Ministério da Justiça

Termo de Cooperação/Projeto:

Acordo de Cooperação Técnica FUB/CDT e MJ/SE Registro de Identidade Civil – Replanejamento e Novo Projeto Piloto

UnB

Documento:

RT Armazenamento Biométrico

Data de Emissão:

25/11/2014

Centro de Apoio ao Desenvolvimento Tecnológico
UnB

Elaborado por:

Universidade de Brasília – UnB
Centro de Apoio ao Desenvolvimento Tecnológico – CDT
Laboratório de Tecnologias da Tomada de Decisão – LATITUDE.UnB

latitude
Laboratório de tecnologias da tomada de decisão

MINISTÉRIO DA JUSTIÇA

José Eduardo Cardozo
Ministro

Marivaldo de Castro Pereira
Secretário Executivo

Helvio Pereira Peixoto
Coordenador Suplente do Comitê Gestor do SINRIC

UNIVERSIDADE DE BRASÍLIA

Ivan Marques Toledo Camargo
Reitor

Paulo Anselmo Ziani Suarez
Diretor do Centro de Apoio ao Desenvolvimento Tecnológico – CDT

Rafael Timóteo de Sousa Júnior
Coordenador do Laboratório de Tecnologias da Tomada de Decisão – LATITUDE

EQUIPE TÉCNICA
Ana Maria da Consolação Gomes Lindgren
Alexandre Cardoso de Barros
Andréa Benoliel de Lima
Celso Pereira Salgado
Delluiz Simões de Brito
Domingos Soares dos Santos
Elaine Fabiano Tocantins
Fernando Saliba
Fernando Teodoro Filho
Guilherme Braz Carneiro
Jhon Kennedy Férrer Lima
José Alberto Sousa Torres
Joaquim de Oliveira Machado
Marcelo Martins Villar
Paulo Cesar Vieira dos Santos
Raphael Fernandes de Magalhães Pimenta
Rodrigo Borges Nogueira
Rodrigo Gurgel Fernandes Távora
Sara Lais Rahal Lenharo

EQUIPE TÉCNICA
Flávio Elias Gomes de Deus (Pesquisador Sênior)
William Ferreira Giozza (Pesquisador Sênior)
Ademir Agustinho de Rezende Lourenço
Adriana Nunes Pinheiro
Alessandro Zimmer
Alysson Fernandes de Chantal
Amanda Almeida Paiva
Andréia Campos Santana
Andreia Guedes Oliveir
Antonio Claudio Pimenta Ribeiro
Carolinne Januária de Souza Martins
Caio Rondon Botelho de Carvalho
Daniela Carina Pena Pascual
Danielle Ramos da Silva
Eduarda Simões Veloso Freire
Fábio Lúcio Lopes Mendonça
Fábio Mesquita Buiati
Glaidson Menegazzo Verzeletti
Johnatan Santos de Oliveira
José Carneiro da Cunha Oliveira Neto
José Elenilson Cruz
Kelly Santos de Oliveira Bezerra
Luciano Pereira dos Anjos
Luciene Pereira de Cerqueira Kaipper
Luiz Antonio de Souto Evaristo
Luiz Claudio Ferreira
Marco Schaffer
Marcos Vinicius Vieira da Silva
Mirele Maria Cavalcante Rocha
Pedro Augusto Oliveira de Paula
Renata Elisa Medeiros Jordão
Roberto Mariano de Oliveira Soares
Sandro Augusto Pavlik Haddad
Sergio Luiz Teixeira Camargo
Soleni Guimarães Alves
Suzane Lais De Freitas
Valério Aymoré Martin
Vinicius de Morais Alvess
Wladmir Rodrigues da Fonseca

HISTÓRICO DE REVISÕES

Data	Versão	Descrição
15/07/2014	0.1	Versão inicial.
19/09/2014	0.2	Versão parcial encaminhada para revisão da Equipe Técnica
25/11/2014	0.3	Versão final encaminhada para revisão da Equipe Técnica

latitude
Laboratório de tecnologias da tomada de decisão

Universidade de Brasília – UnB
Campus Universitário Darcy Ribeiro - FT – ENE – Latitude
CEP 70.910-900 – Brasília-DF
Tel.: +55 61 3107-5598 – Fax: +55 61 3107-5590

SUMÁRIO

FIGURAS

TABELAS

1. INTRODUÇÃO

A Secretaria Executiva (SE/MJ), vinculada ao Ministério da Justiça (MJ), é responsável por viabilizar o desenvolvimento e a implantação do Registro de Identidade Civil, instituído pela Lei nº 9.454, de 7 de abril de 1997, regulamentado pelo Decreto nº 7.166, de 5 de maio de 2010.

Atualmente, a República Federativa do Brasil conta com sistema de identificação de seus cidadãos amparado pela Lei nº 7.116, de 29 de agosto de 1983. Essa lei assegura validade nacional às Carteiras de Identidade, ou Cédulas de Identidade; confere também autonomia gerencial às Unidades Federativas no que concerne à expedição e controle dos números de registros gerais emitidos para cada documento. Essa condição de autonomia, ao contrário do que pode parecer, fragiliza o sistema de identificação, já que dá condições ao cidadão de requerer legalmente até 27 (vinte e sete) cédulas de identidades diferentes. Com essa facilidade legal, inúmeras possibilidades fraudulentas se apresentam de maneira silenciosa, pois, na grande maioria dos casos, os Institutos de Identificação das Unidades Federativas não dispõem de protocolos e aparato tecnológico para identificar as duplicações de registro vindas de outros estados, ou até mesmo do seu próprio arquivo datiloscópico. Consoante aos fatos, os Institutos de Identificação não trabalham interativamente para que haja trocas de informações de dados e geração de conhecimento para manuseio inteligente e seguro para individualização do cidadão em prol da sociedade.

Com foco na busca de soluções para tais problemas, o Projeto RIC prevê a administração central dos dados biográficos e biométricos dos cidadãos no Cadastro Nacional de Registro de Identificação Civil (CANRIC) e ABIS (do inglês *Automated Biometric Identification System*), respectivamente. A previsão desse novo modelo sustenta a não duplicação de registros e a consequente identificação unívoca dos cidadãos brasileiros natos e naturalizados. O Projeto RIC, portanto, visa otimizar o sistema de identificação e individualização do cidadão brasileiro nato e naturalizado com vistas a um perfeito funcionamento da gestão de dados da sociedade, agregando valor à cidadania, à gestão administrativa, à simplificação do acesso aos serviços disponíveis ao cidadão e à segurança pública do país.

Nesse contexto, o termo de cooperação entre MJ/SE e FUB/CDT define um projeto que objetiva identificar, mapear e desenvolver parte dos processos e da infraestrutura tecnológica necessária para viabilizar a implantação do número único de Registro de

Identidade Civil – RIC no Brasil.

O presente documento tem o objetivo de descrever as principais características do armazenamento biométrico em um sistema de identificação civil. Para que se entenda como se armazenam os dados biométricos, primeiro é necessária uma descrição das fases e processos de um sistema biométrico, que vão desde a captura dos dados até a fase de decisão no processo de verificação de identidade de um usuário.

Após essa introdução dos conceitos básicos, dar-se-á uma explicação dos possíveis locais de armazenamentos desses dados assim como dos padrões de armazenamento como ISO/IEC, BioAPI e NIST.

Por último, são feitas recomendações e justificativas do armazenamento dos dados biométricos do projeto RIC, dando ênfase dessa forma, as características de geração do *template*, mecanismos de verificação e identificação do indivíduo.

2. PROCESSOS DE UM SISTEMA BIOMÉTRICO

Um sistema biométrico é, em essência, um sistema que engloba reconhecimento de padrões e classificação. Como tal, este sistema é probabilístico, no sentido de que a saída do sistema, e.g., a classificação de um usuário como genuíno ou impostor, é baseada em uma nota (*score*) atribuída à amostra submetida pelo usuário, que representa o grau de semelhança entre essa amostra e o gabarito de comparação. Logo o sistema é sujeito a certa probabilidade de erro. A incerteza em sistemas biométricos advém de vários fatores: qualidade da amostra coletada, posicionamento em relação ao sensor, robustez dos algoritmos do sistema, alteração do traço biométrico no decorrer do tempo, entre outros.

A seguir são apresentadas algumas definições usadas neste documento.

- Indivíduo: pessoa que se submete ao processamento pelo sistema biométrico
- Traço (*trait*): propriedade biométrica avaliada (e.g., impressão digital, imagem da íris, formato da palma da mão)
- Amostra: aquisição única de um traço do usuário
- Usuário genuíno: usuário cuja identidade corresponde à identidade declarada
- Usuário impostor: usuário cuja identidade não corresponde à identidade declarada
- Modelo (*template*): conjunto de características essenciais (*features*) extraídas da amostra (e.g., minucias de uma impressão digital)
- Comparador (*matcher*): um algoritmo que compara o modelo extraído da amostra com o modelo do gabarito guardado no sistema (ou dispositivo portátil)
- Nota (*score*): um número atribuído pelo validador a uma amostra, que representa o seu grau de semelhança (ou diferença) com o gabarito, que pode ser guardado no banco de dados no sistema (ou dispositivo portátil).
- Sistema multimodal (ou multi-traço): sistema biométrico que utiliza informação de traços diferentes (e.g., impressão digital e imagem de íris).

Usualmente, um sistema biométrico pode ser dividido nos seguintes processos (Anil Jain, 2007), a saber.

- Aquisição / Captura
- Processamento

- Armazenamento
- Comparação (Verificação / Identificação)
- Decisão

A Figura 1 ilustra um diagrama conceitual dos processos de um sistema biométrico. Portanto, para entender o funcionamento do armazenador de dados biométrico, deve-se entender em primeiro lugar como é realizada a captura / aquisição dos dados biométricos do indivíduo, seu formato, suas características e como esses dados são utilizados nas etapas subsequentes do sistema biométrico.

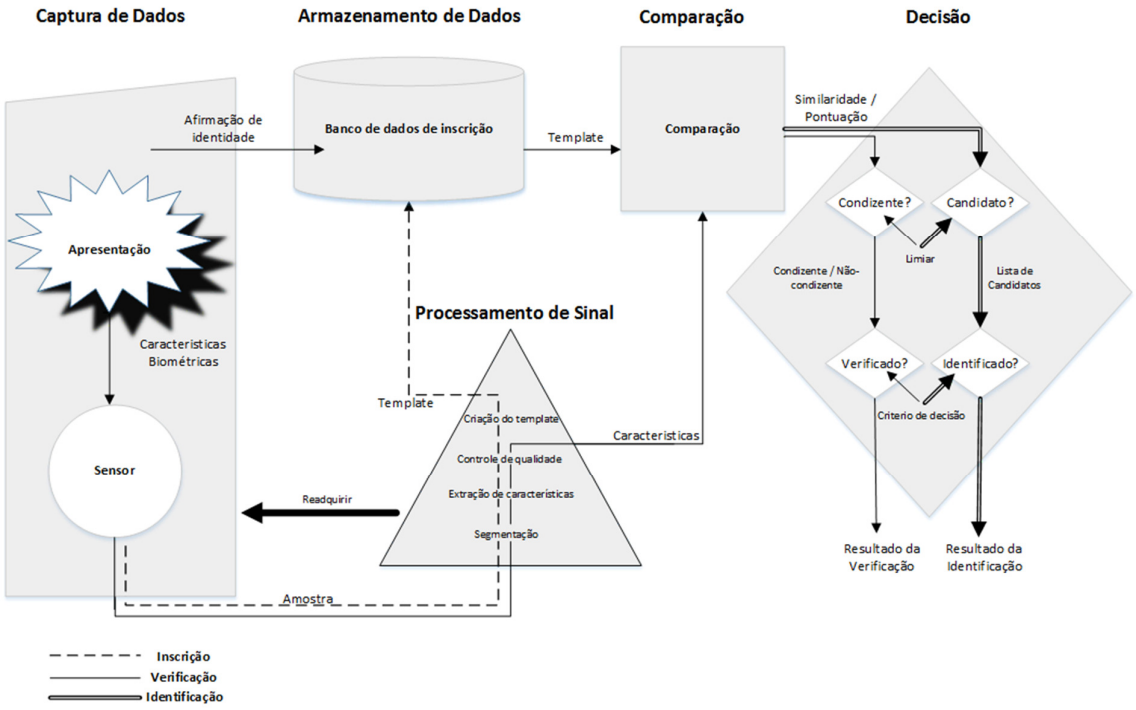

Figura 1 - Processos de um sistema biométrico

(Adaptado de: MODI, Shimon K. Biometrics in Identity Management: Concepts to Applications. Artech House, 2011.)

Todos os processos de um sistema biométrico (Figura 1) podem ser executados em um mesmo dispositivo ou em dispositivos diferentes, dependendo basicamente do tipo de sensor utilizado no momento da captura dos dados do indivíduo e do objetivo geral do sistema biométrico. Assim, a geração do modelo ou *template* biométrico e seu

armazenamento podem ser realizados em diferentes localidades do sistema. Entre os sensores disponíveis, destacam-se os seguintes.

Sensores embarcados: são sensores como os encontrados em fechaduras biométricas ou em catracas de academias/pequenas empresas. Neste caso, toda a base de dados é armazenada no próprio dispositivo de aquisição, que é responsável tanto pelo cadastramento como pela verificação. Tem a vantagem de ser rápido (para pequenas bases até 500 usuários) e de preço intermediário, variando segundo o tamanho da base de dados a ser armazenada além de necessitar de configuração mínima (tipo "*plug and play*"). A principal desvantagem é justamente a falta de flexibilidade na configuração e o tamanho restrito das bases. Esse tipo de sensor não é apropriado para um projeto de grande escala como o RIC devido as desvantagens mencionadas.

Sensores micro-processados: fazem a extração do "*template*", mas não fazem armazenamento/comparação. Existem duas possibilidades de geração do *template*: (1) são gerados os códigos biométricos do indivíduo durante a aquisição inicial das impressões digitais, sendo então enviados a um computador que processará os códigos, gerando o "*template*" e os limiares correspondentes; (2) a comparação dos códigos biométricos já é feita no próprio sensor, que gera o "*template*" e os limiares de decisão, enviando-os ao computador para armazenamento e futura comparação (normalmente encontrado nas soluções comerciais). A vantagem deste equipamento de captura é a necessidade de uma pequena banda de transmissão de dados, pois envia-se apenas o "*template*" ou os códigos biométricos e os limiares. É mais caro e menos flexível (configuração). Os *softwares* que permitem maior gama de customização são normalmente de configuração complexa. Esse tipo de sensor pode vir a ser utilizado no projeto RIC.

Sensores puros: produzem simplesmente imagens "*raster*", ou brutas, do traço biométrico sendo coletado. Todo o processamento/armazenagem precisa ser feito por um computador externo. São normalmente conectados via USB (se externos), via barramento do computador (internos), ou via rede de computadores (menos comuns). Normalmente possuem um SDK (*Software Development Kit*) capaz de ajustar alguns parâmetros de aquisição das imagens (fator gama por exemplo). Apresenta como vantagens ser simples, robusto e barato, mas depende integralmente de um *software* de processamento que pode ou não estar incluído na compra. Se estiver incluído com o dispositivo "de prateleira", adquirido em qualquer loja de informática, possui diversas limitações de operação/configuração/quantidade de impressões, além de ser mais lento pois a imagem

como um todo precisa ser transferida para ser processada, necessitando de mais banda para a transmissão da informação. Esse tipo de sensor pode vir a ser utilizado no projeto RIC.

A Tabela 1 resume as vantagens e desvantagens de cada uma das soluções.

Sensores	Vantagens	Desvantagens	Apropriado ao RIC
Embarcados	- Base de dados armazenada no próprio dispositivo - Rápido - Autenticação local	- Falta de flexibilidade na configuração - Bases pequenas (500 usuários)	**Não** Trata-se de sistemas limitados e com bases pequenas de usuários.
Micro-processados	- Necessidade de pouca banda de transmissão (normalmente se envia apenas o *template*)	- Alto custo - Falta de flexibilidade na configuração	**Sim (Verificação)** Devido ao uso de pouca banda de transmissão no envio das informações. Adequado para o processo de verificação.
Puros	- Produzem imagens brutas - Processamento precisa ser feito por um computador externo (USB, barramento ou rede) - Simples, robusto e barato	- Depende de um *software* de processamento para a geração do *template* - Possui limitações de operação e configuração. - Necessita muita banda para a transmissão da imagem	**Sim (Cadastramento)** Sistema sem complexidade de processamento, sendo simples, robusto e barato. Adequado para o processo de cadastramento.

Tabela 1 - Tipos de sensores biométricos

Baseando-se nas características apresentadas na Tabela 1 e de acordo com as necessidades e requisitos de um projeto de grande escala como o RIC, este documento contemplará, de aqui adiante, somente os sensores micro-processados e os sensores puros, adequados para os processos de verificação e cadastramento, respectivamente.

Outro componente importante nos sistemas de armazenamento e processamento de dados biométricos é o ABIS (Sistema de Identificação Automatizada de Biometrias) (em inglês, *Automated Biometric Identification System*). Trata-se um sistema automatizado de reconhecimento de padrões biométricos, sendo usado para comparar um traço biométrico

com *templates* previamente arquivados no banco de dados do sistema. Portanto, quando se diz, por exemplo, que uma impressão digital está armazenada em um banco de dados de um ABIS, não necessariamente a imagem da impressão está arquivada. Usualmente, o ABIS guarda apenas o *template* (modelo), que é uma coleção de informações obtidas através dos pontos característicos encontradas na impressão, que permitem classificá-las como únicas, separando-as por indivíduo.

2.1 Captura dos Dados

Inicialmente na biometria, cada indivíduo deve ser cadastrado no sistema. Esse processo consiste na captura e armazenamento de um traço biológico do indivíduo que é usado posteriormente no processo de identificação. A Figura 2 ilustra o subsistema de detecção e aquisição de dados biométricos (Modi, 2011).

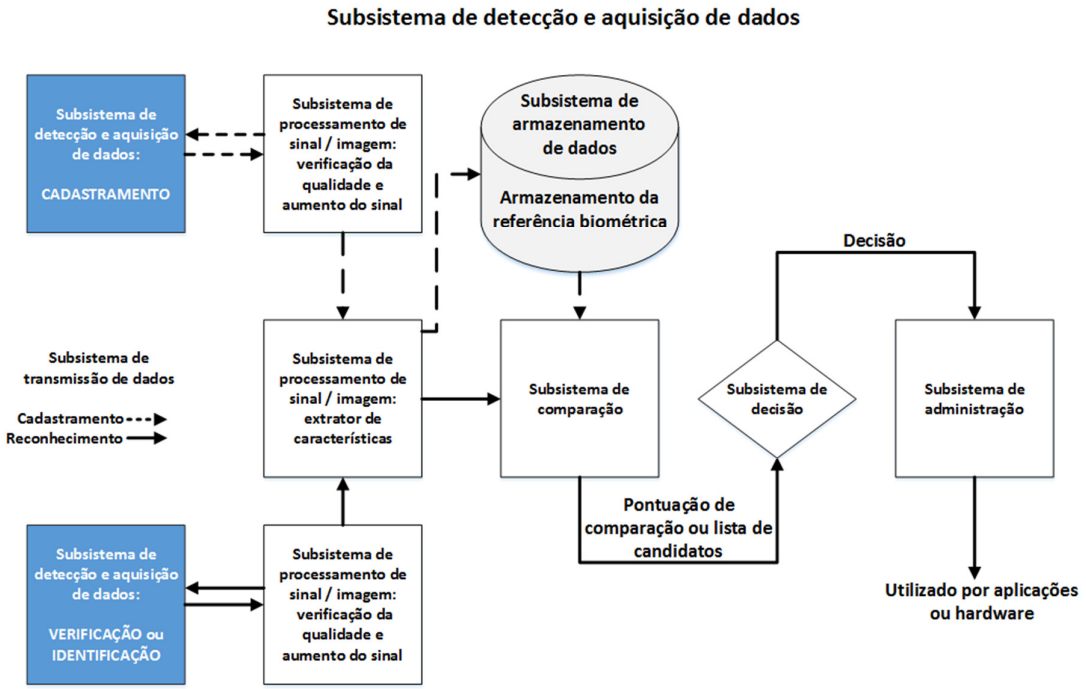

Figura 2 – Captura dos dados

(Adaptado de: MODI, Shimon K. Biometrics in Identity Management: Concepts to Applications. Artech House, 2011.)

A característica biológica é tipicamente adquirida por um dispositivo de *hardware*, conhecido como sensor. A aquisição é a etapa origem da maioria dos erros nos sistemas

biométricos, já que erros na aquisição dos dados biométricos normalmente propagam-se ao resto do sistema e incrementa a possibilidade de falha no sistema em geral. Como se pode ver, a captura dos dados é realizada tanto no processo de cadastramento quanto no processo de verificação/identificação.

2.1.1 Arquivo de saída

O arquivo de saída da etapa de captura dos dados depende basicamente do tipo de sensor utilizado no procedimento de coleta, como comentado anteriormente. Portanto, pode-se gerar uma imagem bruta do traço biométrico assim como um *template*, que é a imagem processada. As figuras 3, 4 e 5 ilustram alguns exemplos de imagens brutas resultantes da saída do sensor. O *template* e seu formato será tratado mais adiante nesse relatório, na seção de processamento.

A imagem bruta normalmente está nos formatos png, tif ou gif. O tamanho médio da imagem bruta (ainda não processada) varia entre 10 KB a 260 KB, dependendo do tipo de sensor, do traço biométrico, do padrão de qualidade adotado, entre outros fatores.

Figura 3 – Exemplos de imagem bruta de saída do processo de coleta de uma impressão digital

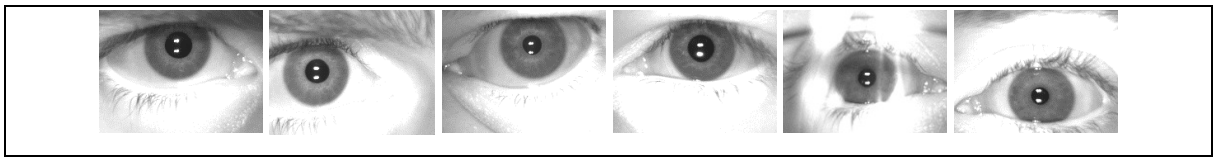

Figura 4 – Exemplos de imagem bruta de saída do processo de coleta de uma íris

Figura 5 – Exemplos de imagem bruta de saída do processo de coleta da face

A Tabela 2 resume o tamanho médio da imagem bruta após a captura dos dados pelo sensor biométrico.

Biometria	Tamanho da imagem (bruta)	Fonte
Face	10 a 20 KB	ATT, The Database of Faces[1]
Impressão Digital	70 a 120 KB	CrossMatch Sample DB[2]
Íris	170 a 260 KB	Neurotechnology, Sample Iris Database[3]

Tabela 2 - Tamanho médio da imagem (bruta) após a captura dos dados

2.2 Processamento

Devido ao fato dos sinais produzidos pela grande maioria dos sensores serem analógicos, é necessário convertê-los em digitais, para que dessa forma, possam ser processados por um computador. Assim, no processo de captura de dados, o processamento dos dados é realizado tanto no cadastramento quanto no processo de verificação/identificação, conforme ilustra a Figura 6.

[1] http://www.cl.cam.ac.uk/research/dtg/attarchive/facedatabase.html
[2] http://www.neurotechnology.com/download.html
[3] http://www.neurotechnology.com/download.html

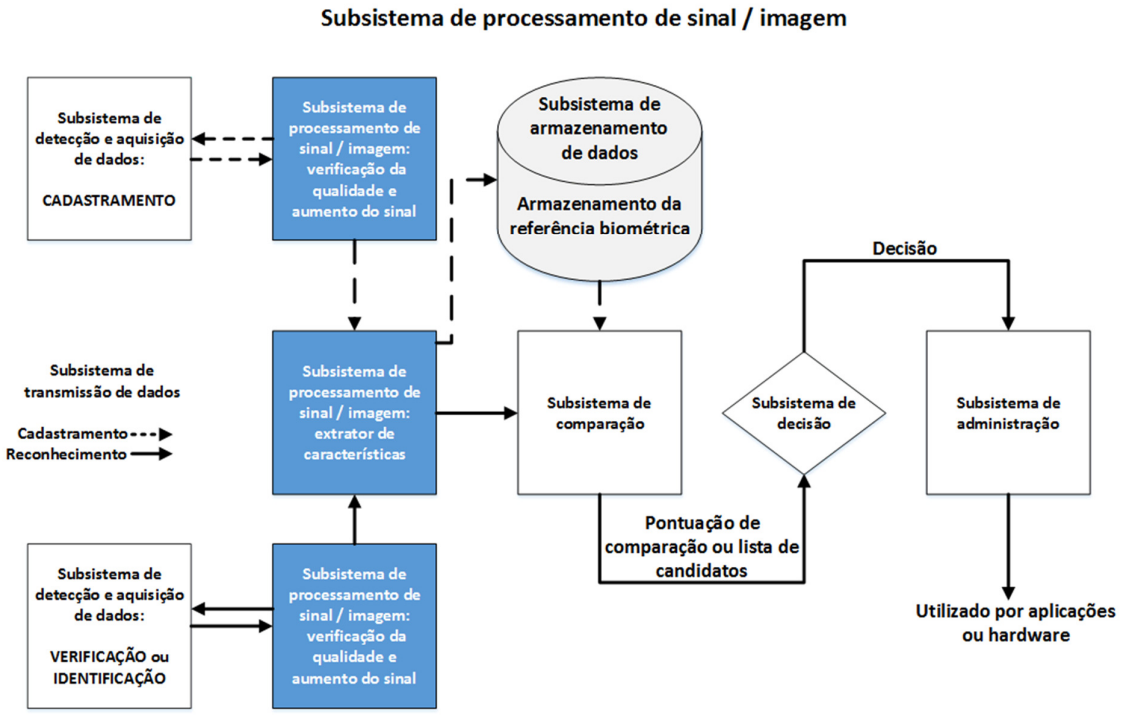

Figura 6 – Processamento dos dados

Na etapa de processamento são realizadas as seguintes atividades.

- Pré-processamento: algoritmos de melhoramento da imagem (detecção, alinhamento, segmentação, etc.)
- Controle de qualidade
- Extração das características para a geração do *template*
- Categorização e pós-processamento
- Compressão dos dados (caso haja necessidade)

É nessa etapa que é gerado o *template* biométrico (amostra), que é posteriormente utilizado no processo de reconhecimento (verificação/identificação) do indivíduo. O *template* da impressão digital é definido seguindo um formato de intercâmbio de dados que mantém as características extraídas no procedimento de cadastramento. As características mais distintivas de impressões digitais são conhecidas como minúcias.

Para que haja interoperabilidade entre diferentes sistemas de identificação biométrica, o NIST definiu um padrão para o formato das minúcias do *template*, no documento ISO/IEC 19794-2. Esse padrão estabelece a estrutura básica do *template* assim como informações

consideradas como dados extras. No documento define-se como determinar o tipo de minúcia, a localização e a direção. A Figura 7 ilustra o formato de um *template* de uma impressão digital.

			Field	Size	Valid Values and Notes
Finger Minutiae Record	Record Header		Format ID	4 bytes	'F' 'M' 'R' 0
			...		
			Image Horizontal Size	2 bytes	in pixels
			Image Vertical Size	2 bytes	in pixels
			Horizontal Resolution	2 bytes	in pixels per cm
			Vertical Resolution	2 bytes	in pixels per cm
			Number of Finger Views n_V	1 byte	0 to 255
			...		
	Single Finger Record (n_V instances)	Finger Header	Finger Position	1 byte	0 to 10
			View Number	4 bits	0 to 15
			...		
			Number of Minutiae n	1 byte	0 to 255
		Finger Minutia Record (n instances)	Type	2 bits	{00=other, 01=termination, 10=bifurcation}
			Position x	14 bits	in pixels
			Reserved	2 bits	
			Position y	14 bits	in pixels
			Direction θ	1 byte	0 to 255 (resolution 1.40625 degrees)
			Quality	1 byte	1 to 100 (0=quality not reported)
		Extended Data	Extended Data Block Length	2 bytes	
		Extended Data (0+ inst.)	Extended Data Area Type Code	2 bytes	only present if Extended Data Block Length>0
			Extended Data Area Length	2 bytes	
			Data Section	(prev. field)	

Figura 7 – Formato de um *template* segundo a norma ISO/IEC 19794-2.

2.2.1 Arquivo de saída (*template*)

A Figura 8 mostra uma tabela que armazena um *template* biométrico, do tipo BLOB. O tamanho médio de um *template* para impressão digital varia entre 3 KB a 6 KB, dependendo do tipo de sensor, do algoritmo de extração das características, entre outros fatores.

Name	Type	Schema
Tables (1)		
Subjects		CREATE TABLE "Subjects" (Id INTEGER PRIMARY KEY, SubjectId TEXT NOT NULL UNIQUE, Template BLOB NOT NULL...
Id	INTEGER	
SubjectId	TEXT	
Template	BLOB	
Thumbnail	BLOB	

Figura 8 – Estrutura do *template*

A Figura 9 mostra um exemplo de uma estrutura de um *template* biométrico de uma impressão digital, já em seu formato hexadecimal.

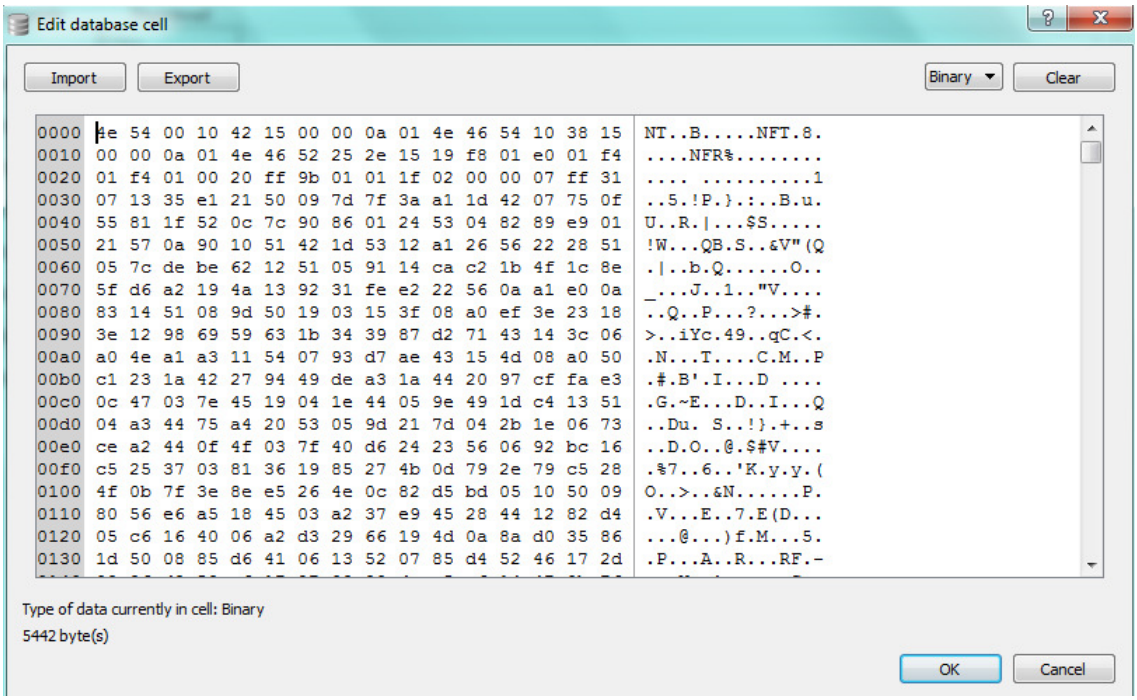

Figura 9 – Dados do *template*

2.3 Armazenamento dos Dados

Uma vez que a representação digital é gerada na etapa anterior, essa informação deve ser armazenada. A característica biológica armazenada na forma digital é conhecida como modelo (*template*). Vários dispositivos biométricos podem realizar a captura simultânea de múltiplas características (por exemplo, face e íris) durante o processo de aquisição para contabilizar graus de variação na medida destas características. Uma vez que o indivíduo é registrado e seus dados biométricos são armazenados no sistema, os dispositivos biométricos são usados na verificação ou identificação do indivíduo, conforme ilustra a Figura 10.

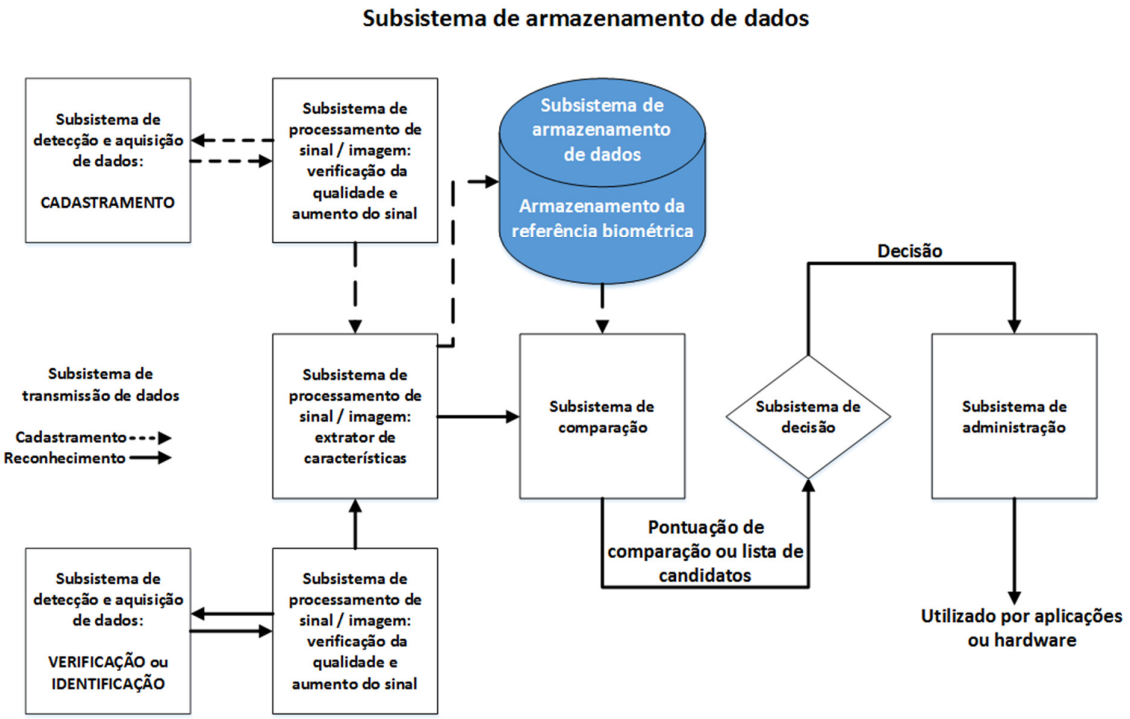

Figura 10 – Armazenamento dos dados

O armazenamento de informação biométrica ocorre somente na etapa de cadastramento do indivíduo, na qual é realizada a coleta dos dados biográficos e biométricos (imagem bruta do sensor). Entretanto, é importante saber como o processo de verificação e identificação usa essa informação previamente coletada na etapa de cadastramento.

No cadastramento, usa-se normalmente os sensores puros, os quais geram a imagem bruta dos traços biométricos coletados. Além da imagem bruta, o *software* de processamento realiza a geração do *template* do traço biométrico, o qual também será armazenado, sendo utilizado no processo de verificação. Os dados brutos e os *templates* são armazenados em bancos de dados diferentes. Isso se deve ao fato de que o dado bruto não é utilizado periodicamente, sendo útil para geração de novo *template*, ou para outros fins. Além disso, o dado bruto ocupa mais espaço em disco e recomenda-se seu armazenamento em um servidor que não tenha dispositivos de comunicação. Por outro lado, o *template* ocupa pouco espaço em disco e pode ser acessado milhares de vezes devido para fins de autenticação, necessitando de um armazenamento que oferece alta performance.

2.4 Verificação / Identificação

Definem-se dois modos de reconhecimento em sistemas biométricos: verificação e identificação. Em modo de verificação (sistema 1:1), o sistema deve responder se o usuário é quem ele declara ser. Em modo de identificação (sistema 1:N) o sistema deve determinar quem é o usuário, dentro de N possíveis identidades.

No momento do reconhecimento do indivíduo, o traço biométrico é lido pelo sensor e a informação analógica fornecida é convertida em digital que, por sua vez, é comparada com a amostra biométrica armazenada (*template*). Tipicamente, a amostra coletada não é exatamente igual à amostra armazenada, devido à ocorrência, normalmente, de variações na leitura. O algoritmo de comparação produz um resultado, informando o grau de similaridade com a amostra armazenada. Caso o resultado apresente um valor dentro do limiar de confiança, o usuário então é autenticado e recebe uma resposta afirmativa do sistema.

Devido a esse fato, são de extrema importância a definição e a configuração do limiar na etapa de decisão, valor este que pode ser ajustado e adaptado de acordo com as necessidades do sistema de identificação biométrica.

De forma mais detalhada, os dois processos de reconhecimento são os seguintes.

Verificação (1:1): é um processo de comparação de um-para-um (1:1) e funciona realizando a comparação entre a amostra coletada e a amostra armazenada no banco de dados. Na verificação, normalmente, se utilizam sensores que realizam a geração do *template* já no momento da captura, sendo enviado apenas o *template* para a comparação. Isso possibilita uma comparação mais rápida dos *templates*, além de ter menor consumo de banda na comunicação dos dados. A localização do registro da pessoa é feita por meio da comparação de outro campo, como o nome ou qualquer outro dado biográfico. Após localizado, o indivíduo tem sua identidade confirmada. A Figura 11 ilustra o processo de verificação, segundo (Modi, 2011).

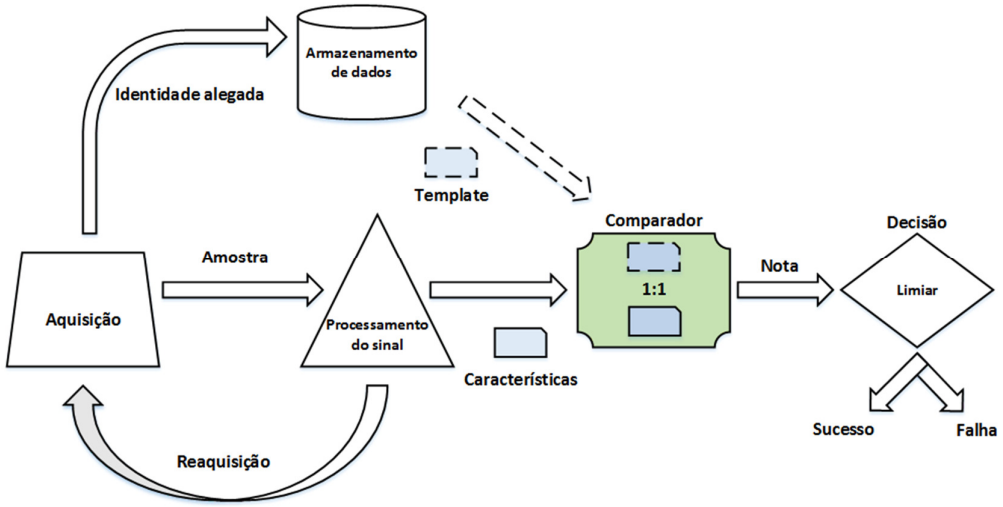

Figura 11 – Processo de verificação (1:1)

Identificação (1:N): é um processo de combinação de um-para-muitos (1:N). O indivíduo não precisa confirmar quem é. A sua amostra biométrica é tomada e comparada a todas existentes na base de dados registrada ou arquivada. Em alguns casos, o sistema não consegue identificar apenas um indivíduo, e sim uma lista de candidatos que possuem as características mais próximas à amostra coletada. Quando é encontrada a melhor combinação, o indivíduo é "identificado" como um indivíduo pré-existente, ou seja, o sistema finalmente encontra a quem pertence a amostra biométrica coletada. Esse é considerado o método mais complexo, pois, o *software* deverá identificar pontos de coincidência de uma imagem em um banco de dados contendo todos os *templates* armazenados no sistema. Isso faz com que sejam consumidos maiores recursos do sistema.

A Figura 12 ilustra o processo de identificação, segundo (Modi, 2011).

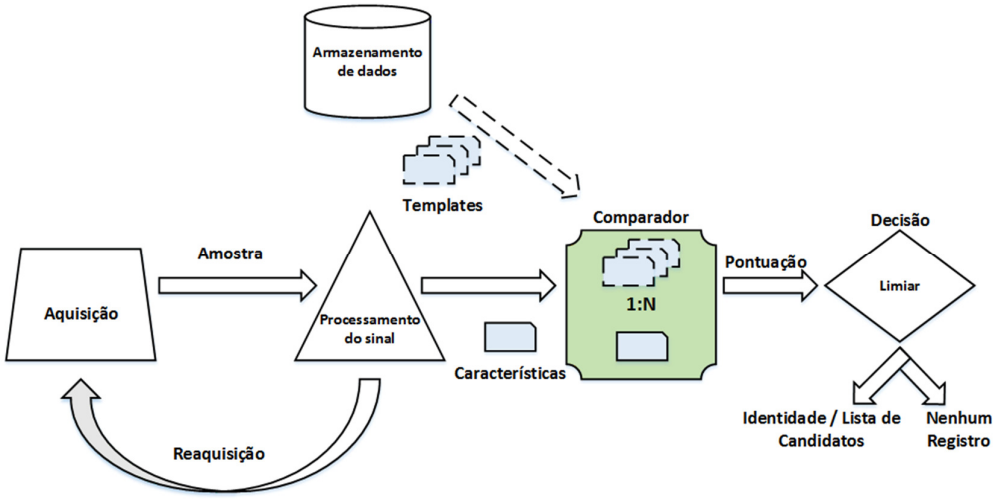

Figura 12 – Processo de identificação (1:N)

Outro conceito que tem ganhado notoriedade nos últimos anos, chama-se de-duplicação. O conceito de de-duplicação refere-se ao processo de examinar, durante o procedimento de cadastramento, se a amostra biométrica que está sendo cadastrada tem alguma amostra correspondente em todo o banco de dados já existente. Desta forma, a amostra e comparada as “N” amostras já cadastradas, uma a uma.

Caso exista alguma amostra correspondente, o indivíduo não é cadastrado, e, portanto, não recebe uma nova identidade a fim de evitar uma entrada duplicada. Caso não exista amostra correspondente, o usuário é cadastrado de forma correta e um número único é associado a amostra apresentada pelo indivíduo (Decann, 2013).

O processo de de-duplicação é necessário para garantir que todos os indivíduos da população tenham apenas um único número no banco de dados. Por exemplo, uma entrada duplicada pode ser criada intencionalmente por um impostor para futuramente fraudar o sistema e obter algum benefício utilizando a identidade de outro indivíduo. Outro exemplo refere-se a ação de um indivíduo tentando se cadastrar duas vezes com números de identidade diferentes.

O conceito de de-duplicação é especialmente utilizado em programas de identificação civil de grande escala como o caso da Índia, México e Indonésia, com enormes bases de dados que precisam garantir a unicidade dos indivíduos cadastrados.

A de-duplicação também pode ser considerada um processo de identificação, no qual é feita uma comparação 1:N. Entretanto, para cada indivíduo que está sendo cadastrado é

realizada uma comparação, o que exige alto poder de processamento do sistema.

Como exemplo da complexidade dessa operação, a Índia cadastra, diariamente, 1 milhão de indivíduos[4], os quais são comparados com os 650 milhões já cadastrados[5], gerando mais de 500 trilhões de comparações por dia.

2.5 Decisão

Após o processo de verificação / identificação, o algoritmo de comparação produz um resultado, informando o grau de similaridade com a amostra armazenada. Caso o resultado apresente um valor dentro do limiar de confiança, o usuário então é autenticado e recebe uma resposta afirmativa do sistema. O limiar de confiança pode ser configurado pelo administrador do sistema biométrico, aumentando ou diminuindo o nível do valor de aceitação. Caso esse valor seja muito baixo, o sensor biométrico autentica indivíduos incorretamente. Por outro lado, caso esse valor seja muito alto, os indivíduos genuínos podem ter problemas na autenticação.

Devido a esse fato, são de extrema importância a definição e a configuração do limiar na etapa de decisão, valor este que pode ser ajustado e adaptado de acordo com as necessidades do sistema de identificação biométrica.

2.6 Considerações Finais

Esta seção objetivou apresentar os processos do sistema de reconhecimento biométrico: aquisição, processamento, armazenamento, verificação / identificação e decisão. A descrição de cada uma das etapas visou aclarar a importância do processo de coleta dos dados biométricos, a geração do *template*, como é realizado o processo de armazenamento, a diferença entre verificação (1:1) e identificação (1:N) e finalmente o mecanismo de decisão.

O sucesso ou a negação da autenticação de um indivíduo em um sistema biométrico depende da configuração apropriada em cada uma das etapas mencionadas.

[4] http://pt.slideshare.net/regunathbalasubramanian/aadhaar-at-5thelephantv3
[5] https://portal.uidai.gov.in/uidwebportal/dashboard.do

3. LOCAIS DE ARMAZENAMENTO DE DADOS BIOMÉTRICOS

Os dados biométricos podem ser armazenados em diferentes localidades. Entre as mais comuns estão os seguintes (Modi, 2011).

- Centralizado
- Descentralizado
- Cliente
- Sensor
- Dispositivo portátil

3.1 Que tipo de dados armazenar?

Vários são os arquivos que podem ser armazenados em um banco de dados biográfico/biométrico. A Tabela 3 ilustra essas opções, de acordo com o IEEE[6].

Dados	Exemplos	Desafios
Biométricos	▪ *Template* ▪ Modelos ▪ Imagens	▪ Quantidade de acessos simultâneos
Biográficos	▪ Nome ▪ Identificador ▪ Sexo, idade, etc. ▪ Endereço ▪ Representador	▪ Documentos falsos ▪ Gerência de uma base de dados separada dos dados biométricos ▪ Tamanho dos arquivos digitalizados
Brutos	▪ Imagem bruta do sensor	▪ Tamanho do arquivo ▪ Segurança e privacidade ▪ Uso além do estipulado originalmente
Logs	▪ Transações biométricas ▪ Eventos ▪ Meta-dados	▪ Rastreamento inadequado de pessoas ▪ Uso inadequado dos dados

[6] http://www.ieeebiometricscertification.org/ieee-cbp-training

Tabela 3 - Tipos de dados que podem ser armazenados

3.2 Centralizado

O armazenamento dos dados biométricos e/ou biográficos pode ser feito em uma base centralizada, isto é, toda a informação estaria armazenada em um único local físico. A Tabela 4 ilustra as vantagens e desvantagens dessa opção de armazenamento.

Vantagens	Desvantagens
▪ Sem redundância dos dados, facilitando a gerência dos dados ▪ Possibilidade de reconhecimento biométrico remoto ▪ Política de segurança centralizada ▪ Gerenciamento local ▪ Facilidade de recuperação dos dados biométricos de referência	▪ Velocidade de transmissão / possível gargalo ▪ Número de transações simultâneas ▪ Dependência da rede de transmissão ▪ Risco de roubo massivo de informação ▪ Risco de roubo das informações brutas das biometrias

Tabela 4 - Armazenamento centralizado

O armazenamento centralizado pode vir a ser utilizado no projeto RIC, dependendo basicamente da quantidade de parceiros tecnológicos envolvidos na implantação do sistema.

3.3 Descentralizado

O armazenamento dos dados biométricos e/ou biográficos pode ser feito em uma base descentralizada, isto é, a informação estaria armazenada em diferentes localidades. A Tabela 5 ilustra as vantagens e desvantagens dessa opção de armazenamento.

Vantagens	Desvantagens
▪ Federação de dados ▪ Diminuição da latência no processo de reconhecimento ▪ Flexibilidade e escalabilidade na autenticação	▪ Redundância ▪ Riscos de segurança na sincronização das informações entre servidores geo-localizados ▪ Manutenção das bases de dados ▪ Maior número de pontos críticos de falhas de segurança

Tabela 5 - Armazenamento descentralizado

O armazenamento descentralizado pode vir a ser utilizado no projeto RIC, dependendo basicamente da quantidade de parceiros tecnológicos envolvidos na implantação do sistema.

3.4 Cliente

O armazenamento dos dados biométricos e/ou biográficos pode ser feito diretamente no cliente. A Tabela 6 ilustra as vantagens e desvantagens dessa opção de armazenamento.

Vantagens	Desvantagens
▪ Útil para sistemas de controle de acesso, como laptops ▪ Pouco espaço de armazenamento	▪ Base de dados limitada ▪ Segurança dos dados

Tabela 6 - Armazenamento no cliente

O armazenamento no cliente não é adequado para o projeto RIC, por diversos fatores como: base de dados limitada, pouca escalabilidade, segurança da informação, entre outros.

3.5 Sensor

O armazenamento dos dados biométricos e/ou biográficos pode ser feito diretamente

no sensor. A Tabela 7 ilustra as vantagens e desvantagens dessa opção de armazenamento.

Vantagens	Desvantagens
▪ Sistema com resposta rápida ▪ Solução eficaz e barata para sistemas de pequena escala ▪ Baixo risco de roubo de informações	▪ Requer integração dos múltiplos sensores (fechaduras, portas, catracas, etc.) ▪ Dificuldade de manutenção ▪ Base de dados limitada

Tabela 7 - Armazenamento no sensor

O armazenamento no sensor é inviável para o projeto RIC, por diversos fatores como: base de dados limitada, pouca escalabilidade, segurança da informação, dificuldade de manutenção, entre outros.

3.6 Dispositivo Portátil

O armazenamento dos dados biométricos e/ou biográficos pode ser feito em um dispositivo portátil. A Tabela 8 ilustra as vantagens e desvantagens dessa opção de armazenamento.

Vantagens	Desvantagens
▪ Melhor mobilidade e flexibilidade do que bases de dados centralizadas ▪ Alto nível de segurança (pode-se necessitar um leitor de cartão para obter as informações no interior do dispositivo) ▪ Usuário se sente no controle dos dados biométricos pessoais ▪ Evita o custo de manutenção de uma base de dados ▪ Oferece o modo de verificação com o uso de autoridade certificadora ▪ Embalagem ou dispositivo inviolável	▪ Manutenção de cartões roubados e duplicados sem a existência de uma base central ▪ Custo de emissão de cartões biométricos (perdidos e/ou cancelados) pode ser relativamente alto ▪ Pode-se fazer uso de imagens digitais de outros indivíduos caso não exista assinatura digital ou outro mecanismo de segurança.

Tabela 8 - Armazenamento no dispositivo portátil

O armazenamento no cliente pode vir a ser utilizado no projeto RIC, caso sejam utilizados cartões inteligentes com chip. Entretanto, é uma opção que deve ser muito bem avaliada, principalmente relacionada aos aspectos de segurança.

3.7 Considerações Finais

Esta seção objetivou apresentar os locais mais comuns de armazenamento de dados biográficos e biométricos. Foram vistos quais os tipos de dados que podem ser armazenados, seus desafios de implantação e verifica-se que tanto o armazenamento centralizado como o descentralizado podem ser utilizados no projeto RIC, dependendo basicamente da quantidade de parceiros tecnológicos que farão parte da implantação dos sistemas do projeto RIC.

4. PADRÕES DE ARMAZENAMENTO DE DADOS BIOMÉTRICOS

Normas e padrões são muito importantes no âmbito da biometria, tendo um papel fundamental na adoção e na implementação de tecnologias biométricas. Do ponto de vista técnico, padrões asseguram interoperabilidade entre produtos e processos. A padronização incrementa a confiança dos indivíduos, criando um mercado para a indústria, sendo também um indicativo da maturidade da tecnologia (Fernando Podio, 2013Fernando Podio, 2013).

O rápido desenvolvimento de tecnologias biométricas e a implementação de sistemas de identificação biométricos de grande escala geram questões críticas como a dependência de um único fabricante, interoperabilidade entre equipamentos, garantia, compatibilidade futura com as normas, entre outras questões. A utilização de normas e padrões reduz os riscos mencionados além de levar a uma popularização da tecnologia, aumentando a concorrência entre fabricantes, reduzindo preços de equipamentos e promovendo a inovação do setor. A seguir, são apresentadas as normas e padrões biométricos mais difundidas.

4.2 ISO/IEC

O organismo ISO (*International Organization for Standardization*) juntamente com a IEC (*International Electrotechnical Comission*) criaram em conjunto um comitê chamado JTC (*Joint Technical Committee*) 1, responsável pela criação de normas e padrões. Em junho de 2002, foi criado um subcomitê para o desenvolvimento de padrões de biometria, o ISO/IEC JTC 1/SC 37[7], conforme organograma ilustrado na Figura 13.

Com o crescente interesse dos países pela adoção da biometria em sistemas de identificação, o SC 37 cresceu rapidamente nos últimos anos, contando com a participação de 28 países como membros participantes (África do Sul, Alemanha, Austrália, Cingapura, China, Coréia, Dinamarca, Egito, Espanha, Estados Unidos, França, Finlândia, Índia, Israel, Itália, Japão, Malásia, Nova Zelândia, Noruega, Polônia, Portugal, Rússia, Reino Unido, República Checa, Suécia, Suíça, Tailândia e Ucrânia,) e 13 como países observadores (Áustria, Bélgica, Bósnia, Canada, Gana, Holanda, Hungria, Indonésia, Irã, Irlanda, Quênia,

[7] http://www.iso.org/iso/home/standards_development/list_of_iso_technical_committees/iso_technical_committee_participation.htm?commid=313770

Romênia e Sérvia).

Dentro da própria ISO, existem outros comitês técnicos que estão envolvidos com biometria, como por exemplo:

- TC68 (*Financial Services*);
- SC17 (*Cards & Personal Identification*) ;
- SC27 IT (*Security Techniques*).

O subcomitê JTC1 SC37 mantém uma estreita relação com os subcomitês mencionados anteriormente para uma coordenação das forças-tarefas, evitando trabalho duplicado.

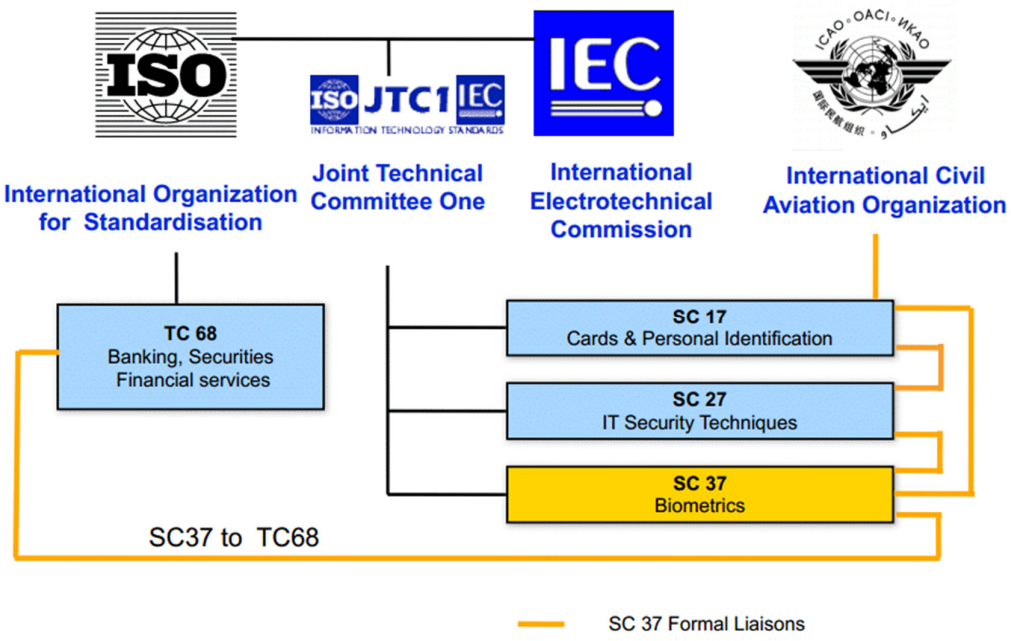

Figura 13 - Comitês ISO IEC

Fonte: http://www.iso.org/iso/iso_technical_committee.html?commid=313770

O subcomitê SC 37 está dividido nos seguintes seis grupos de trabalho[8] (*WG – Working Groups*), (Figura 14).

[8] http://www.iso.org/iso/iso_technical_committee.html?commid=313770

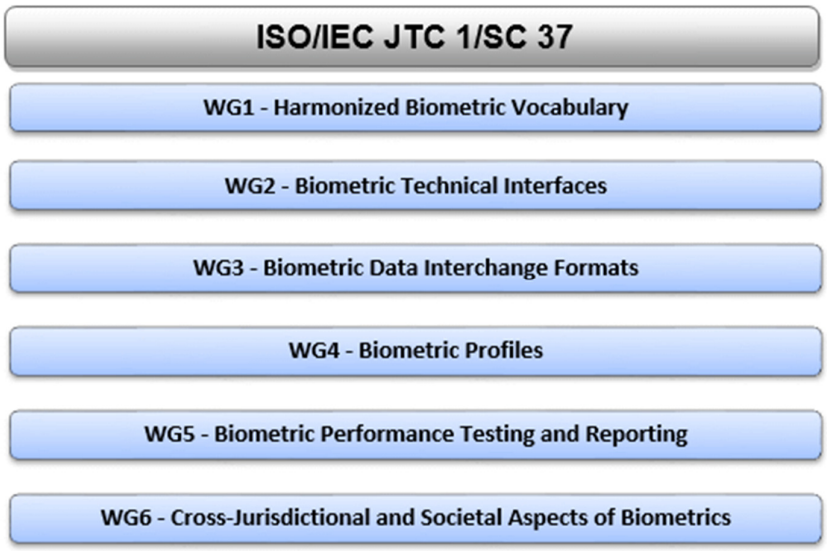

Figura 14 – Subcomitês ISO/IEC JTC 1/SC 37

WG1 (*Harmonized Biometric Vocabulary*): estabelece uma descrição sistemática dos conceitos no campo da biometria relativos ao reconhecimento dos seres humanos e normaliza termos variantes em uso nos padrões biométricos pré-existentes esclarecendo, assim, o uso de termos neste campo.

WG2 (*Biometric Technical Interfaces*): aborda as interfaces e interações necessárias entre os componentes biométricos e subsistemas, bem como a possível utilização de mecanismos de segurança para proteger os dados armazenados e os dados transferidos entre sistemas.

WG3 (*Biometric Data Interchange Formats*): especifica o conteúdo, significado e representação do formato de dados biométricos, que são específicos para uma biometria dada. Padrões de qualidade da amostra biométrica e relatórios técnicos: especifica termos e definições que são úteis para a especificação, utilização e controle de qualidade das imagens e define o propósito, intenção e interpretação dos índices de qualidade de imagem para uma modalidade biométrica. Neste subcomitê se encontram as normas ISO/IEC 19794, sendo as mais utilizadas pelos países nos sistemas de identificação.

WG4 (*Biometric Profiles*): une os vários padrões de base biométrica de uma maneira

consistente e desenvolve relatórios técnicos de apoio à implementação de tecnologias biométricas.

WG5 (*Biometric Performance Testing and Reporting*): especifica métricas de cálculo de desempenho de biometrias, abordagens para testes de desempenho e requisitos para validação dos resultados dos testes.

WG6 (*Cross-Jurisdictional and Societal Aspects of Biometrics*): aborda as aplicações das tecnologias biométricas, especificamente no que diz respeito à acessibilidade, saúde e segurança e suporte a requisitos legais.

Em janeiro de 2014, o ISO/IEC JTC 1/SC 37 tinha 87 normas publicadas (incluindo emendas) em biometria[9]. As Tabelas 9 a 14 a listam os padrões publicados pela ISO / IEC JTC 1/SC 37 que estão divididos pelos grupos de trabalho.

Número	Título
ISO/IEC 2382-37:2012	Information technology -- Vocabulary -- Part 37: Biometrics

Tabela 9 - Grupo de trabalho 1 (WG1) da norma ISO/IEC JTC 1/SC 37

Número	Título
ISO/IEC 19784-1:2006	Biometric application programming interface -- Part 1: BioAPI specification
ISO/IEC 19784-1:2006/Amd 1:2007	BioGUI specification
ISO/IEC 19784-1:2006/Amd 2:2009	Framework-free BioAPI
ISO/IEC 19784-1:2006/Amd 3:2010	Support for interchange of certificates and security assertions, and other security aspects
ISO/IEC 19784-2:2007	BioAPI - Part 2: Biometric archive function provider interface
ISO/IEC 19784-4:2011	BioAPI - Part 4: Biometric sensor function provider interface
ISO/IEC 19785-1:2006	Common Biometric Exchange Formats Framework Part 1: Data element specification
ISO/IEC 19785-2:2006	Part 2: Procedures for the operation of the Biometric Registration Authority
ISO/IEC 19785-3:2007	Part 3: Patron format specifications
ISO/IEC 19785-4:2010	Part 4: Security block format specifications
ISO/IEC 24708:2008	BioAPI Interworking Protocol

9 http://www.iso.org/iso/home/standards_development/list_of_iso_technical_committees/iso_technical_committee.htm?commid=313770

ISO/IEC 24709-1:2007	Conformance testing for the BioAPI Part 1: Methods and procedures
ISO/IEC 24709-2:2007	Part 2: Test assertions for biometric service providers
ISO/IEC 24709-3:2011	Part 3: Test assertions for BioAPI frameworks
ISO/IEC 29141:2009	Tenprint capture using BioAPI

Tabela 10 - Grupo de trabalho 2 (WG2) da norma ISO/IEC JTC 1/SC 37

Número	Título
ISO/IEC 19794-1:2011	Biometric data interchange formats Part 1: Framework
ISO/IEC 19794-2:2011	**Part 2: Finger minutiae data**
ISO/IEC 19794-3:2006	Part 3: Finger pattern spectral data
ISO/IEC 19794-4:2011	**Part 4: Finger image data**
ISO/IEC 19794-5:2011	**Part 5: Face image data**
ISO/IEC 19794-6:2011	**Part 6: Iris image data**
ISO/IEC 19794-7:2007	Part 7: Signature/sign time series data
ISO/IEC 19794-8:2011	Part 8: Finger pattern skeletal data
ISO/IEC 19794-9:2011	Part 9: Vascular image data
ISO/IEC 19794-10:2007	Part 10: Hand geometry silhouette data
ISO/IEC 19794-11:2013	Part 11: Signature/sign processed dynamic data
ISO/IEC 19794-14:2013	Part 14: DNA data
ISO/IEC 29109-1:2009	Conformance testing methodology for biometric data interchange formats defined in ISO/IEC 19794
ISO/IEC 29159-1:2010	Biometric calibration, augmentation and fusion data -- Part 1: Fusion information format

Tabela 11 - Grupo de trabalho 3 (WG3) da norma ISO/IEC JTC 1/SC 37

Número	Título
ISO/IEC 24713-1:2008	Biometric profiles for interoperability and data interchange Part 1: Overview of biometric systems and biometric profiles
ISO/IEC 24713-2:2008	Part 2: Physical access control for employees at airports
ISO/IEC 24713-3:2009	Part 3: Biometrics-based verification and identification of seafarers

Tabela 12 - Grupo de trabalho 4 (WG4) da norma ISO/IEC JTC 1/SC 37

Número	Título
ISO/IEC 19795-1:2006	Biometric performance testing and reporting Part 1: Principles and framework
ISO/IEC 19795-2:2007	Part 2: Testing methodologies for technology and scenario evaluation
ISO/IEC TR 19795-3:2007	Part 3: Modality-specific testing
ISO/IEC 19795-4:2008	Part 4: Interoperability performance testing
ISO/IEC 19795-5:2011	Part 5: Access control scenario and grading scheme
ISO/IEC 19795-6:2012	Part 6: Testing methodologies for operational evaluation
ISO/IEC 19795-7:2011	Part 7: Testing of on-card biometric comparison algorithms
ISO/IEC DIS 29120-1.2	Machine readable test data for biometric testing and reporting -- Part 1: Test reports
ISO/IEC CD 29120-2	Machine Readable Test Data for biometric testing and reporting -- Part 2: Test Input Data

Tabela 13 - Grupo de trabalho 5 (WG5) da norma ISSO/IEC JTC 1/SC 37

Número	Título
ISO/IEC TR 24741:2007	Biometrics tutorial
ISO/IEC DIS 24779-1	Cross jurisdictional and societal aspects of implementation of biometric technologies -- Pictograms, icons and symbols for use with biometric systems Part 1: General principles
ISO/IEC CD 24779-2	Part 2: Fingerprint applications
ISO/IEC CD 24779-4	Part 4: Fingerprint application
ISO/IEC DIS 24779-9	Part 9: Vascular applications
ISO/IEC PDTR 29194	Biometrics - Guide on designing accessible and inclusive biometric systems

Tabela 14 - Grupo de trabalho 6 (WG6) da norma ISO/IEC JTC 1/SC 37

4.3 BioAPI

O consórcio BioAPI (*Biometric Application Programming Interface*)[10] foi fundado em 1998 e está formado por vários fabricantes de equipamentos, institutos de pesquisa, universidades e agências governamentais. O consórcio define um conjunto de interfaces em nível de programação, o qual permite a interação entre diferentes sistemas biométricos

[10] http://www.bioapi.org/

independentemente da tecnologia utilizada e reduz a complexidade no desenvolvimento de aplicações biométricas. O consórcio está atualmente inserido dentro do comitê SC 37, no subgrupo WG2.

4.4 NIST

O Instituto Nacional de Padrões e Tecnologia (NIST - *National Institute of Standards and Technology*) é uma agência governamental não-regulatória da administração de tecnologia do Departamento de Comércio dos Estados Unidos. A missão do instituto é promover a inovação e a competitividade industrial dos Estados Unidos, promovendo normas e padrões internacionais.

A primeira norma de biometria criada pelo NIST foi em 1986 no Laboratório de Tecnologia da Informação (ITL – *Information Technology Laboratory*)[11] para facilitar a troca de imagens de impressões digitais, face e outras biometrias. A norma é conhecida como "*ANSI/NIST-ITL Standard Data Format for the Interchange of Fingerprint, Facial, and Other Biometric Information – Part 1*". Essa norma passou por revisões nos anos 1993, 1997, 2000, 2007 e 2011. A versão corrente da norma é a **ANSI/NIST-ITL 2011** e incorpora intercâmbio de dados para impressão digital, face, palma da mão, íris, cicatrizes, tatuagens e outras futuras modalidades[12]. Entre as entidades que utilizam as normas do NIST estão o FBI (*Federal Bureau of Investigation*), o Departamento de Defesa dos EUA e a Interpol.

4.5 Considerações Finais

Esta seção objetivou apresentar as normas e padrões biométricos mais conhecidos e utilizados atualmente. A utilização de normas e padrões reduz os riscos no momento da implementação de um sistema de identificação biométrico de grande escala evitando a dependência de um único fabricante, garantindo a interoperabilidade entre equipamentos e, assegurando a compatibilidade futura com as normas, entre outras questões. A padronização é de suma importância para a adoção de uma tecnologia. Quaisquer que

[11] http://www.nist.gov/itl/
[12] Data Format for the Interchange of Fingerprint Facial, & Other Biometric Information - Part 1 (ANSI/NIST-ITL 1-2011).

sejam as biometrias utilizadas no RIC, estas devem ser embasadas em padrões aceitos internacionalmente.

5. CONCLUSÃO

Apresentados os conceitos básicos sobre os processos de um sistema biométrico com ênfase na parte de armazenamento dos dados, pode-se nesse momento, fazer algumas recomendações e conclusões sobre o armazenamento biométrico para o projeto RIC.

O ponto a ser enfatizado é a distinção dos requisitos tecnológicos nas etapas de cadastramento e reconhecimento do indivíduo. Cada um desses processos tem sua própria necessidade em termos de sistemas, infraestrutura, comunicação, etc. A Tabela 15 resume as principais características das etapas de cadastramento, verificação e identificação e suas particularidades em quanto ao armazenamento de dados biométricos.

Etapa	Dados enviados	Dados armazenados	Considerações
Cadastramento	▪ Biométricos ○ Imagem bruta ○ *Template* ▪ Dados biográficos	▪ Biométricos ○ Imagem bruta ○ *Template* ▪ Dados biográficos	▪ Estima-se que o pacote de cadastramento por indivíduo seja de 4 MB. ▪ Imagem bruta e *template* são guardados em bancos de dados diferentes. ▪ Processamento off-line.
Verificação (1:1)	▪ Nome e/ou ▪ Identificador e ▪ *Template* biométrico	▪ Nenhum dado é armazenado no processo de verificação	▪ O sensor ou o software cliente realiza a geração do *template*. Um pacote de verificação pode ter aproximadamente 5K de tamanho. ▪ Processamento on-line e de baixa latência (em ordem de 200 ms).
Identificação (1:N)	▪ Imagem bruta do sensor	▪ Nenhum dado é armazenado no processo de identificação	▪ Trata-se do processo mais complexo em termos tecnológicos do projeto RIC. A varredura de um banco de dados de grande escala (200 milhões) necessita de alto poder de processamento. ▪ Processamento off-line e de alta latência.

Tabela 15 – Resumo dos modelos de armazenamento de dados biométricos

Como se pode ver na Tabela 15, somente na fase de cadastramento há armazenamento de informação. No processo de verificação e identificação há a coleta de dados, entretanto, não se armazena nenhuma informação no banco de dados. Outro fator que merece destaque é que na fase de cadastramento, a imagem bruta e o *template* são guardados em bancos de dados diferentes, devido a que possuem diferentes usos dentro do sistema de identificação civil.

Por último, ressaltar que o armazenamento dos dados biométricos em projetos de grande escala (ordem de centenas de milhões de usuários) requer especial atenção quanto à segurança da informação, visto que uma biometria não pode ser substituída por uma nova, como acontece com a substituição de um cartão que foi clonado ou senha que foi roubada. Trata-se praticamente de informação imutável.

REFERÊNCIAS BIBLIOGRÁFICAS

Anil Jain, 2007	Jain, Anil K., Patrick Flynn, and Arun A. Ross. Handbook of biometrics. Springer, 2007.
Modi, 2011	MODI, Shimon K. Biometrics in Identity Management: Concepts to Applications. Artech House, 2011.
Fernando Podio, 2013	F. Podio, "Advances in Biometric Standardisation – Addressing Global Market Requirements for Biometric Standards". International Journal of Biometrics (IJBM) 5 (1): 5–19, http://www.nist.gov/customcf/get_pdf.cfm?pub_id=909998, 2013.
Decann, 2013	DECANN, Brian; ROSS, Arun. De-duplication errors in a biometric system: An investigative study. In: Information Forensics and Security (WIFS), 2013 IEEE International Workshop on. IEEE, 2013. p. 43-48.

Universidade de Brasília – UnB
Centro de Apoio ao Desenvolvimento Tecnológico – CDT
Laboratório de Tecnologias da Tomada de Decisão – LATITUDE
www.unb.br – www.cdt.unb.br – www.latitude.eng.br