas vezes os sensores biométricos são conectados ou integrados ao cliente.
- *Token*: *Token* nada mais é do que um dispositivo portátil capaz de armazenar as BR e em alguns casos é capaz de executar comparações. Dessa forma, *tokens* podem ser USB *memory sticks*, *e-passaports* e *smart cards* entre outros.
- Distribuída: Em relação ao armazenamento, o termo faz referência ao armazenamento das BR e RBR serem em pelo menos duas entidades (*token*, servidor, e cliente) e as referências biométricas não estão disponíveis com apenas uma das entidades. No que diz a respeito da comparação, para obter o resultado da verificação a execução da comparação deve envolver pelo menos duas entidades (*token*, servidor, e cliente).

Os diversos modelos expostos de A a K descrevem diferentes topologias de localização para os diversos subsistemas. Nesse sentido, os modelos de A a F, podem ser usados tanto referências biométricas normais quanto RBR, o que irá determinar o tipo de BR serão as características de segurança e privacidade desejadas para o projeto. Em contrapartida, os modelos G e H são aplicados apenas para RBRs. Os modelos I, J, K além de serem possíveis projetos com BR ou RBR estes descrevem o caso em que a comparação é distribuída em vários locais o que evita que a informação seja coletada em apenas um local para ser comparada. A norma [ISO/IEC 24745, 2022] recomenda que ao projetar um sistema biométrico deve-se preferencialmente seguir algum dos modelos descritos na Subseção 6.5.1 ou uma combinação desses. Isso, levando em consideração sua aplicação bem como as características de privacidade e de segurança de cada um dos modelos. Além disso, a norma [ISO/IEC 24745, 2022] ressalta que ao projetar um sistema biométrico ou implementar qualquer um dos modelos descritos, seu desempenho, privacidade, segurança devem ser avaliados seguindo a norma [ISO/IEC 30136, 2018], norma especializada em avaliar a precisão, sigilo e privacidade dos *templates* biométricos e sistemas de proteção.

6.5.2. Segurança de modelos de aplicação biométrica

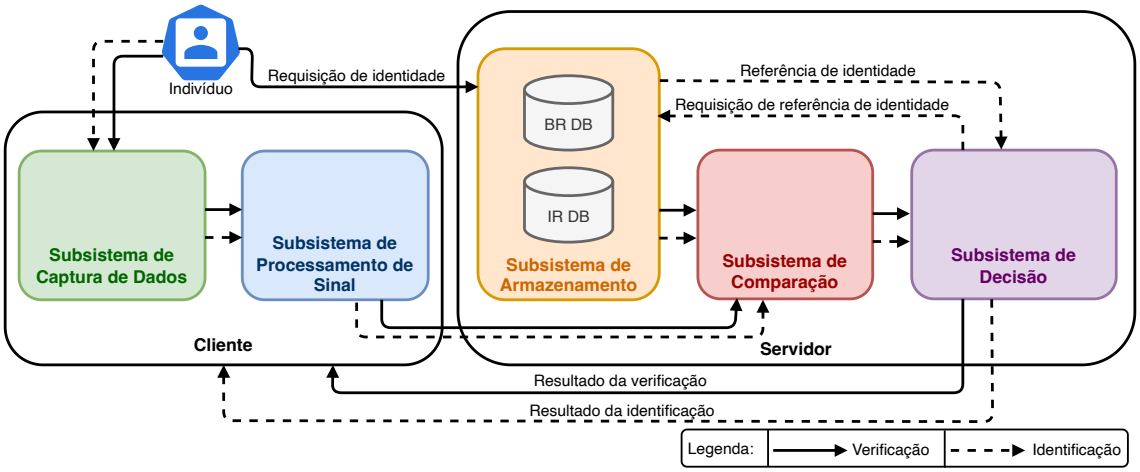
Nessa seção, são abordados cada um dos modelos, destacando suas características e aplicações.

6.5.2.1. Modelo A - comparado no servidor e armazenado no servidor.

No Modelo A, o processo de inscrição dos dados biométricos, as BRs e as respectivas IRs são associadas e armazenadas no servidor. Assim, na identificação, os dados biométricos são capturados e processados no cliente e então as BRs extraídas são transmitidas para o

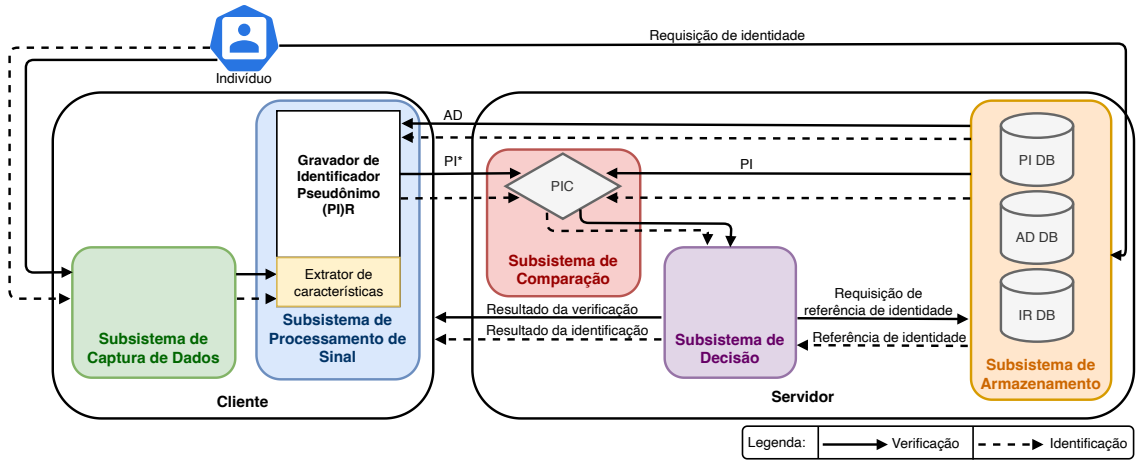
servidor no qual ocorre comparação com as BRs armazenadas no banco de dados e assim a decisão é tomada pelo servidor, como identificado no fluxograma pela linha tracejada – Figura 6.15.

Figura 6.15: Modelo A - Armazenado no servidor e comparado no servidor usando BRs.



No caso do processo de verificação, além da BR, é enviado ao servidor uma requisição de identidade. Assim, a BR presente no banco de dados que está associada a IR reivindicada é comparada com a BR enviada para o servidor e então a decisão é tomada pelo servidor como ilustrado no fluxograma pela linha contínua na Figura 6.15. A Figura 6.16 ilustra os processos de identificação e verificação do Modelo A para o uso de RBR.

Figura 6.16: Modelo A - Armazenado no servidor e comparado no servidor usando RBRs.

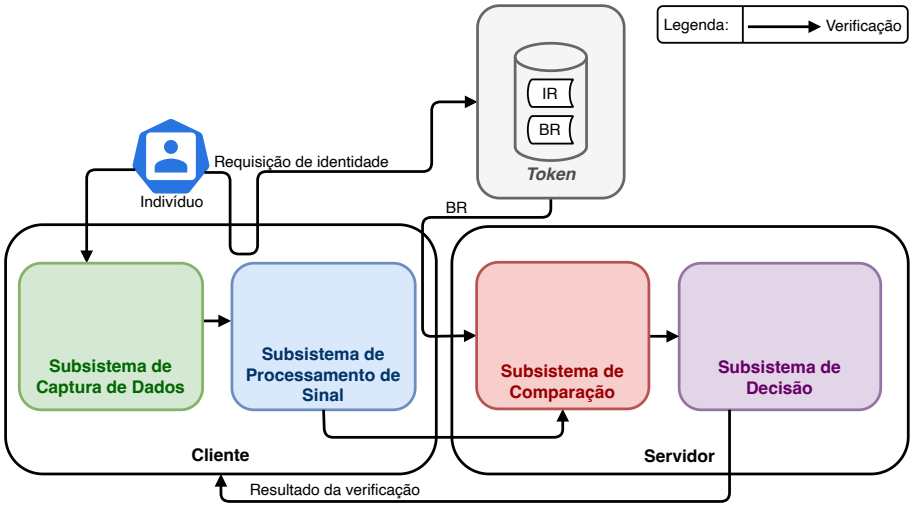


De um ponto de vista de privacidade, nesse tipo de modelo é recomendado o uso de referências biométricas renováveis RBR. Nesse tipo modelo, na inscrição são armazenados os Identificador Pseudônimo (PI) ao invés das BRs. As PIs armazenadas no servidor são associadas às IRs e aos dados auxiliares (AD), que são dados que fazem parte das RBRs e podem ser necessários para reconstruir as PIs. O processo de identificação e verificação é semelhante ao descrito anteriormente para o caso do uso de BR, mas ao invés das BRs serem transmitidas e comparadas, são utilizadas as PIs. As PIs dos dados biométricos extraídos, representados por PI* no fluxograma da Figura 6.16, são geradas no cliente pelo processo de Gravador de Identificador Pseudônimo (*Pseudonymous identifier recorder* - PIR) que utiliza os AD enviadas pelo servidor e os dados biométricos extraídos por meio de sensores para construir as PIs que serão enviadas ao servidor para a comparação. Tanto o processo de verificação quanto o de identificação para RBR podem ser observados no fluxogramas da Figura 6.16 e ocorrem de forma análoga ao caso BR.

6.5.2.2. Modelo B - Comparado no servidor e armazenado no *token*.

A Figura 6.17 ilustra o processo verificação do Modelo B para o uso de BR. Nesse modelo, no processo de inscrição dos dados biométricos, as BRs e as respectivas IRs são associadas e armazenadas em um *token*. Assim, na verificação, os dados biométricos são capturados e processados no cliente e as BRs extraídas são enviadas para o servidor, ocorrendo a comparação com os dados presentes no *token* e assim a decisão.

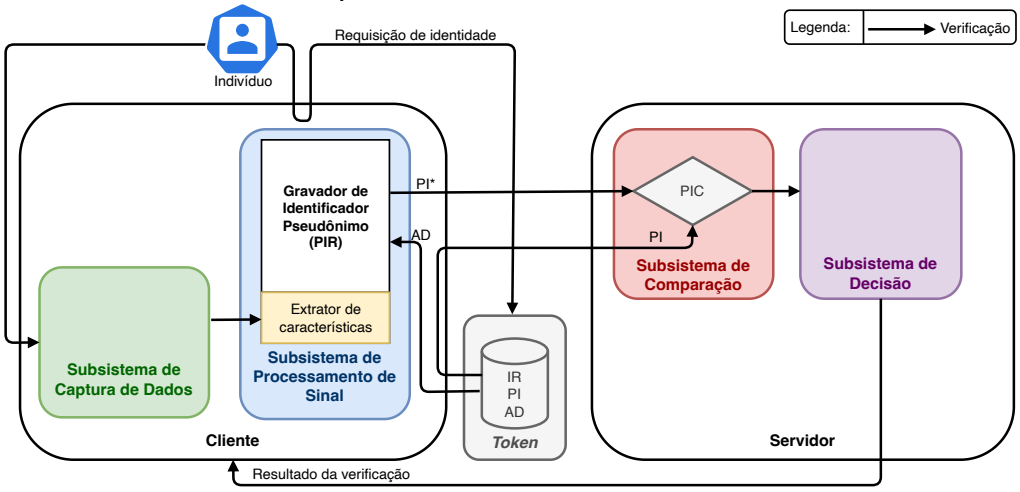
Figura 6.17: Modelo B - Comparado no servidor e armazenado no *token* usando BRs.



Na Figura 6.17, caso um usuário queira verificar sua identidade deve conectar fisicamente um *token* no cliente e enviar seus dados biométricos coletados por meio de um sensor. Dessa forma, o cliente reivindica a identidade do usuário ao *token* e envia tanto as BRs extraídas quanto as BRs do *token* para o servidor no qual ocorre a comparação e então a decisão é tomada pelo próprio servidor. Esse modelo geralmente é usado apenas para verificação, pois não há nenhum dado biométrico no servidor para comparação a não ser aquele que o usuário envia por meio do *token*. Observa-se que como esse modelo faz uso de um *token* portátil não necessita de medidas de segurança no banco de dados uma vez que o *token* está seguro com o usuário. Por outro lado, necessita de segurança na

rede para que os dados enviados para o servidor tanto do *token* quanto do cliente sejam seguros. A Figura 6.18 ilustra o processo de verificação do modelo B para o uso de RBR.

Figura 6.18: Modelo B - Comparado no servidor e armazenado no *token* usando RBRs.

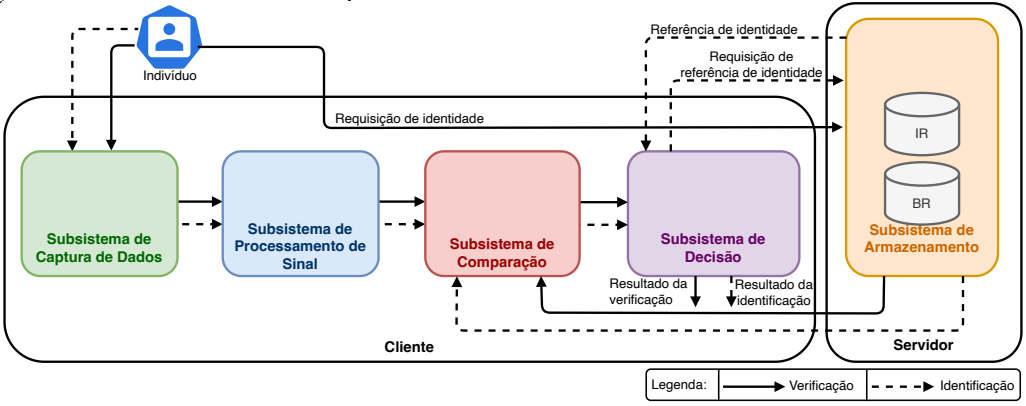


Já no caso com RBR, na inscrição dos dados, são armazenados os PIs, IRs e os ADs no *token* ao invés das BRs e IRs. Ademais, no processo de verificação, a PI que será transmitida ao servidor, representados por PI* no fluxograma da Figura 6.18, é gerada pelo processo de gravador de identificador pseudônimo (PIR) que utilizada os AD do *token* e os dados biométricos extraído por meio de sensores para construir a PI que serão enviadas para o servidor juntamente com a PI presente no *token* e assim ocorre a comparação e a decisão de forma semelhante ao caso com BR.

6.5.2.3. Modelo C - Comparado no cliente e armazenado no servidor.

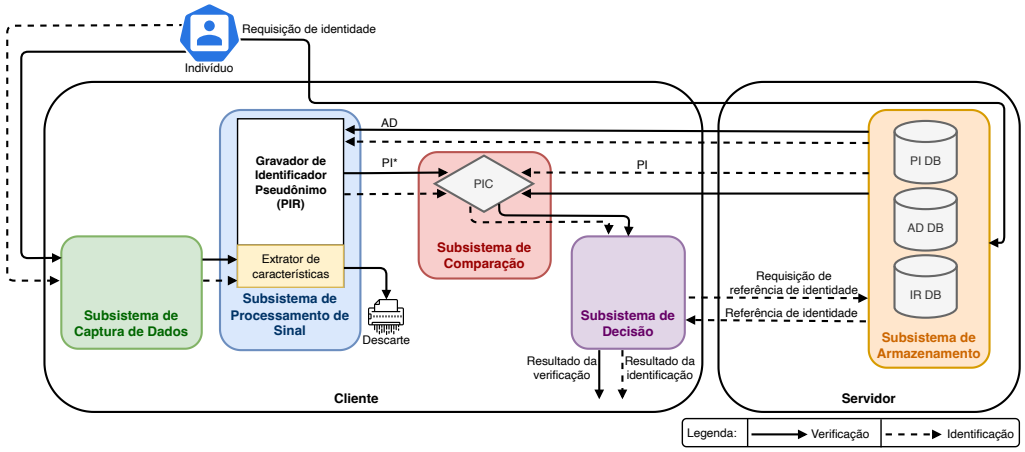
No Modelo C, no processo de inscrição dos dados biométricos, as BRs e as respectivas IRs são associadas e armazenadas no servidor. Assim, no processo de identificação, os dados biométricos são coletados e processados no cliente e as BRs extraídas, no lado do cliente, são comparadas com as BRs armazenadas no banco de dados do servidor que são enviadas ao cliente, e assim, a decisão é tomada pelo próprio cliente, como mostra o fluxograma de linha tracejada da Figura 6.19.

Figura 6.19: Modelo C - Comparado no cliente e armazenado no servidor usando BRs.



Já no processo de verificação, é enviada ao servidor uma requisição de identidade. Assim, a BR presente no banco de dados do servidor que está associada a IR reivindicada é enviada ao cliente e comparada com a BR extraída e então a decisão é tomada pelo servidor como ilustrado pelo fluxograma de linha contínua da Figura 6.19. Observa-se que o cliente deve haver um sensor e um algoritmo de decisão embutido. A Figura˜6.20 ilustra os processos de identificação e verificação do Modelo C para o uso de RBR.

Figura 6.20: Modelo C - Comparado no cliente e armazenado no servidor usando RBRs.

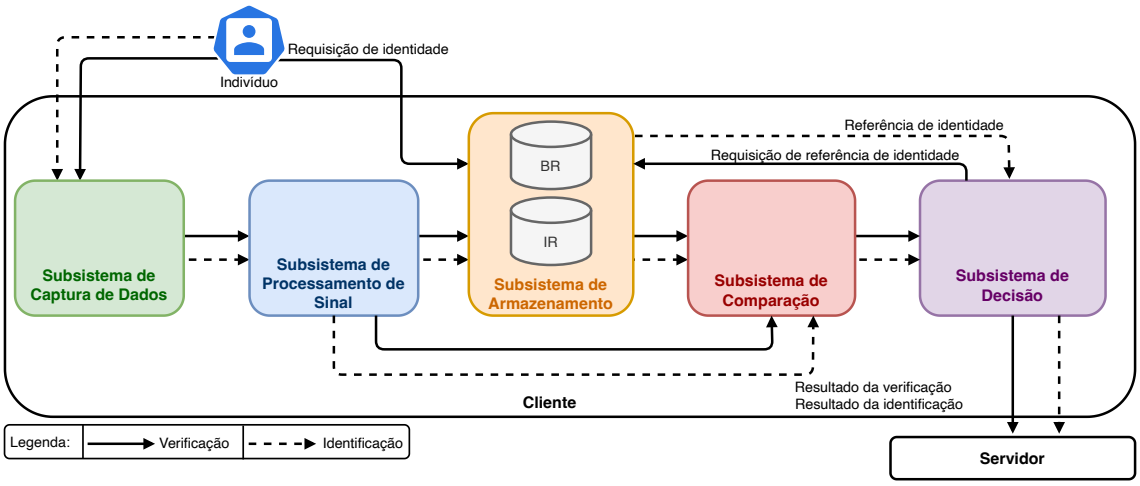


Para o uso de RBR, na inscrição são armazenadas as PI ao invés das BRs. As PI armazenadas no servidor são associadas às IR e aos AD. O processo de identificação e verificação é semelhante ao descrito anteriormente para o caso do uso de BR, mas ao invés das BRs serem transmitidas e comparadas, são utilizadas as PIs. As PIs dos dados biométricos extraídos, representados por PI* no fluxograma da Figura 6.20, são geradas no cliente pelo processo de PIR que utiliza os AD enviadas pelo servidor e os dados biométricos extraídos por meio de sensores para construir as PIs (PI*) que serão comparadas no cliente com a PIs enviadas pelo servidor. Tanto o processo de verificação quanto o de identificação para RBR podem ser observados nos fluxogramas da Figura 6.20 e ocorrem de forma análoga ao caso BR.

6.5.2.4. Modelo D - Comparado no cliente e armazenado no cliente.

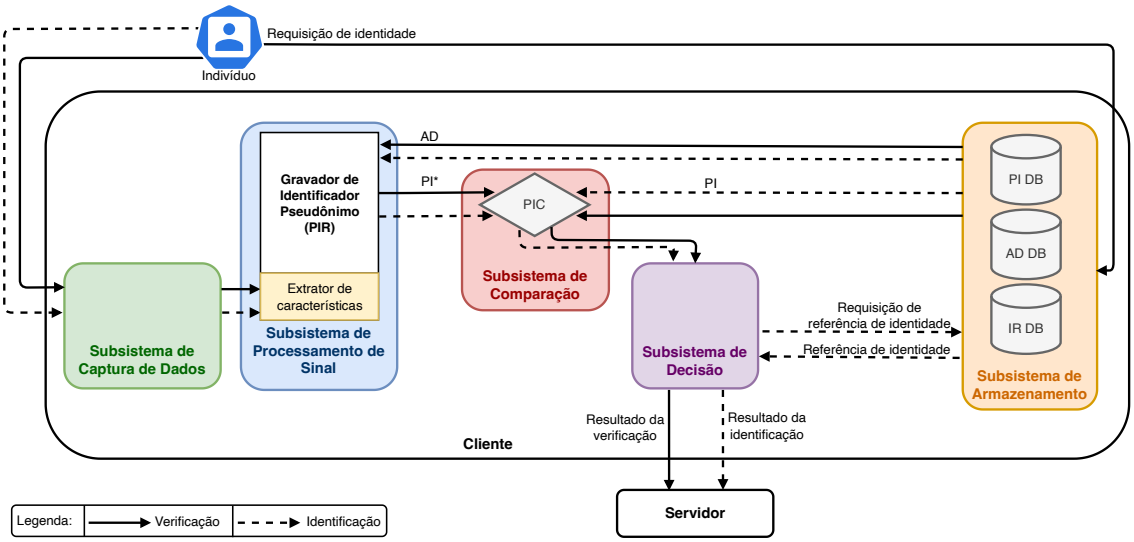
No Modelo D, no processo de inscrição dos dados biométricos, as BRs e as respectivas IRs são associadas e armazenadas no cliente. Assim, na identificação, os dados biométricos são coletados e processados no cliente e as BRs são extraídas. Essa BR extraída é comparada com a BRs presentes no banco de dados do próprio cliente e a decisão é tomada por um algoritmo de decisão presente no mesmo, como ilustrado no fluxograma pela linha tracejada (Figura 6.21).

Figura 6.21: Modelo D - Comparado no cliente e armazenado no cliente usando BRs.



No processo de verificação, é enviada ao cliente uma requisição de identidade. Assim, a BR presente no banco de dados do cliente que está associada a IR reivindicada é comparada com a BR extraída e então a decisão é tomada pelo próprio cliente como exposto pelo fluxograma de linha contínua (Figura 6.21). Nesse sentido, assim como no Modelo C, o cliente deve conter um sensor e um algoritmo de decisão embutido. Esse tipo de modelo é amplamente utilizado para autenticação, principalmente para *laptops*, telefones celulares e fechaduras eletrônicas, pois esse modelo não exige conexão com a rede. Ressalta-se que em alguns casos a autenticação final pode ser feita por um servidor que confirma a verificação feita pelo cliente. A Figura 6.22 ilustra os processos de identificação e verificação do Modelo D para o uso de RBR.

Figura 6.22: Modelo D - Comparado no cliente e armazenado no cliente usando RBRs.

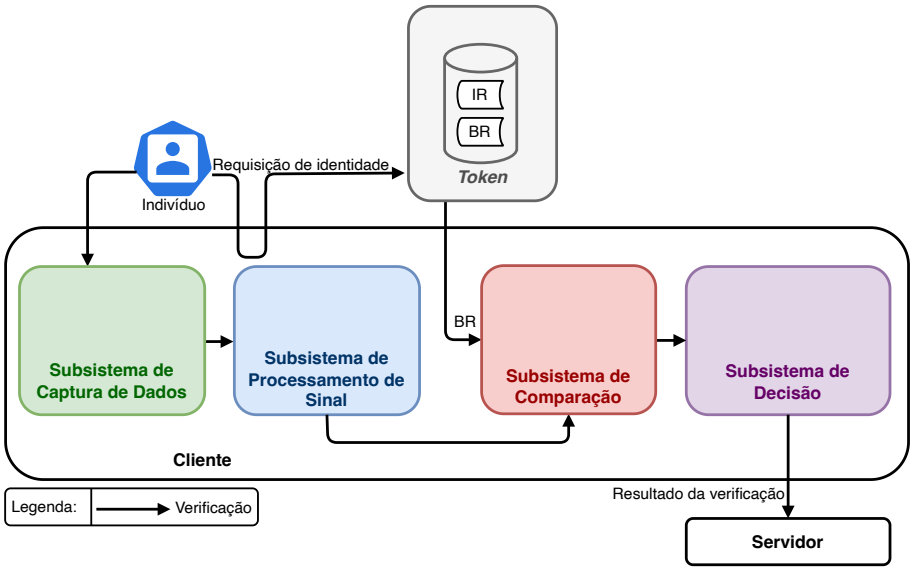


Assim, para o uso de RBR, na inscrição são armazenadas as PI ao invés das BRs. As PIs armazenadas no cliente são associadas às IRs e aos ADs. O processo de identificação e verificação é semelhante ao descrito anteriormente para o caso do uso de BR, mas ao invés das BRs serem comparadas, são utilizadas as PIs. As PIs dos dados biométricos extraídos, representados por PI* no fluxograma da Figura 6.22, são geradas no cliente pelo PIR que utiliza os AD enviadas pelo banco de dados do cliente e os dados biométricos extraídos por meio de sensores para construir as PIs (PI*) que serão comparadas no próprio cliente com a PIs do banco de dados. Tanto o processo de verificação quanto o de identificação para RBR podem ser observados nos fluxogramas da Figura 6.22 e ocorrem de forma análoga ao caso do uso de BR.

6.5.2.5. Modelo E - Comparado no cliente e armazenado no *token*.

No Modelo E, no processo de inscrição dos dados biométricos, as BRs e as respectivas IRs são associadas e armazenadas em um *token*. Assim, na verificação, os dados biométricos são capturados e processados no cliente e as BR extraídas são comparadas com os dados presentes no *token* e toma a decisão, como mostra no fluxograma da Figura 6.23. Então, caso um usuário queira verificar sua identidade deve conectar fisicamente um *token* no cliente e enviar seus dados biométricos ao cliente por meio de um sensor. Dessa forma, o cliente reivindica a identidade do usuário ao *token* e a BR do *token* é comparada com a BR extraída e então a decisão é tomada pelo próprio cliente.

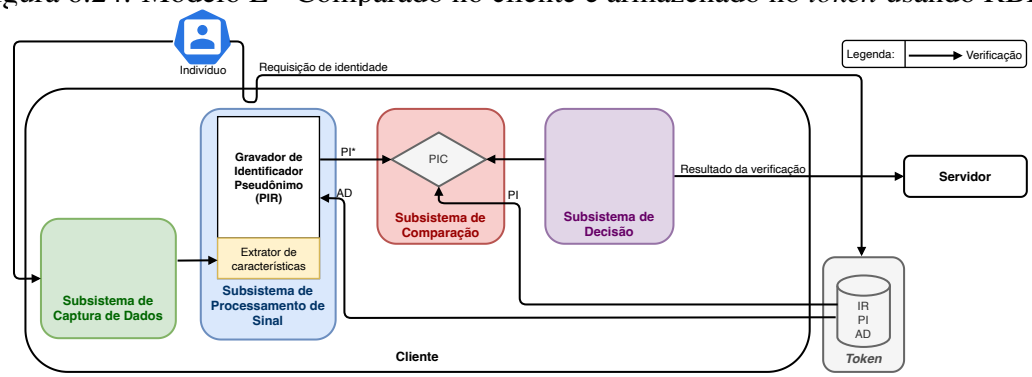
Figura 6.23: Modelo E - Comparado no cliente e armazenado no *token* usando BRs



Para implementar o Modelo E, assim como no Modelo C, o cliente deve conter tanto o sensor quanto um algoritmo capaz de fazer a comparação e a decisão. Da mesma maneira que Modelo D, em alguns casos a autenticação final pode ser feita por um servidor que confirma a verificação feita pelo cliente. Além disso, observa-se que esse modelo é utilizado apenas para verificação e frequentemente usado na forma em que o cliente

funciona como do tipo quiosque e é instalado em lugares públicos como aeroportos e prédios comerciais para autenticação pessoal. Um exemplo de uso é no controle de fronteira em aeroportos internacionais em que o e-passaporte funciona como *token*. A Figura 6.24 ilustra os processo de verificação do Modelo E para o uso de RBR.

Figura 6.24: Modelo E - Comparado no cliente e armazenado no *token* usando RBRs.

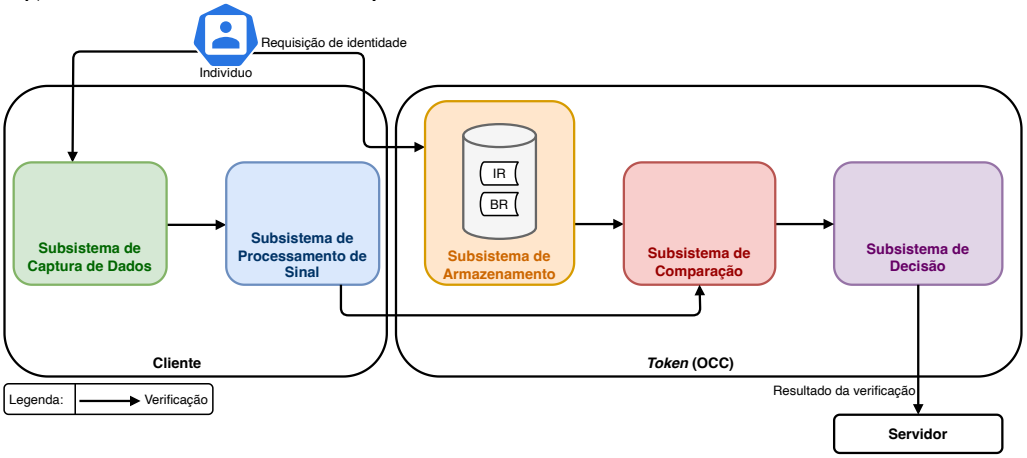


Já no caso com RBR, na inscrição dos dados, são armazenados os PIs, IR e o ADs no *token* ao invés das BRs e IRs. Adicionalmente, no processo de verificação, a PI que será transmitida ao servidor, representados por PI* no fluxograma (Figura 6.24), é gerada pelo processo de PIR que utilizada os AD do *token* e os dados biométricos extraído por meio de sensores para construir a PI (PI*) no cliente que serão comparadas com a PI presente no *token* e a decisão ocorre de forma semelhante ao caso do uso de BR.

6.5.2.6. Modelo F - comparado no *token* e armazenado no *token*.

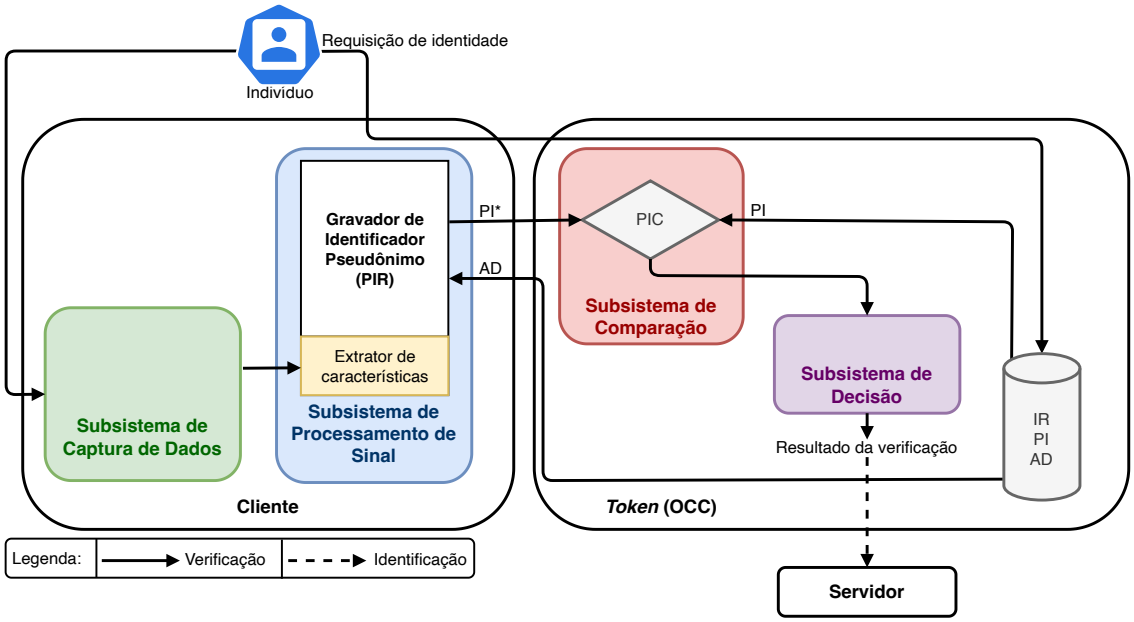
No Modelo F, no processo de inscrição dos dados biométricos, as BRs e as respectivas IRs são associadas e armazenadas em um *token*. Assim, na verificação, os dados biométricos são capturados e processados no cliente e as BR extraídas são enviadas para o *token* e então são comparadas com os dados presentes no próprio. Assim, a decisão é tomada como descrito no fluxograma da Figura 6.25.

Figura 6.25: Modelo F - comparado no *token* e armazenado no *token* usando BRs



Caso um usuário queira verificar sua identidade deve enviar seus dados biométricos para o cliente com o *token* do tipo *on-card comparison* (OCC). Assim, o cliente extrai as BRs e as IRs do usuário e as envia para o *token* para o processo de comparação. O resultado da comparação é enviado ao servidor. Dessa forma, os dados biométricos limitam-se ao *token* e ao cliente, e não é passado para o servidor. Nesse caso, o cliente pode ser um caixa eletrônico e o *token* ou cartão do tipo OCC do usuário. Observa-se que esse tipo de tecnologia é amplamente utilizado em sistemas bancários por ser consideravelmente segura, uma vez que assume-se que o *token* é capaz de fornecer um ambiente de execução seguro e isolado. A Figura 6.26 ilustra os processo de verificação do Modelo F para o uso de RBR.

Figura 6.26: Modelo F - comparado no *token* e armazenado no *token* usando RBRs.

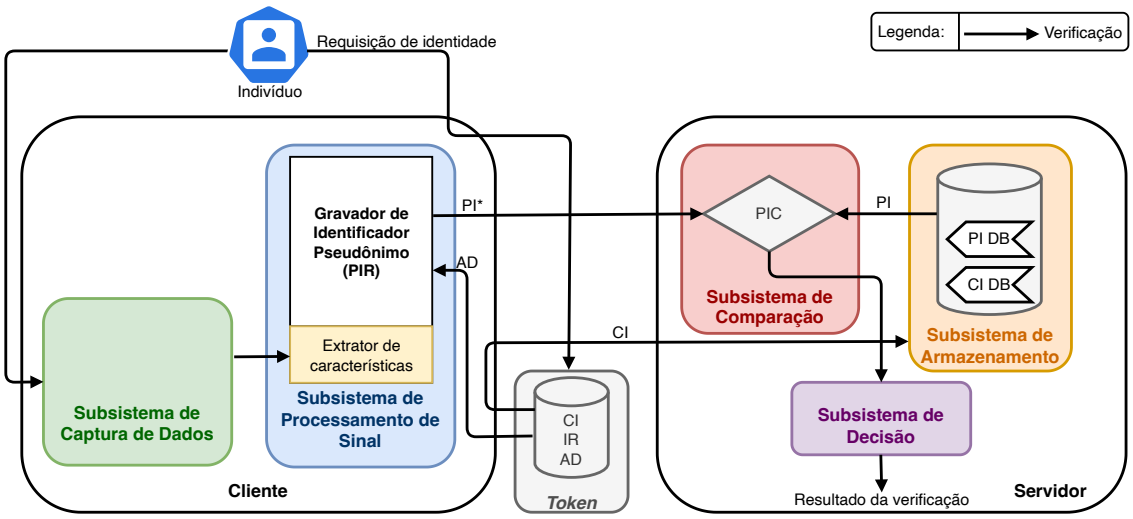


Já no caso com RBR, na inscrição dos dados, são armazenados os PIs, IRs e o ADs no *token* ao invés das BRs e IRs. Além disso, no processo de verificação, a PI que será usada na comparação, representados por PI* no fluxograma da Figura 6.26, esta é gerada no cliente pelo processo de PIR que utilizada os AD do *token* e os dados biométricos extraídos por meio de sensores para construir a PI (PI*) que serão comparadas com a PI presente no *token*. A decisão ocorre de forma semelhante ao caso com o uso de BR como mostra o fluxograma da Figura 6.26. Observa-se que também é possível que a PIR ocorra no próprio *token* o que implica com que os AD permanecessem dentro do *token* e minimizando as chances de ter a privacidade comprometida.

6.5.2.7. Modelo G - Comparado no servidor e armazenado de forma distribuída.

O Modelo G é aplicável apenas para RBR. Logo, no processo de inscrição dos dados biométricos, a PI é criada e armazenada no servidor com um *identificador comum* (CI) já a IR, o AD e a CI correspondente é armazenada em um *token*. Durante a verificação, o *token* envia para o cliente os AD e o CI e assim como nos outros modelos, por meio do processo de PIR, o cliente transforma os dados biométricos em PI que é representado como PI* no fluxograma da Figura 6.27. Na sequência, o cliente envia a PI* e o CI para o servidor que compara com a PI correspondente a CI enviada e a decisão é tomada. O benefício desse modelo é a de que a verificação só é possível quando tanto o *token* quanto o servidor possuírem os dados corretos e, nesse sentido reduzir a chances de adulteração uma vez que tanto no servidor quanto no *token* os dados deverão estar comprometidos. Além disso, isso permite que as referências biométricas sejam revogadas no servidor sem necessitar do *token*.

Figura 6.27: Modelo G - comparado no servidor e armazenado de forma distribuída.

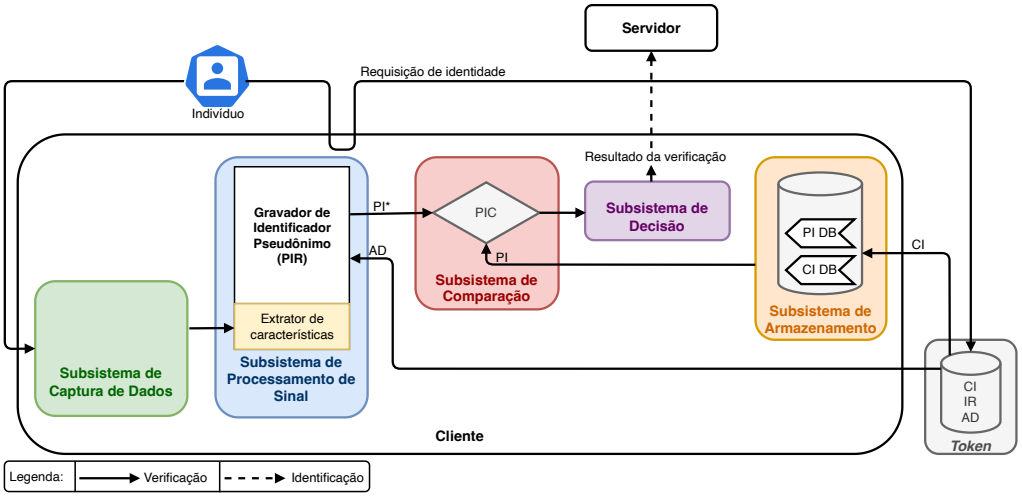


Outro benefício é o fato do usuário possuir o controle do processo de verificação, uma vez que ele é o detentor do *token*. Esse modelo é indicado para sistemas de autenticação para transação online como *e-banking*, transações com cartão de crédito *online* e como substitutos dos PIN ou como melhorias para caixas eletrônicos. Nesse sentido, esse modelo visa minimizar a quantidade de informações que são trocadas entre o cliente e o servidor, além de impedir a transmissão de partes dos dados RBR do servidor para o cliente. Ressalta-se que não é recomendável armazenar o PI em um *token* e os AD no servidor.

6.5.2.8. Modelo H - comparado no cliente e armazenado de forma distribuída.

O Modelo H também é aplicável apenas para RBR. Logo, no processo de inscrição dos dados biométricos, a PI é criada e armazenada no cliente com um CI. Já a IR, o AD e o CI correspondentes são armazenados em um *token*. Durante a verificação, o *token* envia para o cliente os AD e o CI e, assim como nos outros modelos, por meio do processo de PIRs, o cliente transforma os dados biométricos em PI que é representado como PI* no fluxograma da Figura 6.28. Na sequência, o subsistema do cliente compara a PI* com a PI correspondente ao CI e a decisão é tomada. Nesse modelo, o cliente pode ser do tipo quiosque, como os encontrados em locais públicos como aeroportos e em locais públicos edifícios, para autenticação pessoal. Este modelo também pode ser aplicado no controle de fronteira usando o passaporte eletrônico ou outro *token*.

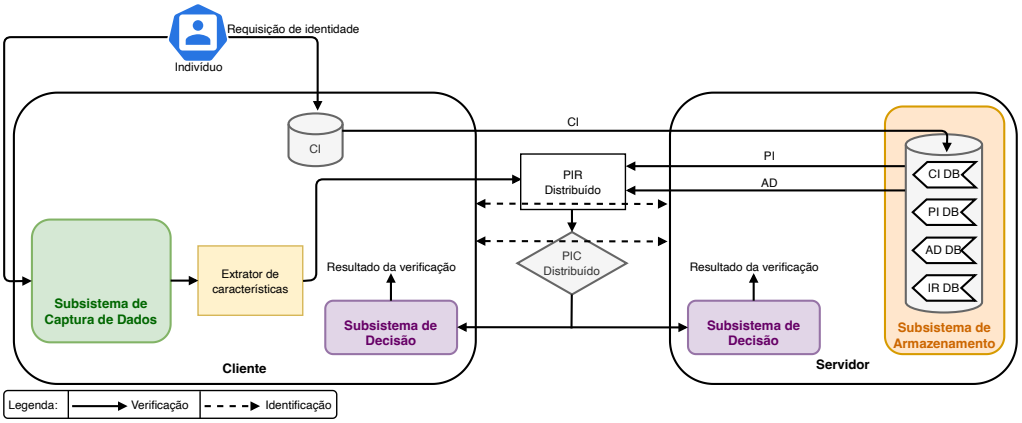
Figura 6.28: Modelo H - comparado no cliente e armazenado de forma distribuída.



6.5.2.9. Modelo I - Comparado de forma distribuída e armazenado no servidor.

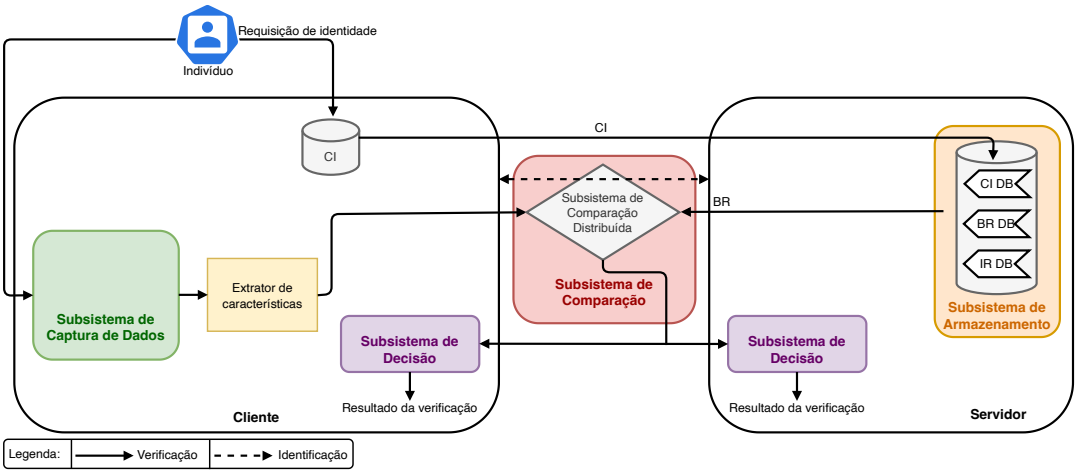
A Figura 6.29 ilustra os processo de verificação do Modelo I para o uso de BR.

Figura 6.29: Modelo I - Comparado de forma distribuída e armazenado no servidor usando BRs.



No Modelo I, no processo de inscrição dos dados biométricos, as AD, IR, PI e um CI são armazenados no servidor e o outro CI é armazenado no cliente. No processo de verificação, o servidor e o cliente nunca compartilham as AD, IR, PI mas apenas o CI. Nesse sentido, tanto o servidor quanto o cliente executam um protocolo interativo para realizar comumente os processos de comparação comparador de identificador pseudônimo / *pseudonymous identifier comparator* (PIC) e de PIR sem nunca compartilhar à outra parte os seus dados (AD, IR, PI no lado do servidor e os dados biométricos coletados no lado do cliente). Por fim, baseado nesse protocolo o interativo, o servidor e o cliente recebe apenas o resultado final da PIC. No fluxograma da Figura 6.29 é ilustrada uma das possíveis variações desse modelo usando RBRs. Esse modelo é indicado apenas aos casos em que a comunicação com a rede e a computação local são suficientemente boas, uma vez que a execução da verificação costuma ser mais pesada do que em comparação a um modelo que não há esse processo interativo. A Figura 6.30 ilustra os processo de verificação do Modelo I para o uso de RBR.

Figura 6.30: Modelo I - Comparado de forma distribuída e armazenado no servidor usando RBRs.

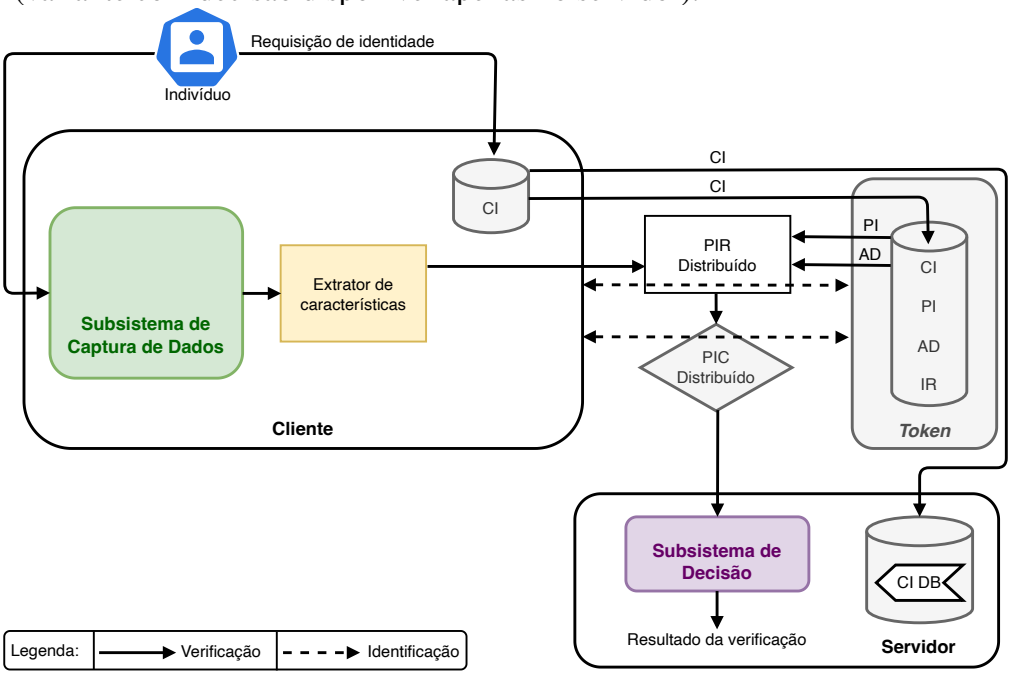


O Modelo I pode ser implementado usado RBRs (Figura 6.30), para que seja possível a implementação, o Subsistema de Comparação deve ser computado de forma distribuída por meio do uso de técnicas de comparação baseadas em métricas simples, como distância de *Hamming* ou distância euclidiana.

6.5.2.10. Modelo J - comparado de forma distribuída e armazenado no *token*.

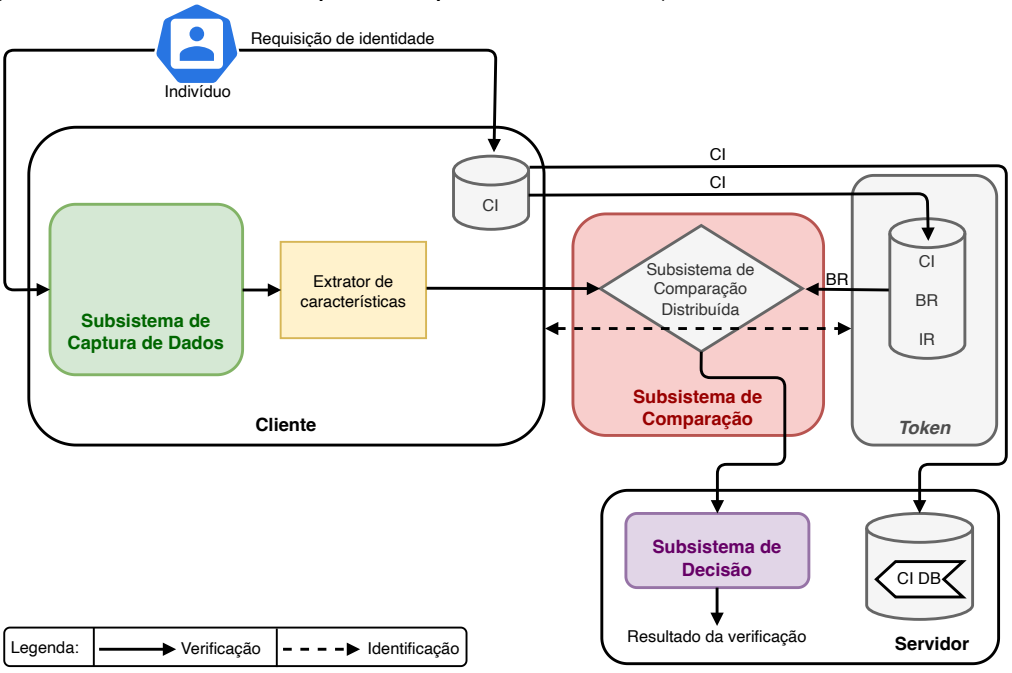
No Modelo J, no processo de inscrição dos dados biométricos, as AD, IR, PI e um CI são armazenados no *token* e o outro CI é armazenado no cliente. No processo de verificação, assim como no modelo anterior, o *token* e o cliente nunca compartilham as AD, IR, PI mas apenas o CI. Nesse sentido, tanto o servidor quanto o cliente executam um protocolo interativo para realizar comumente os processos de comparação (PIC) e de PIR sem nunca compartilhar à outra parte seus dados (AD, IR, PI no lado do *token* e os dados biométricos coletados no lado do cliente). Por fim, baseado nesse protocolo interativo, o *token* e o cliente recebem apenas o resultado final da PIC. A Figura 6.31 exemplifica uma das possíveis variações desse modelo usando RBRs. Esse modelo é indicado apenas aos casos em que a computação local for suficientemente boa.

Figura 6.31: Modelo J - Armazenado no *token*, comparado de forma distribuído usando RBR (variante com decisão disponível apenas no servidor).



A Figura 6.32 ilustra os processo de verificação do Modelo J para o uso de BR. Assim como no modelo anterior, o modelo pode ser implementado usado BRs como ilustrado no fluxograma da Figura 6.32 na condição de que o Subsistema de Comparação possa ser computado de forma distribuída.

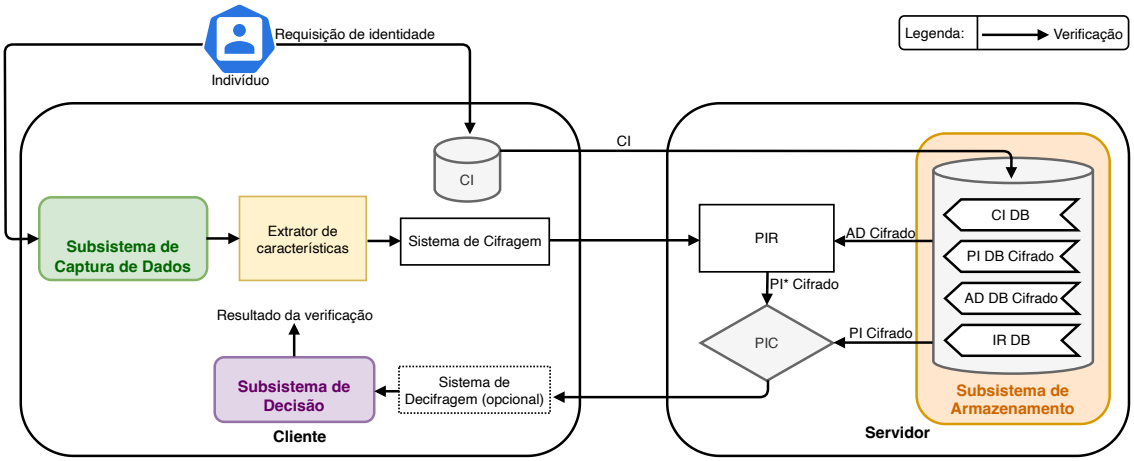
Figura 6.32: Modelo J - Armazenado no *token*, comparado de forma distribuído usando BR (variante com decisão disponível apenas no servidor).



6.5.2.11. Modelo K - comparado de forma distribuída e armazenado de forma distribuída.

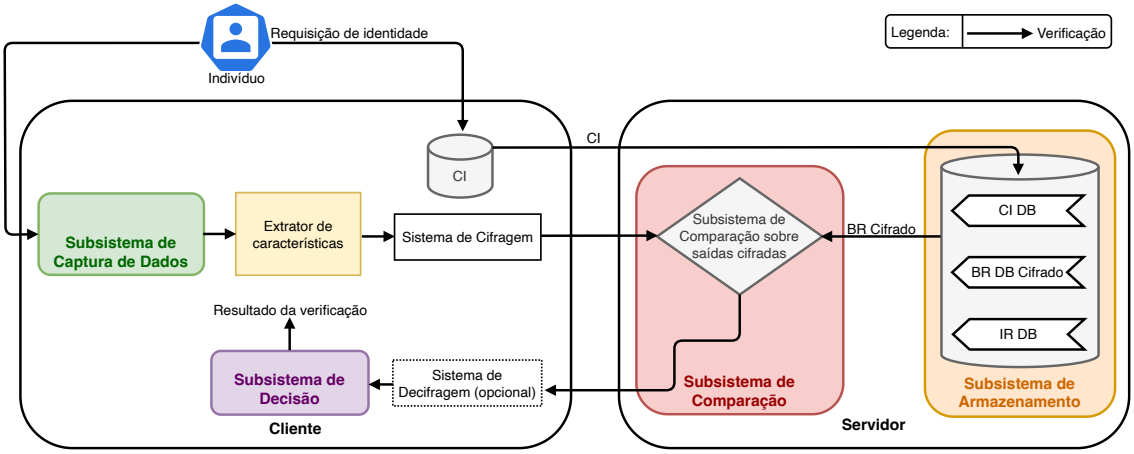
A Figura 6.33 ilustra os processo de verificação do modelo K para o uso de RBR. Nesse modelo, no processo de inscrição dos dados biométricos, as AD, IR, PI são armazenadas de forma distribuída no cliente, servidor e no *token* (caso exista) e um CI é armazenado em cada uma das plataformas. Nesse sentido, o AD e o PI são armazenados de forma cifrada, de modo que possam executar operações sem que seja decifrados previamente. Um exemplo de aplicação é o uso de criptografia homomórfica. Durante a verificação, os processos de PIR e PIC são realizados ou no lado do cliente, *token* ou servidor, e são executados diretamente nos dados cifrados. Na sequência, o resultado da comparação (PIC) é diretamente enviado para o Subsistema de Decisão, como ilustrado no fluxograma da Figura 6.34 para o caso da PIC e da PIR ocorrendo no servidor. Para garantir a confidencialidade dos dados cifrados, o proprietário da chave criptográfica deve ser a parte que não armazena esses dados cifrados. Esse modelo é indicado apenas aos casos em que a computação local for suficientemente boa, uma vez que a execução da verificação em modelos cifrados costuma exigir maior capacidade computacional.

Figura 6.33: Modelo K - Armazenada de forma distribuída, comparado distribuída (variante com PIR e PIC no lado do servidor) usando RBRs, sendo o Sistema de Decifragem opcional.



A Figura 6.33 ilustra os processo de verificação do Modelo K para o uso de BR. Assim como nos modelos anteriores, esse modelo pode ser implementado usado BRs na condição de que o Subsistema de Comparação possa operar de forma cifrada.

Figura 6.34: Modelo K - Armazenada de forma distribuída, comparado distribuidamente (variante com PIR e PIC no lado do servidor) usando BRs, sendo o Sistema de Decifragem é opcional.



6.6. Considerações finais

Os modelos servem como guias para os desenvolvedores de sistemas biométricos e devem ser escolhidos conforme as necessidades e o contexto do projeto. Com isso, para um sistema ser considerado seguro, é essencial que tenha como base algum desses modelos. Embora alguns dos modelos dessa descrito na Seção 6.5 sejam considerados mais teóricos e com poucas aplicações práticas, é importante que estes sejam levados em consideração em implementações e em um contexto adequado ou para servirem como inspiração para outras aplicações. A utilização das características biométricas dos seres humano continua em expressivo crescimento nas mais variadas aplicações, e em muitos cenários de forma indiscriminada. As características biométricas por se tratarem de dados sensíveis, necessitam de mecanismos de proteção adequados para garantir aspectos de segurança, privacidade e conformidade. No contexto brasileiro, a Lei Geral de Proteção de Dados (LGPD) regula as atividades de tratamento dos dados pessoais.

O presente capítulo apresenta as características de tratamento dos dados biométricos e suas especificidades em seu respectivo ciclo de vida, com base na norma ISO/IEC 24745:2022. Também os requisitos recomendados de segurança para o tratamento destes dados pelos sistemas, bem como as ameaças e as contramedidas recomendadas. Dada a característica ,por parte dos sistemas que utilizam dados biométricos para realizar a autenticação e autorização nos sistemas, as necessidades fundamentais de renovação e revogação destes dados biométricos em caso de comprometimento ou necessidade específica de alguma aplicação são de considerável relevância. Assim, os mecanismos para proteção de *templates* biométricos e as suas características foram introduzidas, apresentando os importantes conceitos de biometria revogável ou biometria cancelável. Além de modelos e cenários recomendados para tratamento destes dados sensíveis por parte dos sistemas em suas mais variadas aplicações, com base em requisitos de segurança apresentados.

Apesar dos requisitos de segurança e privacidade para o tratamento dos dados biométricos, e mecanismos de proteção dos *templates* biométricos, existem diversas de-

mandas que necessitam ser abordadas em trabalhos futuros, dada a complexidade que envolvem estes sistemas heterogêneos compostos por hardware e software, bem como aspectos legais. Por fim, existem oportunidades de pesquisa envolvendo o ciclo de vida de tratamento de dados com relação à segurança e privacidade, bem como tratamento das ameaças nas etapas (captura, extração de características, comparação, decisão e armazenamento) dos sistemas, em especial os sistemas de autenticação.

Agradecimentos

O presente trabalho foi em parte financiado pelo CNPq (Projeto 304643/20 20-3), CAPES (Código de Financiamento 001), FAPESP (Projeto 2020/09850-0), e Ripple's University Blockchain Research Initiative (UBRI).

Os autores agradecem o apoio do Laboratório de Arquitetura e Redes de Computadores (LARC) do Departamento de Engenharia de Produção e Sistemas Digitais (PCS) da Escola Politécnica da Universidade de São Paulo (USP).

Os autores agradecem o apoio do Laboratório de Processamento Paralelo e Distribuído (LabP2D) no Centro de Ciências tecnológicas (CCT) / Programa de Pós-Graduação em Computação Aplicada (PPGCAP) da Universidade do Estado de Santa Catarina (UDESC) e da Fundação de Amparo à Pesquisa e Inovação do Estado de Santa Catarina (FAPESC).

Referências

[Araújo et al., 2005] Araújo, L., Sucupira, L., Lizarraga, M., Ling, L., and Yabu-Uti, J. (2005). User authentication through typing biometrics features. *IEEE transactions on signal processing*, 53(2):851–855.

[Armknecht et al., 2015] Armknecht, F., Boyd, C., Carr, C., Gjøsteen, K., Jäschke, A., Reuter, C. A., and Strand, M. (2015). A guide to fully homomorphic encryption. Cryptology ePrint Archive, Paper 2015/1192. https://eprint.iacr.org/2015/1192.

[Balakrishnan et al., 2021] Balakrishnan, S., Venkatesan, V. K., and Syed Shahul Hameed, M. (2021). An embarking user friendly palmprint biometric recognition system with topnotch security. pages 1028–1032.

[Bloom, 1970] Bloom, B. H. (1970). Space/time trade-offs in hash coding with allowable errors. *Commun. ACM*, 13(7):422–426.

[Bolle et al., 2013] Bolle, R. M., Connell, J. H., Pankanti, S., Ratha, N. K., and Senior, A. W. (2013). *Guide to biometrics*. Springer Science & Business Media.

[Conrads, 2019] Conrads, J. (2019). Ddos attack fingerprint extraction tool : making a flow-based approach as precise as a packet-based. http://essay.utwente.nl/79567/.

[Costa et al., 2006] Costa, L. R., Obelheiro, R. R., and Fraga, J. S. (2006). Introdução à Biometria. In *Minicursos do VI Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais*, volume 1, page 49. SBC, Santos/SP.

[Cross and Smith, 1995] Cross, J. and Smith, C. (1995). Thermographic imaging of the subcutaneous vascular network of the back of the hand for biometric identification. In

Proceedings The Institute of Electrical and Electronics Engineers. 29th Annual 1995 International Carnahan Conference on Security Technology, pages 20–35. IEEE.

[Faria, 2014] Faria, B. G. (2014). Implementação e avaliação do abid (aplicativo biométrico de impressão digital) utilizando o método fuzzy vault e ferramentas open source. Master's thesis, Universidade Presbiteriana Mackenzie.

[Gomez-Barrero et al., 2017] Gomez-Barrero, M., Maiorana, E., Galbally, J., Campisi, P., and Fierrez, J. (2017). Multi-biometric template protection based on homomorphic encryption. *Pattern Recognition*, 67:149–163.

[Gomez-Barrero et al., 2016] Gomez-Barrero, M., Rathgeb, C., Galbally, J., Busch, C., and Fierrez, J. (2016). Unlinkable and irreversible biometric template protection based on bloom filters. *Information Sciences*, 370-371:18–32.

[Hernandez-Ortega et al., 2023] Hernandez-Ortega, J., Fierrez, J., Morales, A., and Galbally, J. (2023). Introduction to presentation attack detection in face biometrics and recent advances. *Handbook of Biometric Anti-Spoofing: Presentation Attack Detection and Vulnerability Assessment*, pages 203–230.

[ISO/IEC 24745, 2022] ISO/IEC 24745 (2022). Information security – cybersecurity and privacy protection – biometric information protection. Standard, International Organization for Standardization.

[ISO/IEC 29100, 2011] ISO/IEC 29100 (2011). Information technology — security techniques — privacy framework. Standard, International Organization for Standardization.

[ISO/IEC 30136, 2018] ISO/IEC 30136 (2018). Information technology — performance testing of biometric template protection schemes. Standard, International Organization for Standardization.

[Jain et al., 1996] Jain, A., Bolle, R., and Pankanti, S. (1996). Introduction to biometrics. In Jain, A. K., Bolle, R., and Pankanti, S., editors, *Biometrics*. Springer, Boston, MA.

[Jain et al., 1999] Jain, A., Bolle, R., and Pankanti, S. (1999). *Biometrics: personal identification in networked society*, volume 479. Springer Science & Business Media.

[Jain and Kant, 2015] Jain, R. and Kant, C. (2015). Attacks on biometric systems: an overview. *International Journal of Advances in Scientific Research*, 1(07):283–288.

[Jin et al., 2004] Jin, A. T. B., Ling, D. N. C., and Goh, A. (2004). Biohashing: two factor authentication featuring fingerprint data and tokenised random number. *Pattern Recognition*, 37(11):2245–2255.

[Juels and Sudan, 2006] Juels, A. and Sudan, M. (2006). A Fuzzy Vault Scheme. *Designs, Codes and Cryptography*, 38(2):237–257.

[Juels and Wattenberg, 1999] Juels, A. and Wattenberg, M. (1999). A fuzzy commitment scheme. In *Proceedings of the 6th ACM Conference on Computer and Communications Security*, CCS '99, page 28–36, New York, NY, USA. Association for Computing Machinery.

[Kaur and Khanna, 2016] Kaur, H. and Khanna, P. (2016). Biometric template protection using cancelable biometrics and visual cryptography techniques. *Multimedia Tools and Applications*, 75:16333–16361.

[Kelkboom et al., 2011] Kelkboom, E. J. C., Breebaart, J., Kevenaar, T. A. M., Buhan, I., and Veldhuis, R. N. J. (2011). Preventing the decodability attack based cross-matching in a fuzzy commitment scheme. *IEEE Transactions on Information Forensics and Security*, 6(1):107–121.

[Khan et al., 2015] Khan, S. H., Akbar, M. A., Shahzad, F., Farooq, M., and Khan, Z. (2015). Secure biometric template generation for multi-factor authentication. *Pattern Recognition*, 48(2):458–472.

[Li and Jain, 2009] Li, S. Z. and Jain, A. (2009). *Encyclopedia of Biometrics: I-Z.*, volume 1. Springer Science & Business Media.

[Li and Jain, 2015] Li, S. Z. and Jain, A. K., editors (2015). *Encyclopedia of Biometrics*. Springer, New York, NY, 2 edition.

[Maiorana et al., 2010] Maiorana, E., Campisi, P., Fierrez, J., Ortega-Garcia, J., and Neri, A. (2010). Cancelable templates for sequence-based biometrics with application to on-line signature recognition. *Trans. Sys. Man Cyber. Part A*, 40(3):525–538.

[Maltoni et al., 2009] Maltoni, D., Maio, D., Jain, A. K., and Prabhakar, S. (2009). *Handbook of Fingerprint Recognition*. Springer Professional Computing. Springer London, 2 edition.

[Marcondes, 2019] Marcondes, J. (2019). Biometria, sistema biométrico: O que é, como funciona?. Disponível em: https://gestaodesegurancaprivada.com.br/biometria-sistema-biometrico-o-que-e-como-funciona/. Acesso em: 18 jul 2023.

[Martinez-Diaz et al., 2006] Martinez-Diaz, M., Fierrez-Aguilar, J., Alonso-Fernandez, F., Ortega-Garcia, J., and Siguenza, J. (2006). Hill-climbing and brute-force attacks on biometric systems: A case study in match-on-card fingerprint verification. In *Proceedings 40th Annual 2006 International Carnahan Conference on Security Technology*, pages 151–159.

[Matos, 2000] Matos, R. M. d. (2000). Autenticação de usuários através da utilização de sistemas biométricos. Dissertação de mestrado, Universidade Federal do Rio Grande do Sul, Porto Alegre, RS, Brasil. Dissertação de Mestrado, UFRGS.

[Mtibaa et al., 2021] Mtibaa, A., Petrovska-Delacrétaz, D., Boudy, J., and Ben Hamida, A. (2021). Privacy-preserving speaker verification system based on binary i-vectors. *IET Biometrics*, 10(3):233–245.

[Nafea et al., 2016] Nafea, O., Ghouzali, S., Abdul, W., and Qazi, E.-u.-H. (2016). Hybrid multi-biometric template protection using watermarking. *The Computer Journal*, 59(9):1392–1407.

[Oliveira Filho, 2014] Oliveira Filho, I. d. L. (2014). *Algoritmo Papílio como Método de Proteção de Templates para Aumentar a Segurança em Sistemas de Identificação Biométricos*. Tese de doutorado, Universidade Federal do Rio Grande do Norte, Natal, RN, Brasil.

[Pabitha and Latha, 2013] Pabitha, M. and Latha, L. (2013). Efficient approach for retinal biometric template security and person authentication using noninvertible constructions. *International Journal of Computer Applications*, 69:28–34.

[Palmeiras, 2021] Palmeiras, S. E. (2021). Política de privacidade e proteção de dados. Disponível em: https://sep-bucket-prod.s3.amazonaws.com/wp-content/uploads/2021/08/politica-de-privacidade_12082021.pdf. Acesso em: 21 jul 2023.

[Palmeiras, 2023] Palmeiras, S. E. (2023). Comunicado: Cadastro de biometria facial dos lientes - passaporte. Disponível em: https://www.palmeiras.com.br/noticias/comunicado-cadastro-de-biometria-facial-dos-clientes-passaporte/. Acesso em: 21 jul 2023.

[Patel et al., 2015a] Patel, V. M., Ratha, N. K., and Chellappa, R. (2015a). Cancelable biometrics: A review. *IEEE Signal Processing Magazine*, 32(5):54–65.

[Patel et al., 2015b] Patel, V. M., Ratha, N. K., and Chellappa, R. (2015b). Cancelable biometrics: A review. *IEEE Signal Processing Magazine*, 32(5):54–65.

[Ratha et al., 2001a] Ratha, N. K., Connell, J. H., and Bolle, R. M. (2001a). Enhancing security and privacy in biometrics-based authentication systems. *IBM Systems Journal*, 40(3):614–634.

[Ratha et al., 2001b] Ratha, N. K., Connell, J. H., and Bolle, R. M. (2001b). Enhancing security and privacy in biometrics-based authentication systems. *IBM Systems Journal*, 40(3):614–634.

[Rathgeb et al., 2014] Rathgeb, C., Breitinger, F., Busch, C., and Baier, H. (2014). On application of bloom filters to iris biometrics. *IET Biometrics*, 3(4):207–218.

[Rathgeb and Uhl, 2011] Rathgeb, C. and Uhl, A. (2011). A survey on biometric cryptosystems and cancelable biometrics. *EURASIP Journal on Information Security*, 2011(1):3.

[Schauren, 2016] Schauren, L. F. (2016). Segurança no sistema brasileiro de votação eletrônica. Trabalho de Conclusão de Curso. Instituto de Informática. Universidade Federal do Rio Grande do Sul. Disponível em: https://lume.ufrgs.br/handle/10183/151030.

[T. R. Jacqueline, 2012] T. R. Jacqueline, Salem Nathálea, W. M. B. V. (2012). Modelo intencional genérico de sistemas biométricos. In *Anais do WER12 - Workshop em Engenharia de Requisitos, Buenos Aires, Argentina, Abril 24-27, 2012*.

[Tribunal Reginal Eleitoral, 2023] Tribunal Reginal Eleitoral (2023). Perguntas e respostas - parte 1. Disponível em: https://www.tre-sp.jus.br/eleicoes/eleicoes-anteriores/eleicoes-2018/perguntas-e-respostas-parte-1. Acesso em: 20 jul 2023.

[Tribunal Superior Eleitoral, 2023] Tribunal Superior Eleitoral (2023). Urna eletrônica. Disponível em: https://www.tse.jus.br/internet/temporarios/urna-seguranca/identificacao-biometrica.html. Acesso em: 20 jul 2023.

[Wojewidka, 2020] Wojewidka, J. (2020). The deepfake threat to face biometrics. *Biometric Technology Today*, 2020(2):5–7.

[Yang et al., 2022] Yang, W., Wang, S., Kang, J. J., Johnstone, M. N., and Bedari, A. (2022). A linear convolution-based cancelable fingerprint biometric authentication system. *Computers & Security*, 114:102583.

[Zadeh, 1965] Zadeh, L. (1965). Fuzzy sets. *Information and Control*, 8(3):338–353.