

# Biometric authentication of fingerprints obtained by photo

## Autenticação biométrica de impressões digitais obtidas por foto

João Vitor de Souza Costa<sup>1\*</sup>, Cristian Thiago Moecke<sup>1</sup>, Luciana de Oliveira Rech<sup>1</sup>

**Abstract:** In recent years, there has been an increase in the use of fingerprints for authentication and identity verification. However, this approach requires specialized and costly hardware to extract the biometric information, which hinders its popularization and makes it less accessible. Simultaneously, there has been a rise in the usage of smartphones, which, coupled with technological advancements, has allowed for the evolution of cameras in these devices, enabling them to capture high-quality photos. In this context, this project aims to create an alternative method for biometric extraction, primarily using a photo of the fingerprint taken with a smartphone. By employing a technique of capture and post-processing of photos, utilizing a series of filters, the fingerprints become more evident, facilitating their comparison with biometrics obtained from traditional biometric readers or through this alternative approach. It is important to note that, although biometric readers are increasingly common in smartphones, the operating systems of these devices do not provide APIs or interfaces for capturing biometrics for external validation, limiting identity confirmation only within a local scope due to privacy concerns. Lastly, the project proposes the development of a REST API for identity verification based on fingerprints extracted from photos or specialized biometric readers. This API has the purpose to reduce costs and facilitate access for individuals who do not possess a biometric reader.

**Keywords:** Biometric authentication — Fingerprint — Smartphone — Image processing — API REST

**Resumo:** Nos últimos anos, observou-se um aumento no uso de impressões digitais para autenticação e verificação de identidade. No entanto, essa abordagem requer hardware especializado de alto custo para extrair as informações biométricas, o que dificulta sua popularização e torna a utilização menos acessível. No mesmo período houve ainda uma intensificação na utilização de smartphones, que, aliado ao avanço tecnológico, possibilitou a evolução das câmeras presentes nesses dispositivos, tornando-os capazes de tirar fotos de alta qualidade. Nesse contexto, este projeto visa criar uma forma alternativa para a extração de biometrias, através de uma foto da digital a partir principalmente de um smartphone. Por meio de uma técnica de captura e pós-processamento das fotos, utilizando uma série de filtros, as impressões digitais se tornam mais evidentes, facilitando sua comparação com biometrias obtidas por leitores biométricos tradicionais ou por meio dessa abordagem alternativa. É importante ressaltar que, embora leitoras biométricas também sejam cada vez mais comuns em smartphones, os sistemas operacionais desses dispositivos não oferecem APIs ou interfaces de captura de biometrias para validação externa, limitando a confirmação de identidade apenas no âmbito local, por questões de privacidade. Por fim, o projeto propõe o desenvolvimento de uma API REST para a verificação de identidade com base nas impressões digitais extraídas por foto ou por leitor biométrico especializado. Essa API tem a finalidade de reduzir os custos envolvidos e facilitar o acesso para pessoas que não possuem um leitor de biometrias.

**Palavras-Chave:** Autenticação biométrica — Impressões digitais — Smartphone — Processamento de imagens — API REST

<sup>1</sup> Departamento de Informática e Estatística, Universidade Federal de Santa Catarina, Florianópolis - Santa Catarina, Brasil

\*Corresponding author: joaovitor.sc24@gmail.com

DOI: <http://dx.doi.org/10.22456/2175-2745.XXXX> • Received: dd/mm/yyyy • Accepted: dd/mm/yyyy

CC BY-NC-ND 4.0 - This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License.

## 1. Introdução

O uso de biometrias para identificação de pessoas é uma realidade há muito tempo. Na década passada as impressões digitais e a verificação biométrica eram utilizados majoritari-

amente para fins jurídicos e identificação criminal [1]. No entanto, com a popularização e avanço tecnológico, vários setores adotaram o uso da biometria intermediada com o computador para inúmeras finalidades. Dentre elas, as mais uti-

lizadas são: autenticação de usuários (seja essa autenticação feita para acesso a uma área restrita, desbloquear o smartphone, fazer login em aplicativos e acesso a dados sensíveis) e a identificação de pessoas - sendo utilizada para votações, emissões de documentação e emissões de certificados digitais [2].

Biometria, como o próprio nome já diz, significa a medição de características físicas ou comportamentais individuais de cada ser, usadas para identificá-lo [3]. Existem várias formas de fazer essa identificação biométrica, dentre elas estão: impressões digitais dos dedos, face, palma da mão, íris, retina, voz, comportamento, DNA, entre outras [2]. Das formas citadas uma das mais difundidas é a identificação biométrica por meio das impressões digitais. Isso se deve ao fato de as impressões serem únicas (são distintas até mesmo para gêmeos univitelinos e entre os diferentes dedos da mão), perenes (formadas durante a gestação e não sofrem mudanças significativas ao longo da vida) e imutáveis (não se alteram com o desgaste ou após acidentes).

A identificação biométrica por meio de impressões digitais geralmente é realizada usando leitores biométricos equipados com sensores ópticos. No entanto, esses leitores têm um alto custo [4] e são difíceis de obter em certas áreas, como regiões rurais. Além disso, eles não são facilmente integrados pelos desenvolvedores, que necessitam implementar inúmeras formas de utilizar as mais variadas leitoras disponíveis no mercado, por não existir uma padronização de comunicação e cada uma possuir um SDK distinto [5]. Somado ao fato de ser um dispositivo caro, os leitores biométricos não estão amplamente difundidos e não são comumente encontrados em residências e empresas, o que dificulta o acesso geral à autenticação biométrica por meio de impressões digitais. Isso obriga muitas pessoas a se deslocarem pessoalmente para locais que possuam esses dispositivos, o que não é ideal em um contexto pandêmico como o atual.

Apesar de ser cada vez mais comum a existência de leitores de impressão digital em smartphones, esses sensores não são diretamente acessíveis aos apps para captura de biometria, ficando dedicados ao desbloqueio de senhas no próprio celular [6]. Ou seja, não é permitido a um APP obter as minúcias biométricas para compará-las a uma base pré-existente externa - é permitido apenas obter uma confirmação da correspondência da biometria com aquela previamente cadastrada no smartphone.

A fim de sanar os problemas citados, esse projeto se propõe a trazer uma ferramenta que irá utilizar a câmera dos smartphones para a extração das digitais do usuário e ser possível realizar a verificação biométrica da digital com base em outra obtida independente do método escolhido, seja ele o tradicional por meio de hardwares específicos ou pela câmera do smartphone. A utilização de smartphones para o fim proposto é mais acessível e relativamente mais barato que um leitor tradicional, já que os smartphones são utilizados também para outros fins e são amplamente utilizados pela população. Outra motivação seria que o SERPRO até mesmo

já abriu um edital para o desenvolvimento de uma aplicação com esta finalidade [7].

É também necessário garantir a segurança da base de fotos, já que se alguém conseguir acessar indevidamente esta base, poderia facilmente burlar o sistema e roubar a identidade de outra pessoa. Além disso, é importante identificar formas de assegurar que o dedo capturado é de uma pessoa viva e que não é um dedo falso. A garantia de segurança deste novo método será discutida posteriormente no texto. Além disso será analisado a qualidade das biometrias dentro do padrões internacionais, probabilidade de aceitação de um falso positivo ou falso negativo (com análise das taxas de FAR, FRR, TAR, TRR e EER) e realizar uma comparação da confiabilidade das digitais obtidas por meio da extração por foto em confronto à extração tradicional.

Nesta seção estão descritas as motivações para a realização do trabalho, bem como seus objetivos, já o restante do documento será organizado da seguinte forma: Na seção 2, será apresentada toda a fundamentação teórica necessária para a correta compreensão deste trabalho. Na seção 3, serão apresentados os trabalhos relacionados ao tema de obtenção de biometrias (impressões digitais) por fotos, destacando a implementação e análise feitas nestes trabalhos correlatos. Na seção 4, será apresentada a proposta deste trabalho, exibindo as tecnologias envolvidas, desenvolvimento das técnicas de tratamento de imagens, batimento biométrico e da API proposta. Na seção 5, serão apresentados os testes e os resultados obtidos com validação de qualidade e análise das taxas de FAR, FRR, TAR, TRR e EER obtidas. Por fim, na seção 6, será apresentado as conclusões, com revisão geral, contribuição, limitações e os próximos passos para trabalhos futuros.

## 2. Fundamentação Teórica

Nesta seção serão descritos os principais conceitos relacionados a este trabalho, como o que é biometria e para que serve, como funcionam as impressões digitais, formato de armazenamento dessas biometrias, algoritmos de aferição de qualidade, a segurança envolvida no processo, autenticação e verificação biométrica, entendimento básico de fotografia e tratamento de imagens.

### 2.1 Biometria

Biometria vem da junção das palavras gregas Bios (que significa “vida”) e metron (que significa “medida”), significando então a medição de características físicas ou comportamentais individuais de cada ser, usadas para identificá-lo [3]. O princípio básico da biometria é a utilização das inúmeras características que distinguem um ser de outro para identificar um único indivíduo [2].

Existem várias formas de biometria, dentre elas estão: impressões digitais dos dedos, face, palma da mão, íris, retina, voz, comportamento (como a pessoa anda, digita, escreve ou até mesmo assina), DNA, veias, entre outras. Das formas citadas, as mais utilizadas atualmente são reconhecimento de

face e impressões digitais, as quais são amplamente difundidas por serem relativamente fáceis de serem coletadas e analisadas [2].

A utilização do reconhecimento facial tem como vantagem ser rápido e o baixo custo envolvido, porém apresenta problemas com algumas características fundamentais para um bom reconhecimento biométrico, como a unicidade (irmãos gêmeos compartilham de faces muito semelhantes), a perenidade (mudam de acordo com as demasiadas fases da vida) e a imutabilidade (podem mudar com acidentes). Por outro lado temos as impressões digitais, que sanam todos os problemas do reconhecimento facial, aliado a boa confiabilidade, porém mais demorado e custoso [8].

A biometria é amplamente utilizada nos dias de hoje, sendo muito comum em emissão de documentos oficiais do governo, certificados digitais, votações (biometria eleitoral), identificação, controle de acesso a ambientes e áreas restritas, login em smartphones e em aplicativos mobile, e para identificação criminal (principal grande uso nas décadas anteriores).

## 2.2 Impressões digitais

Impressão digital (também conhecidos como datilograma ou dermatoglifo) é o desenho formado pelas papilas (elevações da pele), presentes na ponta dos dedos, deixado em uma superfície lisa. As impressões digitais possuem algumas características importantes, como a unicidade (são distintas até para gêmeos univitelinos e entre os demais dedos da mão), perenidade (as papilas são formadas na gestação e não mudam consideravelmente ao longo da vida, até mesmo na morte) e imutabilidade (não mudam se desgastadas ou após acidentes), que permitem identificar de forma muito confiável uma pessoa [9].

É importante citar que elas possuem um alto grau de variação entre os próprios dedos e os dedos de outras pessoas, porém existem raros casos de pessoas que não possuem impressões digitais - Síndrome de Nagali [10]. O uso de impressões digitais para identificar pessoas não é uma prática recente, sendo utilizada já na antiguidade como forma de autenticar documentos e selar operações comerciais [11]. As digitais foram o primeiro método especificamente utilizado para classificação e identificação oficial de seres humanos, tendo Henry Faulds publicado o primeiro artigo (1880) em que discutia o uso de impressões digitais como meio de identificação e classificação pessoal, assim como o uso de tinta de impressora como forma para obtê-las. Posteriormente Francis Galton publicou seu livro “Impressões Digitais”, embasado no trabalho de Faulds. O livro trazia o primeiro sistema de classificação das impressões digitais, com três padrões [1] básicos analisando as minúcias dos dedos – laçada (loop), arqueada (arch) e verticilo (whorl) – que são detalhadas na figura 1.

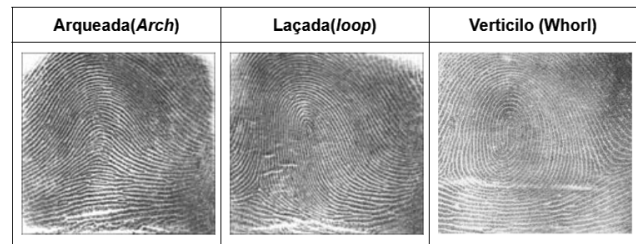


Figure 1. Tipos de impressões digitais

Com o passar dos anos a prática de analisar as minúcias dos dedos se tornou mais comum [12], criando a área de datiloscopia (processo de identificação humana por meio das impressões digitais), que evoluiu ainda mais com o sistema de classificação das minúcias (formas mínimas que compõem a impressão digital, possuindo vários padrões distintos que podem ser utilizados em conjunto para identificar uma pessoa), definindo algumas formas padrões a serem analisadas nos dedos, conforme a figura 2.

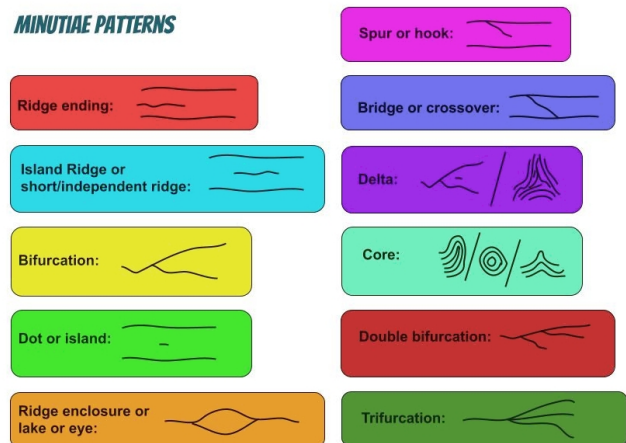


Figure 2. Padrões de minúcias

Inicialmente a coleta de digitais ocorria por meio de aplicação de tinta no dedo e realização de pressão em uma folha de papel lisa, a qual ficava marcada com as impressões do sujeito, porém com a popularização e modernização, surgiram várias formas de fazer essa coleta [12], sendo elas a coleta por sensores ópticos (sensores que tiram uma espécie de foto do dedo por meio de infravermelho), sensores CMOS ou capacitivos (utilizam de corrente elétrica para gerar a imagem das digitais), sensores por ultrassom (utilizam de ondas sonoras de alta frequência para obter a imagem da impressão digital) e sensores termais (utilizam das diferentes temperaturas entre os sulcos e as papilas para formar a imagem).

Por fim, é importante ressaltar que a qualidade da impressão digital obtida depende do método utilizado na coleta, e com um bom método e uma boa biometria, normalmente são encontrados entre 40 e 100 minúcias. [13]

### 2.2.1 WSQ

Uma das formas de registro das minúcias da impressão digital é com base em imagens em escala de cinza, as quais serão armazenadas numa base de comparação que tende a ser muito grande, portanto é necessário utilizar de algum algoritmo de compressão. O algoritmo utilizado para fazer essa compressão otimizada em imagens em escala de cinza é o WSQ (Wavelet Scalar Quantization), que é um algoritmo baseado na teoria de wavelet e foi desenvolvido pelo FBI em parceria com o Los Alamos National Laboratory, e com o NIST, tendo se tornado um padrão na área de biometrias. O arquivo gerado após a execução do algoritmo possui a extensão .wsq e é geralmente utilizado para armazenar imagens com 500 ppi. [14]. Vale destacar que o WSQ possui uma perda de qualidade por compressão, portanto gerar um WSQ a partir de outro resultará em uma menor qualidade [15].

### 2.2.2 NFIQ

Para validar a qualidade de um WSQ o NIST especificou um algoritmo conhecido como NFIQ - NIST Fingerprint Image Quality. Esse algoritmo em sua primeira versão funciona analisando as minúcias encontradas na digital capturada e fornece um score NFIQ que varia de 1 a 5, sendo 1 a melhor qualidade e 5 a pior qualidade. Por exemplo, no contexto das biometrias utilizadas no processo de emissão de certificados digitais na ICP-Brasil, só são aceitas biometrias com qualidade de NFIQ de 1 a 3 inclusive, sendo consideradas de baixíssima qualidade as que possuem score 4 e 5. (ICP-Brasil, 2021). Já a segunda versão do algoritmo NFIQ tem uma melhor capacidade de avaliação das biometrias, podendo distinguir melhor o que é ou não uma boa biometria e para isso adicionou mais níveis de scores, que após a execução do algoritmo fornece um score de 1 a 100. Sendo assim, muito mais preciso que a versão inicial do NFIQ. [14]

### 2.3 Segurança

O roubo ou falsificação de biometrias são práticas comuns no dia de hoje [16], onde muitos sistemas utilizam das biometrias para permitir ou não o acesso a determinada área, o que faz com que ela seja alvo de muitos ataques. Porém cada tipo de biometria possui ataques diferentes, sendo a mais visada a biometria facial, por ser facilmente obtida e copiada. Os atacantes utilizam de uma foto do usuário do qual querem se passar ou até mesmo utilizam de tecnologias de deepfake para imitar o rosto do indivíduo [17].

Nestes casos de roubo ou cópia de biometria facial a principal ação a fim de proteger o usuário é só permitir o envio de streams de vídeo controlado pela aplicação responsável pela coleta da face, que deve ser segura a manipulações, validando a vivacidade do conteúdo apresentado por meio de prova de vida (liveness check).

Já nos casos de ataque às impressões digitais, estes ocorrem normalmente com o uso de dedos de silicone - que foram feitos com base no dedo do indivíduo que se quer atacar - ou com a amputação do dedo do usuário. Para isso é necessário ter algum mecanismo de detecção de vivacidade do dedo,

algo que nas leitoras ópticas específicas é realizado via uma tecnologia de LFD (Live Finger Detection) que por meio de padrões em dedos falsos e infravermelho, é possível assegurar de que o dedo ali presente é de uma pessoa viva e também não é uma cópia [18].

Com isso, fica evidente que ter o controle da coleta reduz drasticamente a possibilidade de ataques, visto que caso a fonte de coleta seja segura ou houver a presença de alguém confiável para fazê-la, é muito mais difícil fraudar a biometria sem que seja percebido. Ainda é necessário tomar mais algumas medidas, como o uso de algoritmos confiáveis e de precisão para extrair e comparar as biometrias, uma base confiável de dados, checagens adicionais e uso da biometria somente como parte da solução e não como substituto de todas as formas de segurança.

### 2.4 Autenticação Biométrica

A autenticação biométrica consiste em validar a veracidade da identidade de um usuário por meio da verificação biométrica, processo que irá verificar a equivalência da biometria apresentada com outra previamente cadastrada (comparação 1:1) e atestada como verdadeira (identificação 1:n). Para a verificação biométrica ocorrer, é necessário que a biometria verdadeira do usuário já tenha sido extraída em um template biométrico anteriormente e cadastrado-a em uma base biométrica de templates confiáveis, só então é possível, por meio de nova coleta, verificar a autenticidade dessa nova biometria com base na anterior [2]. Este processo de cadastro e match com a base de dados é exibido na 3, assim como a necessidade de a cada cadastramento fazer uma pesquisa na base a fim de encontrar biometrias semelhantes e evitar possíveis fraudes (identificação 1:n).

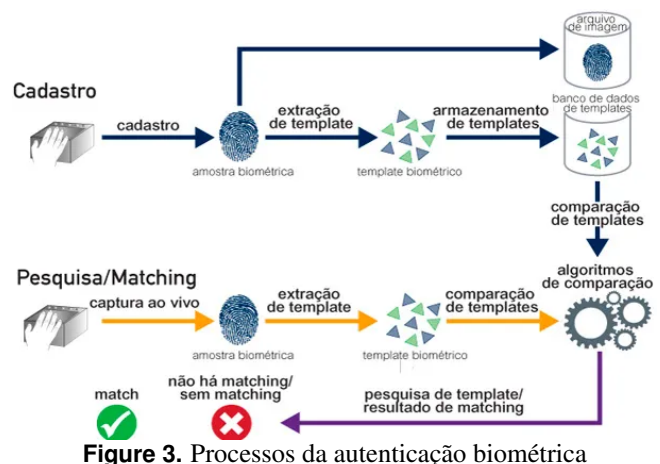


Figure 3. Processos da autenticação biométrica

Antigamente, a verificação biométrica era realizada manualmente, comparando duas biometrias coletadas para determinar se pertenciam à mesma pessoa. Essa análise era baseada em um certo grau de similaridade aceitável entre as duas amostras. No entanto, atualmente, a validação manual foi substituída por sistemas automatizados e especialistas em verificação biométrica. É importante destacar que o grau de



similaridade é definido previamente por um valor conhecido como "matching threshold" (limite de correspondência), que determina até que ponto duas biometrias são consideradas semelhantes e pertencentes à mesma pessoa. Um valor adequado de threshold pode ter um grande impacto na quantidade de falsos positivos ou falsos negativos na base biométrica [19].

Por fim, a autenticação biométrica para ser segura necessita atingir uma certa porcentagem de aceitação ou não de usuários com base na similaridade das mesmas, para isso existe a taxa de FAR (False acceptance rate), FRR (False rejection rate), TAR (True acceptance rate), TRR (True rejection rate) e EER (Equal error rate). O significado delas são: [20] [21] [22] [23]

- FAR: Também conhecida como taxa de fraude, é a probabilidade de um usuário não autorizado ser aceito pelo sistema de autenticação biométrica. É importante minimizá-la para aumentar a segurança do sistema.
- FRR: Também conhecida como taxa de rejeição, é a probabilidade de um usuário autorizado não ser aceito pelo sistema de autenticação biométrica. Minimizar essa medida é essencial para aumentar a confiabilidade do sistema.
- TAR: Também conhecido como taxa de match, é a probabilidade de um usuário autorizado ser aceito corretamente pelo sistema de autenticação biométrica. Maximizar essa medida é crucial para aumentar a segurança do sistema.
- TRR: É representado como a porcentagem de vezes que uma pessoa não autorizada é negada corretamente pelo sistema, para que um sistema de autenticação seja mais seguro, essa medida deve ser maximizada.
- EER: é a taxa em que o FAR é igual ao FRR. Mede a acurácia de um sistema biométrico, encontrando o ponto de equilíbrio entre falsas negações e falsas aceitações. Minimizar esse valor é importante para garantir a melhor segurança do sistema.

As taxas aceitas pela ICP-Brasil, por exemplo para um PSBio com base no DOC-ICP05.03 v3.0 (2021) é de 0,01% de FAR e 99% de TAR. Ainda quanto às taxas aceitas, o NIST especifica que o recomendado para uma verificação de impressões digitais é de um TAR de 96% para um FAR de 1%, assim como um TAR de cerca de 85% para um FAR de 0,001%. De acordo com o NISTIR 7204 (2005). Ainda de acordo com o NIST o recomendado para uma verificação biométrica envolvendo faces é de um TAR de 90% para um FAR de 1% e um TAR de 70% para um FAR de 0,01%, isso com uma boa condição de iluminação, para cenários externos esses índices caem para 37% de TAR para um FAR de 1%

Para a realização deste trabalho o algoritmo utilizado para extração de templates é desenvolvido pela Neurotechnology, que é um dos melhores existentes no mundo, tendo recebido inúmeros prêmios como um dos mais rápidos e precisos [24] [25], porém existem outras alternativas gratuitas de menor desempenho, como o SourceAFIS e o MINDTCT (criado pelo

NIST), porém de qualidade inferior. A escolha ou desenvolvimento de um bom extrator, interfere diretamente na qualidade do sistema biométrico.

Além do extrator é também necessário um matcher para realizar a comparação de dois templates e confirmar ou não a autenticação biométrica. Assim como o extrator, o matcher também interfere na qualidade do sistema biométrico, porém esse tem um impacto ainda maior, já que é quem efetivamente irá determinar se duas biometrias pertencem ou não ao mesmo indivíduo. Novamente o matcher utilizado será fornecido pela Neurotechnology, mas podem ser encontrados outros matchers como o SourceAFIS e o BOZORTH3 (criado pelo NIST), mas que novamente apresentam qualidade inferior.

## 2.5 Fotografia

Fotografia consiste na técnica de criar imagens por exposição luminosa em uma superfície fotossensível. A fotografia evoluiu consideravelmente ao longo dos anos, partindo de fotos em preto e branco com câmeras analógicas para fotos coloridas tiradas por câmeras digitais. A câmera digital presente nos smartphones é composta por um sensor chamado de CCD ou CMOS que ao receber luz, converte esta luz em um código eletrônico digital - um quadro com o valor das cores de todos os pixels da imagem - que será armazenado na memória como um arquivo digital, podendo ter vários formatos [26].

A imagem digital é composta por pixels, que são os pontos mínimos que formam a imagem, podendo ser iluminados por diferentes cores. Uma câmera com mais pixels tem maior definição e resolução, pois possui mais pontos de cores para gerar a imagem final, medida em megapixels (MP). Um megapixel é equivalente a um milhão de pixels. Ainda sobre resolução, é importante mencionar que ela normalmente é descrita como PPI (pixels por polegada), onde quanto maior o PPI, maior a resolução da imagem e mais detalhes podem ser exibidos. No entanto, é importante destacar que o PPI é válido apenas para a exibição na tela, pois depende de uma área física, o que não existe na imagem digital [27].

Por fim, é importante ressaltar que existem ainda várias composições de lentes na fotografia [28], com três categorias de lentes, que são a grande angular (ângulo de visão grande, apresenta distorção), média (ou norma - lente que mais se aproxima do olho humano) e teleobjetiva (distorção de perspectiva). Existe ainda a funcionalidade das lentes, como as lentes macro, que permitem que a foto possa ser tirada de mais perto do objeto. Por isso, ela é ideal para captar detalhes e diferentes texturas, como nas impressões digitais. Na maioria das câmeras podem ser utilizados dois níveis de zoom, o zoom óptico (feito com um conjunto de lentes e evita a perda de qualidade) e o zoom digital (utiliza de software para se aproximar do conteúdo, perdendo qualidade já que não está efetivamente ficando mais próximo do objeto).

## 2.6 Tratamento de imagens

Tratamento de imagens é a prática de alterar imagens por meio de softwares, sendo uma atividade comum em fotografia profissional e sistemas que fazem uso de fotos. Os fotógrafos

aplicam filtros e edições para melhorar a aparência da imagem original. Além disso, algoritmos de tratamento de imagens são amplamente utilizados para atingir objetivos específicos, como realçar detalhes, remover fundos ou objetos, entre outros. O software GIMP (GNU Image Manipulation Program) é uma ferramenta de edição de imagens de código aberto comumente utilizada. Filtros e algoritmos importantes serão detalhados nas próximas subseções para a conclusão deste trabalho.

### 2.6.1 Equalização

A equalização de uma imagem é um processo de uniformização que busca igualar a iluminação em diferentes áreas da imagem. Existem dois métodos comuns de equalização: a equalização adaptativa do histograma (AHE) e a equalização de histograma adaptativa limitada por contraste (CLAHE). A equalização de histograma consiste em aumentar a distribuição global das intensidades dos pixels em uma imagem, melhorando o contraste e a nitidez. O AHE aplica a equalização de forma global, porém pode comprometer regiões específicas da imagem.

Para resolver esse problema, o CLAHE realiza a equalização em blocos distintos da imagem, aumentando o contraste de cada região individualmente. No entanto, isso pode resultar em um aumento de ruídos. Para lidar com isso, é aplicado um limite de contraste [29]. Em comparação, as imagens geradas pelo CLAHE são mais nítidas do que as geradas pelo AHE e são adequadas para uma variedade maior de imagens. No entanto, o CLAHE requer mais tempo de processamento.

### 2.6.2 Filtros passa-baixa e passa-alta

Na área de tratamento de imagens é muito comum utilizar filtros que analisam a frequência das imagens e que com base nela permitem somente uma parte da frequência se acentuar, dessa categoria existem os filtros de passa-baixa e passa-alta [30] [31], alguns exemplos destes filtros são:

- Filtro de Laplace (passa-alta): Utilizado para detectar regiões de alta variação de cor, ou seja, bordas.
- Filtro Gaussiano (passa-baixa): Utilizado para reduzir o nível de ruído, a fim de diminuir a distorção na imagem.
- Filtro de Gabor (passa-baixa): Utilizado para reforçar texturas nas imagens, podendo recuperar informações das imagens ou até mesmo omitir ruídos.

### 2.6.3 Segmentação

A segmentação de imagens é o processo de fracionar a imagem em partes comuns, ou seja, encontrar elementos semelhantes e distintos para separá-los. A segmentação possui vários usos, já que a partir de uma imagem é possível obter as regiões que possuem algum objeto de interesse como pessoas, carros, contornos ou regiões de foco [32]. Para atingir esse fim, essa técnica utiliza de várias maneiras de identificar as regiões de interesse, como uma segregação baseada em regiões, cores, threshold, entre outras.

### 2.6.4 Binarização

A binarização de uma imagem, consiste no processo de alterar o espectro de 256 tons de uma imagem para somente 2 ou seja binário. O algoritmo mais utilizado é o algoritmo de Otsu que consiste em encontrar um valor de threshold para a binarização da imagem [33]. Após encontrado o valor de threshold o algoritmo irá fazer com que todas as intensidades abaixo do valor sejam alteradas para 0 e todas as intensidades acima dela sejam alteradas para 1 (ou 255 para a visualização da imagem).

### 2.6.5 Inversão de cores

A técnica de inversão de cores é um tipo de tratamento de imagens que transforma as cores da imagem com base no seu espectro, tornando-as opostas após a execução [34]. Com a execução deste filtro as imagens brancas passam a ser pretas e vice-versa, além de alterar todas as outras cores para o oposto.

## 3. Trabalhos Relacionados

Neste capítulo serão descritos os trabalhos relacionados mais relevantes na área, a qual ainda foi muito pouco explorada. Após extensa busca na literatura, foram selecionados sete principais artigos, que foram classificados em três áreas distintas, que tratam de: melhoria de uma imagem de impressão digital, extração de biometria sem contato e extração por câmera de smartphones. Ao final do capítulo será feita uma comparação dos trabalhos relacionados com este em questão, além de um direcionamento para novas oportunidades de pesquisa.

### 3.1 Melhoria de imagens de impressões digitais

Na área de melhoria de imagens de impressões digitais obtidas por leitoras tradicionais, foram encontrados dois trabalhos relevantes.

O primeiro trabalho, intitulado "Minutiae Extraction from Fingerprint Images - a Review" [13], propõe o desenvolvimento de um algoritmo para processar imagens biométricas obtidas por leitores ópticos especializados, com o objetivo de tornar as minúcias mais visíveis e facilitar a extração e comparação biométrica. O algoritmo utiliza o filtro de Gabor como base e requer filtros para estimar a orientação e a frequência das elevações na impressão digital. Após o processamento, um algoritmo de extração é proposto. O trabalho destaca que o desenvolvimento de um extrator de biometrias é complexo e exige um esforço significativo para sua implementação, sendo um dos focos do trabalho. Os resultados mostraram uma melhoria nas imagens testadas, mas ressaltaram a dependência da qualidade da imagem inicial obtida pelas leitoras.

Já o trabalho "Fingerprint Image Enhancement and Minutiae Extraction" [35], possui um foco maior em melhorar as imagens obtidas através do leitor óptico especializado. Assim como o primeiro trabalho, o principal filtro utilizado é o filtro de Gabor, mantendo os dois filtros de estimativas exigidos. O estudo realizou diversos testes e obteve bons resultados com o

algoritmo proposto. No entanto, assim como no trabalho anterior, a melhoria depende fortemente da qualidade da imagem inicial, e em alguns casos, o algoritmo pode incorretamente alterar a biometria, levando a uma possível associação errônea com outra pessoa. O autor concluiu que o algoritmo facilita a extração de minúcias e melhora a comparação biométrica, mas não pode ser aplicado em todas as imagens, resultando em um desempenho inferior em alguns casos.

### 3.2 Extração de impressões digitais sem contato

Na área de extração de biometrias sem contato, foram encontrados três trabalhos relevantes.

O trabalho "Towards Contactless, Low-Cost and Accurate 3D Fingerprint Identification" [36] propõe a obtenção de impressões digitais em 3D por meio de uma única câmera. O estudo utiliza um ambiente controlado com uma câmera específica com custo de 100 dólares e 7 LEDs para iluminar adequadamente o dedo. O algoritmo desenvolvido busca transformar a foto em uma representação 3D da biometria, com destaque para as minúcias, para posterior comparação com outras biometrias 3D obtidas pelo método proposto. No desenvolvimento do trabalho nada é citado sobre a possibilidade de comparar essas biometrias com as obtidas pelos métodos tradicionais de contato, sendo o foco do desenvolvimento a implementação da conversão de fotos 2D em 3D (melhorando-as utilizando o filtro de Gabor) e a comparação entre elas. Os autores também desenvolveram um algoritmo de matching baseado em biometrias 3D. Após a realização de experimentos, concluiu-se que o método proposto obteve melhores resultados do que outros métodos de obtenção de biometrias 3D, porém ainda não está pronto para ser utilizado em um sistema de grande escala, devido a uma taxa de erro elevada (EER de 18,56%).

No trabalho "Mosaicing Touchless and Mirror-Reflected Fingerprint Images" [37], é desenvolvido um dispositivo especializado para a captura de imagens de impressões digitais sem contato. Esse dispositivo é composto por uma câmera, um anel de LED, difusores e dois espelhos posicionados ao lado do orifício onde o dedo é colocado. Os autores também criaram um algoritmo para processar as imagens obtidas, que incluem três ângulos diferentes do dedo: frontal, lateral direito e lateral esquerdo. Esse algoritmo destaca as minúcias e sobrepõe os três ângulos para obter uma impressão digital mais larga. Assim como nos trabalhos anteriores, o filtro de Gabor é utilizado como o principal método de processamento de imagem, resultando em imagens altamente precisas. No entanto, durante o desenvolvimento do trabalho, não foram realizadas verificações biométricas entre as biometrias obtidas por contato e as obtidas sem contato, sendo o foco apenas na comparação do número de minúcias corretamente identificadas nas imagens. Após a realização de testes, observou-se um aumento significativo no número de minúcias utilizando o método proposto, tornando-o equivalente a uma biometria obtida por contato direto do dedo na superfície de leitura, porém não é esclarecido o resultado de FAR ou EER obtido

nos testes.

O artigo "Contactless Fingerprint Recognition Using Deep Learning - A Systematic Review" [38] é uma revisão dos principais trabalhos na área de extração de impressões digitais sem contato. Nesse artigo, os autores realizam uma análise das três principais abordagens para obtenção de biometrias, que são: foto, deep learning e o método tradicional. Eles apresentam os resultados diferentes obtidos em vários trabalhos e destacam as similaridades entre eles, como o uso de filtros para melhorar as biometrias e um processo rigoroso de coleta. O foco principal dessa pesquisa é a utilização de deep learning na obtenção de biometrias sem contato, mas os resultados obtidos ainda não são aplicáveis em sistemas de larga escala. Os resultados obtidos em sistemas baseados em fotos não foram muito explorados, não sendo tão relevantes para o desenvolvimento deste trabalho em questão. Porém, ainda por meio da análise realizada por este artigo é possível evidenciar o quanto as pesquisas neste tema ainda precisam evoluir e a existência de poucos trabalhos na área.

### 3.3 Extração de impressões digitais via câmera dos smartphones

Nesta seção serão apresentados os principais trabalhos encontrados na área de extração de impressões digitais por fotos obtidas através de um smartphone, sendo estes da mesma área do trabalho em questão. Assim como já detalhado anteriormente, o foco da área é a utilização em larga escala por qualquer pessoa que possua um smartphone, sendo uma solução mais barata e acessível.

O primeiro trabalho encontrado com foco em fotos de smartphones é o Scaling-Robust Fingerprint Verification with Smartphone Camera in Real-life Scenarios [39], que trata da utilização de fotos em larga escala para um sistema de verificação biométrica. No desenvolvimento deste trabalho foram utilizados 3 modelos de celulares diferentes e o foco do trabalho foi na segmentação correta do fundo da imagem, já que para uma utilização em larga escala o algoritmo de remoção do fundo precisa ser bem preciso e funcionar corretamente para os mais variados fundos possíveis. Além do foco na segmentação, o trabalho focou em desenvolver um algoritmo que fosse capaz de recortar automaticamente a região de interesse dos dedos, ou seja, a ponta (ROI). Após a aplicação do algoritmo os autores testaram algumas verificações biométricas e obtiveram resultados satisfatórios, porém o matcher utilizado tem qualidade moderada, o que pode impactar nos resultados obtidos. Além disso, não foi realizada nenhuma comparação com as biometrias obtidas pelo método tradicional, somente foi realizado comparações entre as próprias fotos com um EER variando de 2% a 8% para biometrias obtidas no mesmo aparelho, e EER variando de 9% a 12% com biometrias obtidas por celulares diferentes.

Por fim, o trabalho mais completo encontrado foi o Efficient Fingerprint Extraction and Matching Using Smartphone Camera [40], que utiliza de um aplicativo desenvolvido para a finalidade de tirar fotos dos dedos, o qual identifica a ponta dos



dedos e foca automaticamente na região de interesse. Após a captura da foto obtida pelo aplicativo proposto pelos autores, é então aplicado um algoritmo de processamento da imagem com foco em CLAHE e filtro de Gabor, além da detecção da zona de interesse, recorte e alinhamento. Por fim é realizada a extração de minúcias e comparação. A imagem obtida pelo método proposto é de alta qualidade e nos testes realizados utilizando um matcher de qualidade intermediária foi possível obter resultados aceitáveis, porém as verificações ocorrem apenas entre as fotos extraídas do celular com as biometrias obtidas por leitoras especializadas, ou seja, não realizam uma análise da eficácia do método proposto a partir das imagens obtidas no APP e processadas. Quanto aos resultados o EER obtido na comparação com WSQs foi de 6% a 15%. Ainda foi possível concluir que imagens obtidas utilizando o HDR da câmera melhoram o resultado, e que o filtro de Gabor tem um bom desempenho no algoritmo proposto, sendo foco de desenvolvimento. Vale também ressaltar que o método proposto não trata da remoção de fundo, dada a justificativa de que o corte na zona de interesse não faz necessário o uso de segmentação.

### 3.4 Considerações finais

Neste capítulo foram apresentados diversos trabalhos de temas relacionados ao proposto neste trabalho em questão, e foi possível evidenciar que é sim possível obter biometrias de impressões digitais obtidas por câmeras fotográficas. Para isso necessitam de um bom método de captura da foto, um bom algoritmo de processamento de imagem, realçando minúcias e centralizando a região de interesse, além de um bom extrator de minúcias e matcher. Um resumo das características de cada trabalho mencionado é exibido na figura 4.

| Trabalho                       | Gabor | E.E. | U.G. | C.O. | C.E. | API | Q.A. |
|--------------------------------|-------|------|------|------|------|-----|------|
| BANSAL; SEHGAL; BEDI, 2011     | S     | S    | S    | N    | N    | N   | S    |
| THAI, 2003                     | S     | S    | S    | N    | N    | N   | S    |
| KUMAR; KWONG, 2015             | S     | S    | N    | N    | N    | N   | N    |
| CHOI; CHOI; KIM, 2010          | S     | S    | N    | S    | N    | N   | D    |
| CHOWDHURY; IMTIAZ, 2022        | N     | D    | D    | N    | N    | N   | D    |
| RAGHAVENDRA; BUSCH; YANG, 2013 | N     | N    | S    | N    | N    | N   | D    |
| GUPTA; ANAND; RAI, 2017        | S     | N    | S    | N    | N    | N   | S    |
| Fingerprint Photo Matcher      | N     | N    | S    | S    | S    | S   | S    |

**Legenda:**

Gabor = Utilização do filtro de Gabor no tratamento das imagens  
 E.E. = Necessidade de Equipamento Especializado  
 U.G. = Método para uso em geral em massa e para qualquer contexto  
 C.O. = Foco em Como Obter as fotos  
 C.E. = Comparação Extensa dos resultados e diferentes métodos  
 API = Desenvolvimento de API para utilização do método  
 Q.A. = Qualidade aceitável dentro dos parâmetros internacionais  
 S = Sim  
 N = Não  
 D = Depende do método abordado

**Figure 4.** Trabalhos relacionados e suas características

Observa-se que nenhum trabalho mencionado neste capítulo exibe a qualidade da biometria obtida em termos de NFIQ e não comparam os resultados obtidos entre todas as possíveis formas de avaliação, como qualidade em comparação com duas biometrias do método tradicional, comparação com duas

biometrias do método proposto e comparação entre uma biometria do método proposto com uma do método tradicional, além de não dedicarem esforços em técnicas e câmeras necessárias para se obter a melhor foto. É importante também reforçar que apenas dois trabalhos focam na utilização em larga escala e de uso geral, sendo acessível por qualquer pessoa.

Por fim, apenas um trabalho apresentado teve resultados próximos do aceitável nos parâmetros internacionais e nenhum propôs uma API de fácil utilização do método proposto para os mais variados fins, assim como o objetivo deste trabalho. Neste ponto, caracteriza-se a importância deste trabalho, onde além de ser feita a extração das impressões digitais, irá ser realizado um estudo completo da qualidade dessa biometria obtida, com taxas de FAR, FRR, TAR, TRR e EER dentro dos padrões internacionais, comparação da biometria com WSQs e com outras fotos, além de uma API com processo automático, que ao receber a foto faz todo o processamento necessário para extrair as impressões digitais e até mesmo validá-las como pertencentes ou não ao mesmo indivíduo.

Fica evidente a oportunidade de pesquisa na área, em novos métodos de coleta sem contato em larga escala e de uso geral, além da oportunidade de desenvolver um algoritmo mais eficaz para o tratamento das imagens com filtros de Gabor somados com outros algoritmos de processamento de imagens, bem como um teste com um grande banco de dados em um cenário real de utilização e uma aplicação para captura automática dos dedos.

## 4. Fingerprint photo matcher

Neste capítulo, apresentamos o Fingerprint Photo Matcher, uma API REST para verificar biometria usando duas digitais fornecidas. As digitais podem ser extraídas de leitores tradicionais ou de uma foto das impressões digitais. Garantimos um nível de qualidade aceito internacionalmente pelo NIST. Discutimos os desafios iniciais do desenvolvimento da aplicação, o histórico de testes, e a explicação, definição e escolha dos algoritmos e técnicas envolvidas.



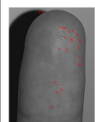
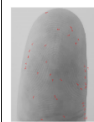
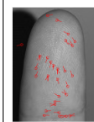
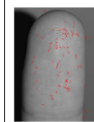
### 4.1 Definição do método de desenvolvimento

Para o desenvolvimento desta API, é necessário possuir ou implementar um extrator e matcher de biometrias. Devido a complexidade de desenvolvê-los, foi decidido pela utilização de um SDK biométrico especializado de alta capacidade e desempenho, produzido pela Neurotechnology e cujo acesso para a realização deste trabalho foi fornecido pela BRy Tecnologia. Em posse do SDK, era necessário confirmar sua capacidade de processar imagens de impressões digitais, que não possuem o formato WSQ, e extraí-las em um template que possa ser comparado futuramente, já que o foco deste trabalho consiste na validação de fotos de digitais. Desafio que se mostrou possível com a utilização deste motor biométrico. Na documentação do SDK temos uma relação do score de Threshold com o FAR do sistema biométrico, e foi utilizado o score 48 que tem relação com um FAR de 0,01% e também



por ser o valor aceito para um PSBIO (Prestador de Serviço Biométrico) credenciado pelo ITI.



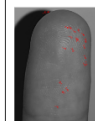
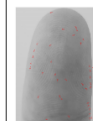
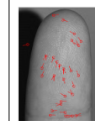
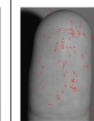
Foi então realizada uma sequência de capturas do dedo do autor utilizando um smartphone Samsung Galaxy S10 e um Samsung Galaxy S20 explorando diferentes ângulos, lentes e modos de captura. Foram tiradas fotos com e sem HDR, com e sem flash e distantes ou próximas ao dedo. Para o foco foram testadas várias técnicas como: mão aberta, apenas um dedo erguido, dedo próximo ao fundo uniforme, e dedo com fundo distante. Os principais modelos de fotos obtidos, já com recorte na zona de interesse (ponta dos dedos), estão relacionados na figura 5 e a técnica de captura com melhor resultado neste primeiro momento foi a de fundo uniforme próximo.

|   |   |   |   |   |   |
|---|---|---|---|---|---|
|  |  |  |  |  |  |
| NFIQ: 5   | NFIQ: 5   | NFIQ: 2   | NFIQ: 5   | NFIQ: 5   | NFIQ: 2   |
| Sem HDR, sem flash e distante   | Sem HDR, sem flash e próximo  | Sem HDR, com flash e próximo  | Com HDR, sem flash e próximo  | Com HDR, com flash e distante   | Com HDR, com flash e próximo  |

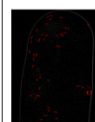

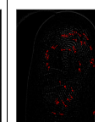
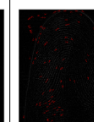
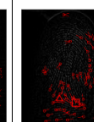
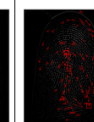
**Figure 5.** Sequência de fotos com smartphones

Após aferição visual e pela própria execução do extrator para validar as biometrias, foi possível perceber que o HDR e o flash eram os principais fatores na obtenção de fotos com minúcias bem perceptíveis, já que foi mais fácil obter fotos com NFIQs melhores desta maneira. Além disso é possível perceber uma boa influência da proximidade do dedo, porém, com lentes que não sejam do tipo macro ou zoom, conseguir focar na ponta dos dedos com a câmera próxima ao dedo é uma tarefa difícil. Portanto é possível concluir que as condições ideais da foto são obtidas por câmeras com HDR, flash e lentes macro que conseguem focar melhor nas minúcias. Ter o controle do foco e do modo de captura é crucial para uma boa foto.

Por fim, para atestar a viabilidade do projeto e definir a estratégia de desenvolvimento, era necessário fazer algumas verificações biométricas básicas com WSQs obtidos por leitoras ópticas especializadas, garantindo assim o funcionamento do matcher com biometrias obtidas pelos dois métodos, além de fornecer uma ideia inicial da qualidade das fotos. Para isso foram realizadas verificações biométricas (utilizando o matcher disponibilizado) com as fotos anteriores e também com as mesmas fotos, porém tratadas com alguns filtros que são eles: aumento de brilho, contraste e filtro Gaussiano, todos aplicados pelo GIMP por meio dos sliders disponíveis, como é possível visualizar na figura 6 e 7.

|   |  |   |   |   |   |
|---|--|---|---|---|---|
|  |  |  |  |  |  |
| NFIQ: 5   | NFIQ: 5  | NFIQ: 2   | NFIQ: 5   | NFIQ: 5   | NFIQ: 2   |
| Score: 24<br>No Match<br>FAR ~ 1%   | Score: 10<br>No Match<br>FAR ~ 10%   | Score: 66<br>Match<br>FAR ~ 0.001%  | Score: 13<br>No Match<br>FAR ~ 10%  | Score: 12<br>No Match<br>FAR ~ 10%  | Score: 174<br>Match<br>FAR ~ 0.000001%  |

**Figure 6.** Verificações (1:1) com fotos iniciais originais

|   |  |   |   |   |   |
|---|--|---|---|---|---|
|  |  |  |  |  |  |
| NFIQ: 5   | NFIQ: 1  | NFIQ: 1   | NFIQ: 5   | NFIQ: 5   | NFIQ: 1   |
| Score: 17<br>No Match<br>FAR ~ 1%   | Score: 22<br>No Match<br>FAR ~ 1%  | Score: 55<br>Match<br>FAR ~ 0.01%   | Score: 8<br>No Match<br>FAR ~ 10%   | Score: 8<br>No Match<br>FAR ~ 10%   | Score: 248<br>Match<br>FAR ~ 0.000001%  |

**Figure 7.** Verificações (1:1) com fotos iniciais tratadas com filtro Gaussiano

Com base nos resultados obtidos, conclui-se que é possível realizar um match entre uma foto de um dedo e um WSQ por meio do SDK da Neurotechnology. Além disso, é possível verificar que as imagens com flash, HDR e próximas aos dedos possuem maior desempenho e que realizando alguma filtragem na imagem é possível melhorar o resultado obtido. Neste primeiro teste básico já foi possível obter quatro matches e nível de FAR dentro do aceito pelos padrões internacionais, porém sendo ainda necessário a evolução da captura e tratamento da imagem para que seja mais fácil de obtê-las e processá-las sendo aplicável a todas as fotos.

Por fim, um último teste antes da definição dos próximos passos de desenvolvimento foi realizado, executando a comparação de duas biometrias obtidas por foto, sendo elas de ótima qualidade, porém não resultando em um match. Isso comprova que a extração por fotos e filtros ainda necessita evoluir para se tornar utilizável e que é necessário o desenvolvimento de um algoritmo de tratamento especial para essas fotos, que será proposto neste trabalho mais adiante, assim como um método de captura.

O algoritmo de processamento de imagens necessário será discutido na próxima seção, e será desenvolvido com Java utilizando o framework Spring e a partir do seguinte método de desenvolvimento: implementação de múltiplos algoritmos de tratamento de imagens, aferição de desempenho destes algoritmos, para determinar o algoritmo final de tratamento, métodos de conexão e utilização do SDK da Neurotechnology (tanto para extração quanto para match), por meio da API disponibilizada pela BRy, além do desenvolvimento de uma API para utilização deste conjunto.

## 4.2 Definição do algoritmo de processamento

A partir dos testes iniciais realizados ficou evidente a necessidade de um algoritmo de tratamento de imagens, para isso,

após extensa pesquisa na área, análise dos trabalhos relacionados e testes manuais, foram desenvolvidos vários algoritmos, que juntos fazem a imagem ficar mais nítida e com minúcias mais aparentes. Para o desenvolvimento destes algoritmos foi utilizado a biblioteca OpenCV, para facilitação do processo.

Para definir o algoritmo final de processamento, era necessário fazer a implementação de vários algoritmos de tratamento de imagens que juntos irão compor a implementação final. Portanto, o primeiro algoritmo desenvolvido é o algoritmo para espelhar a imagem (flip) que recebe a imagem e faz o espelhamento da mesma no eixo vertical, feito desta maneira para equivaler com as biometrias obtidas em leitores tradicionais. Implementou-se um algoritmo para converter a imagem para escala de cinza, já que para a aplicação futura dos filtros de AHE e CLAHE é necessário que a imagem esteja em escala de cinza.

Com a conversão para escala de cinza realizada é possível utilizar o filtro AHE para otimizar o contraste da imagem, como o resultado do AHE não se mostrou tão eficiente, já que enfatizou as minúcias mas gerou áreas com muita luz, é necessário implementar o CLAHE, que utiliza a função específica do OpenCV. Apesar de uma máquina conseguir visualizar as alterações de contraste de uma região, a aplicação do CLAHE se mostrou muito influente na melhora do NFIQ obtido.

Após a aplicação do filtro de CLAHE fica evidente a melhora na visualização das minúcias, porém percebe-se que as minúcias estão invertidas com relação às exibidas em um WSQ, ou seja, onde na imagem, com o filtro aplicado, está branco, no WSQ é preto, o que pode impactar no match entre os dois tipos de biometrias no futuro. Por conta disso faz-se necessário o desenvolvimento de um algoritmo de inversão de cores.

Como as imagens obtidas por WSQs possuem somente a cor branca para o fundo e preta para as áreas altas das minúcias, é fundamental binarizar a imagem para obter o resultado desejado, eliminando qualquer tom de cinza presente. Outro método importante para a exibição apropriada da biometria, já que inicialmente esta fica muito distante da câmera e aparece uma região maior do dedo do que somente a área de interesse, é o método de crop que faz o recorte da imagem mais centralizada. Vale destacar que o crop existente tem um tamanho padrão que pode não obedecer para todos os cenários de foto, câmera e dispositivos, necessitando para implementação em larga escala de um algoritmo com crop da zona de interesse com melhor qualidade e inteligência.

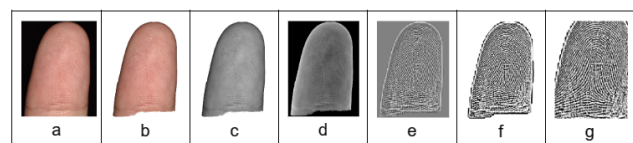
Além dos filtros já exibidos, detectou-se a possibilidade de implementar outros antes da definição final do algoritmo de processamento de imagens, filtros dos quais poderiam ser úteis para a conclusão da tarefa. O primeiro dos algoritmos testados foi a normalização, que iguala a iluminação em todos os pixels, porém não foi utilizado para o algoritmo final. Como o filtro de Gabor foi o mais utilizado nas implementações de trabalhos relacionados, uma tentativa de desenvolvimento foi realizada, porém após a execução fica claro que para o correto funciona-

mento do filtro de Gabor é necessário a implementação de um de mapa de frequência das minúcias e orientação destas, que é muito difícil de ser implementado e irá variar com cada imagem e tamanho da mesma, além de ser difícil de padronizá-lo para fotos obtidas de diferentes dispositivos, padrões de iluminação, resolução e posicionamento diferentes. Outro filtro bastante citado na literatura é o Canny Edge Detector que é capaz de realçar as bordas e remover o conteúdo não pertencente às bordas, porém não trouxe o resultado esperado para as biometrias, exibindo muito ruído junto da imagem, já que este é um filtro passa-alta.

Por fim, após a aplicação dos vários filtros, viu-se que alguns deles realçam detalhes no fundo da imagem, que não é uma zona de interesse, e dependendo do que estiver presente no fundo da foto, pode impactar muito negativamente na qualidade da extração e no match dessa biometria. Portanto é imprescindível a segmentação da foto original, removendo o fundo presente desta.

Avançando para a versão final do algoritmo de processamento de imagem, este será composto por vários dos métodos implementados. Para a escolha do algoritmo proposto foi realizada a captura de fotos dos 10 dedos do autor, processamento das imagens pelos algoritmos e extração das minúcias. Após a extração é possível verificar o NFIQ obtido, a composição de algoritmos que gerasse os melhores NFIQs seria a versão final do algoritmo. Como critério de desempate foi utilizado a aferição visual. Após inúmeros testes (que não serão exibidos para resumir o desenvolvimento), o algoritmo que obteve o melhor resultado é composto pela execução em ordem dos algoritmos de espelhamento, remoção de fundo, conversão para escala de cinza, inversão da imagem, CLAHE e binarização.

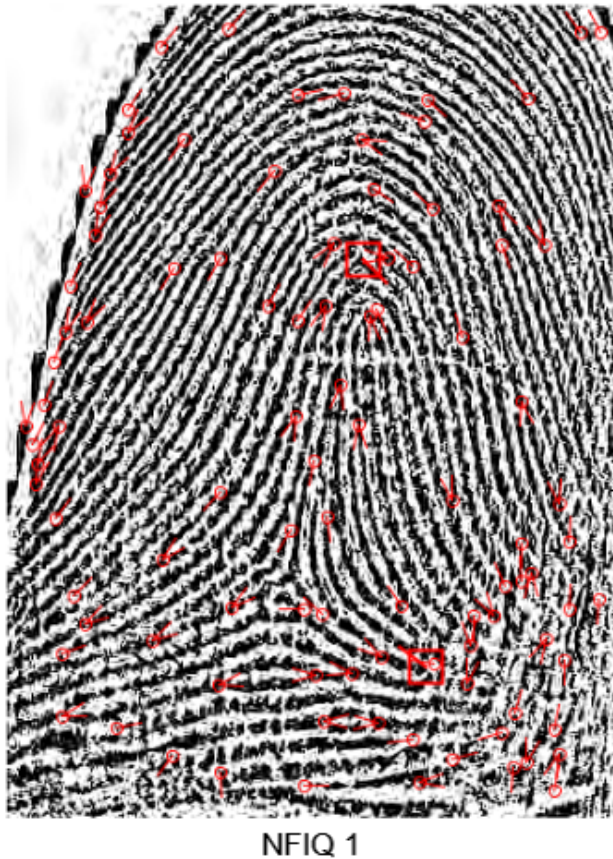
Para um melhor entendimento do algoritmo proposto, os passos intermediários do método são exibidos na figura 8, assim como o resultado final extraído (NFIQ 3) e com exibição das minúcias na figura 9.



Legenda:

- a) Flip - Imagem espelhada
- b) Segmentação - Imagem sem fundo
- c) Tons de cinza - Imagem em tons de cinza
- d) Inversão - Imagem com cores invertidas
- e) CLAHE - Imagem com aplicação do CLAHE
- f) Binarização - Imagem binarizada
- g) Crop - Imagem recortada no centro

**Figure 8.** imagem obtida após cada etapa do processamento em série



**Figure 9.** Imagem processada pelo algoritmo proposto com minúcias

Percebe-se uma grande melhoria na visualização das minúcias da foto original, sendo relativamente fácil de comparar-se visualmente duas biometrias extraídas pelo método proposto, que juntamente com o NFIQ 1 extraído (dentro dos parâmetros aceitáveis internacionalmente) comprova a eficácia do algoritmo. É importante ressaltar que embora o NFIQ 1 obtido nessa biometria seja equivalente ao obtido nos testes iniciais, o valor inicial foi provavelmente mascarado por uma “falha” na implementação do NFIQ 1.0, que por apresentar mais pontos condizentes com possíveis minúcias fez com que o score fosse maior, executando o NFIQ 2.0 sobre a mesma biometria foi obtido um score de 42, que seria equivalente a um NFIQ 1.0 de 3. Essa “falha” na implementação do NFIQ 1.0 foi corrigida na implementação do NFIQ 2.0 [41] que melhora a qualidade da validação e consegue distinguir melhor entre os níveis de qualidade, já que essa possui uma avaliação de 0 a 100.

Cabe ressaltar que o código de extração e comparação de biometrias utilizou a API disponibilizada pela BRy Tecnologia que utiliza o SDK da Neurotechnology, sendo assim, não há uma grande implementação por conta do autor.

### 4.3 Desempenho do algoritmo

Após a implementação de todos os algoritmos exibidos na seção anterior, é necessário garantir que estes sejam execu-

tados rapidamente, não impedindo o uso em larga escala. Portanto foi realizada uma análise no tempo de execução dos filtros, e praticamente todos eles se mostraram bem eficazes, com tempo de execução na casa de algumas dezenas ou centenas de milissegundos, o que é completamente aceitável para processamento das imagens. Porém o filtro de segmentação executa em um tempo variável, com forte dependência da imagem, onde em imagens com poucos detalhes ao fundo (pouca variação) e pequenas (aproximadamente 800 x 800 pixels) é possível concluir a segmentação em média em 600ms, porém em imagens maiores e com mais detalhes o filtro pode levar até 5s para finalizar a execução.

Na tentativa de sanar o problema de tempo de execução do algoritmo de remoção de fundo proposto inicialmente, foi realizada uma nova busca na literatura para a implementação de um novo método mais eficiente. Apesar de na nova implementação o resultado estar correto e até melhor que o resultado obtido no algoritmo inicial, assim como o tempo de execução ter diminuído de uma média de 3s para 600ms, o algoritmo proposto não consegue remover corretamente o fundo em todos os casos, o que é mais impactante para a aplicação do que o baixo desempenho obtido no primeiro exemplo. Desta forma, para os objetivos deste trabalho, optou-se por utilizar o primeiro algoritmo, deixando a otimização como um trabalho futuro, já que este funciona para todos os casos.

Com isso conclui-se que os algoritmos possuem um bom tempo de execução, tendo uma pequena demora na conclusão somente em imagens maiores e com muitos detalhes no fundo, porém no pior dos casos testados o tempo foi de 5s e com tempo médio de 900ms, o que é aceitável, já que esse algoritmo será executado uma única vez no momento da coleta dos dedos, não impactando na base final.

### 4.4 Desenvolvimento da API

Nesta seção será descrita a API desenvolvida. Esta API foi criada por meio do Postman com documentação e exemplos de uso. A API é composta por quatro endpoints, sendo um deles responsável exclusivamente pelo processamento de imagem, outro por extrair os templates (realizando ou não o tratamento de imagem), e dois para verificação biométrica, onde um deles é exclusivo para verificar dois templates já extraídos, e o segundo para processar as imagens caso necessário, extrair e verificar os dois templates obtidos.

O primeiro dos endpoints pertencentes a API do Fingerprint Photo Matcher é o endpoint de processamento da imagem, que pode ser acessado via REST por uma chamada POST para a URL da aplicação (localhost:8080 se executada localmente) e path /process-image, informando no body um json contendo o base64 da imagem a ser processada. Após realizada a chamada para o process-image, o base64 da imagem processada é retornado no corpo da resposta.

A API possui também o endpoint de extração de template, que pode ser requisitado via POST na URL da aplicação com path /extract-template. No body da requisição é necessário informar um json contendo um booleano de avaliação de



qualidade (retornando o NFIQ) e a lista de biometrias a serem avaliadas contendo o nome da biometria, base64 e booleano processImage para processar a imagem caso seja uma foto e não um WSQ. O retorno é composto pelo template e pela lista de biometrias com o nome, NFIQ e base64.

Já o endpoint de verificação que também realiza o processamento de imagens pode ser acessado pelo path /verify através de uma chamada POST com body contendo duas estruturas iguais ao endpoint de extração encapsuladas em cada template. O retorno desse endpoint contém um json com a operação solicitada, resultado da operação (match ou não), score, resultado esperado (utilizado em testes) e descrição.

Por fim, existe o endpoint de verificação de templates, um POST com path /verify-templates que possui o mesmo retorno do endpoint anterior, porém com estrutura json da requisição mais simples, contendo apenas os dois templates a serem validados (que podem ser obtidos a partir do endpoint de extração).

Portanto está definida a interface de utilização da API proposta para este trabalho.

## 5. Experimentação e análise dos resultados

Neste capítulo serão apresentados os resultados dos experimentos realizados com o Fingerprint Photo Matcher. O objetivo desses experimentos é demonstrar que o método proposto pode ser utilizado para identificar uma pessoa, e que pode ser utilizado em larga escala para os mais variados fins.

Para garantir que os testes sejam confiáveis é preciso obter uma base de dados completa, vasta e com todos os casos possíveis, com o objetivo de testar o processamento e a verificação biométrica. Para popular a base foram coletados todos os 10 dedos do autor duas vezes a partir da leitora especializada já citada anteriormente (Suprema Biomini Slim S20) e armazenados em WSQs, formando uma base de 20 dedos obtidos tradicionalmente. Já para a parte da base que contém as fotos dos dedos, foram realizadas 4 fotos de cada dedo do autor, totalizando 40 fotos.

Com a base formada é possível executar 3600 comparações biométricas, sendo este um número considerável. Cabe ressaltar que quanto maior a base melhor seria a validade do teste, porém fazer a coleta de biometrias de terceiros para exposição neste trabalho exige um processo de aprovação em conselho de ética, optando-se por deixar para trabalhos futuros.

### 5.1 Base de testes

Assim como já mencionado anteriormente, foram obtidas 60 biometrias no total, sendo 20 destas WSQs obtidas tradicionalmente e as 40 restantes são fotos dos dedos obtidas a partir de um smartphone Samsung Galaxy S20.

Para a composição da base final de biometrias obtidas por fotos foram feitos diversos testes, os testes consistiram de inúmeras fotos do dedo do autor capturadas de maneiras variadas, por exemplo, com os dedos abertos ou fechados, com apenas um dedo levantado, com o fundo uniforme ou

não e também com o fundo próximo ou distante. Algumas imagens de exemplificação dos métodos mencionados podem ser visualizadas na figura 10:

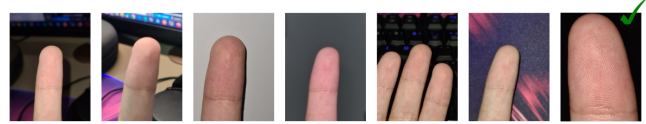


Figure 10. Exemplos de captura

Após os testes foi definido um método de captura que permite uma melhor qualidade visual das minúcias, portanto todas as biometrias obtidas por foto que compõem a base foram obtidas seguindo o mesmo procedimento. Este método de coleta de biometrias consiste em: Capturar uma foto do dedo com ele distante dos outros, utilizar a câmera de zoom do smartphone, deve-se aproximar o dedo o máximo possível da lente da câmera e manter o fundo bem distante, por fim utilizar as configurações de HDR e flash ativadas.

Ao utilizar o flash, garante-se uma iluminação adequada para capturar os detalhes essenciais das impressões digitais, somado ao fundo distante ajuda a criar um contraste que evidencia somente o dedo na imagem e “apagando” o fundo. Dessa forma, o resultado final é uma foto com a biometria em primeiro plano e um fundo uniforme preto (como exposto anteriormente na figura 10 na imagem com uma marcação verde), destacando claramente as características biométricas do dedo.

É fundamental ressaltar que, após as diversas tentativas de captura, experimentando várias posições do dedo e diferentes fundos, o método descrito revelou-se a melhor maneira de garantir uma imagem clara e detalhada, que permita a precisão e confiabilidade do processo de reconhecimento biométrico. O uso de um fundo uniformemente preto é uma consequência dessa abordagem, com o objetivo de eliminar distrações visuais que possam comprometer a análise e a identificação biométrica. Ao utilizar outros métodos de captura, as imagens obtidas frequentemente contêm um excesso de informações além do dedo, o que pode resultar em distração e falta de foco na área de interesse durante o processamento dessas imagens, como exibido anteriormente na figura 10.

Por fim, para a composição da base foi realizado um pequeno recorte de todas as imagens para que estas contivessem somente a ponta dos dedos e que o centro das minúcias (core) estivesse no centro da imagem. Isso é importante para uma melhor comparação biométrica e garantia do processamento correto. Por conta da complexidade de implementação optou-se pela utilização das imagens obtidas desta maneira, porém idealmente deveria ser utilizado um aplicativo mobile que indique e auxilie na obtenção da foto, além de já fazer um recorte na zona de interesse.

### 5.2 Testes de processamento

A primeira experimentação necessária para validar a qualidade do algoritmo de processamento desenvolvido é a validação do



processamento das imagens, exibindo a imagem pós-processada e extraindo o template biométrico a partir dela, sendo possível então exibir o NFIQ obtido para a biometria e também a imagem com as minúcias detectadas expostas.

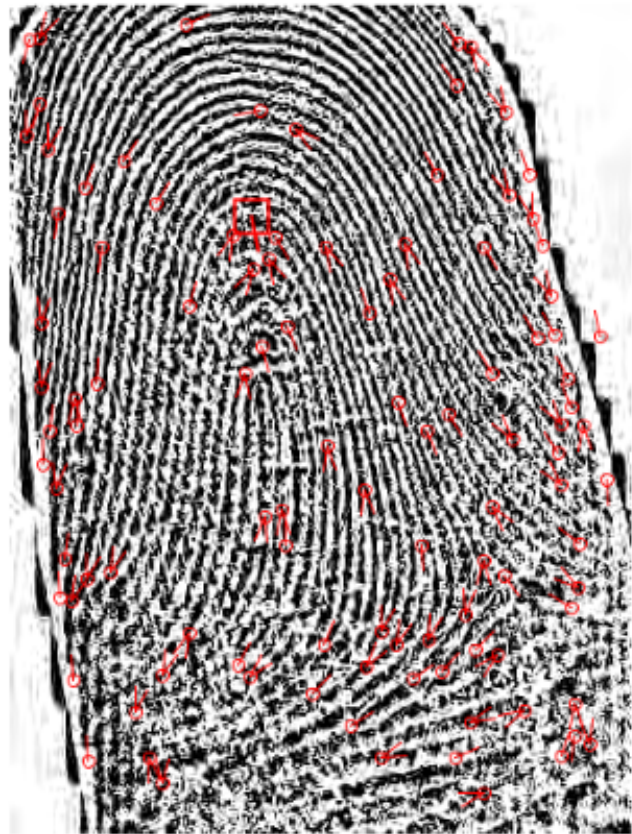
Para isso foi desenvolvido o teste de processamento de imagens, nessa etapa o sistema irá ler todas as biometrias que compõem a base para processá-las uma a uma com o método de processamento já exibido anteriormente e após a execução deste método irá chamar o extrator da Neurotechnology para extrair, validar o NFIQ e exibir as minúcias obtidas em uma nova foto PNG.

Para que seja possível compreender o resultado final detalhado na seção 5.4 é necessário primeiro entender os resultados obtidos nesta etapa das experimentações, portanto será ilustrado cada passo com o resultado obtido. Uma das 40 biometrias que compõem o banco de testes de imagens obtidas por smartphone está exposta a seguir na figura 11.



**Figure 11.** Foto do dedo do autor (LEFT\_HAND\_MIDDLE-1)

Após a execução do teste para este dedo em específico foi obtido após o passo de processamento de imagem uma biometria com NFIQ 2 como disponível após a execução do passo de extração, que pode ser visto com as minúcias em destaque na figura 12.



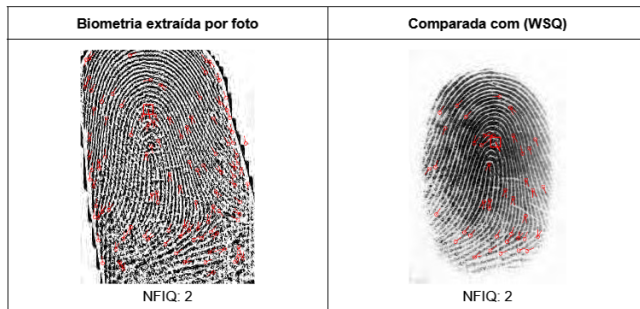
NFIQ 2

**Figure 12.** Foto do dedo do autor processada pelo algoritmo proposto com minúcias (LEFT\_HAND\_MIDDLE-1)

É evidente a melhora na exibição das minúcias após o processamento e também que a extração pode ser executada sem problemas gerando um bom template biométrico. Vale ressaltar que para a imagem obter o melhor resultado e poder ser comparada mais facilmente com os WSQs posteriormente, é necessário que a imagem seja redimensionada para conter 500 ppi, ou seja, possuir o mesmo tamanho das capturas feitas por leitores especializados tradicionais, já que o extrator e matcher utilizados seguem os padrões para hardwares especializados.

Por conta disso as fotos presentes na base de imagens foram todas redimensionadas para conter aproximadamente 500 ppi, juntamente do crop realizado no algoritmo proposto, porém seria muito importante possuir um método para automatizar o redimensionamento para 500 ppi, que não será explorado neste momento, ficando como uma melhoria para trabalhos futuros.

Após a exibição do WSQ com as minúcias fica evidente que a comparação visual entre os dois métodos é extremamente possível, e possuindo um treinamento de papiloscopia é fácil de identificar que as duas biometrias pertencem a mesma pessoa, assim como evidenciado na figura 13.



**Figure 13.** Foto processada ao lado de um WSQ

Um fato muito importante percebido na execução do teste descrito nesta seção é que o algoritmo de processamento de imagem está bem otimizado, trazendo bons resultados em um tempo baixo, levando em média um segundo para processar cada dedo. Cabe ressaltar que os mais de 60 processamentos estão disponíveis no repositório do projeto para uma avaliação completa dos testes realizados nesta etapa.

### 5.3 Testes de verificação

Após a experimentação bem sucedida do processamento das fotos é necessário prosseguir com a avaliação do método proposto e confirmar que este é capaz de verificar biometrias independente do tipo de captura e armazenamento. Portanto, é preciso realizar uma comparação (1:1) com todas as biometrias pertencentes a base.

Nesta etapa do teste o sistema irá comparar todas as biometrias obtidas por fotos do dedo entre si, depois compará-las com todos os WSQs coletados por meio dos leitores ópticos especialistas e por fim comparar todos os WSQs entre si. A verificação biométrica irá utilizar o matcher da Neurotechnology já mencionado anteriormente.

Para exemplificar melhor o resultado obtido após a execução da etapa será novamente utilizado como base o dedo já exibido na etapa anterior, para este dedo foram executado alguns testes, entre eles a verificação (1:1) entre o próprio dedo obtido por imagens com ele mesmo, resultando em um match com score de 2700.

Já a comparação entre o dedo 1 obtido por leitoras especializadas com ele mesmo resultou em match com score de 1555.

E por fim a verificação entre o dedo obtido por foto com o mesmo dedo obtido pela leitora resultou também em um match biométrico e desta vez com score 165, indicando um FAR de menos de 0,000001%, o que é um valor excelente.

Foram executados ainda mais de 3600 comparações seguindo o mesmo formato exposto acima, onde a maioria deve resultar em não batimento biométrico já que não se tratam do mesmo dedo, todos os testes estão disponíveis no repositório do projeto e não serão detalhados nessa seção, porém será analisado o resultado final dos testes na seção 5.4.

### 5.4 Análise dos resultados

Após a execução das etapas detalhadas nas seções anteriores o teste gera ainda alguns relatórios com detalhamento dos

resultados obtidos nos testes, permitindo assim uma validação da qualidade do método proposto e uma resposta para cada uma das questões que fundamentaram os testes.

Os dois relatórios que exibem o resultado do processamento das biometrias possuem a mesma estrutura e indicam quantas biometrias foram processadas e qual a quantidade de biometrias para cada valor de NFIQ possível, lembrando que variam de 1 a 5 sendo 1 o melhor.

Para o processamento de biometrias obtidas por fotos foi obtido o seguinte relatório: Foram processadas 41 fotos e destas 41, 13 possuem NFIQ 1, 10 possuem NFIQ 2, uma possui NFIQ 3, 15 possuem NFIQ 4 e duas possuem NFIQ 5, ou seja, 24 de 41 estão dentro dos valores aceitáveis internacionalmente. Por conta disso o resultado das verificações posteriores pode ser negativamente afetado, já que com uma base de menor qualidade a verificação tende a não ser possível em todos os casos.

Já para as biometrias obtidas por scanners especializados o seguinte relatório foi gerado: Foram processadas 22 biometrias, 10 destas possuem NFIQ 1, 11 possuem NFIQ 2 e apenas uma possui NFIQ 3, sendo todas as 22 biometrias aceitas pelos padrões internacionais, o que deve levar a um impacto positivo na verificação entre si.

Para a etapa de verificação das biometrias obtidas por foto obtivemos o seguinte resultado: Foram executados 1681 verificações 1:1 entre as fotos e destas foram obtidos 1548 não correspondências de um total de 1508 esperadas, possuindo uma incidência de 102,65% de não correspondência, ou seja, recusando mais do que deveria, além de 133 correspondências de um total esperado 173 o que representa uma incidência de 76,87%. É possível visualizar também o estudo das taxas obtidas, que a partir de uma ocorrência de zero falsas aceitações, 40 falsas rejeições, 133 aceitações verdadeiras e 1508 rejeições verdadeiras foi obtido uma taxa de FAR de 0% (pelo score o FAR deve ser de 0,001%), FRR de 2,37%, TAR de 76,87%, TRR de 100% e EER de 1,18% e por fim totalizando um acerto geral de 97,62% das comparações. Estes valores obtidos podem ser considerados ótimos internacionalmente e suficientes para uma primeira versão do método proposto, já que a base de biometrias extraídas por um smartphone possui uma baixa qualidade de NFIQ, sendo os valores obtidos melhores do que o recomendado para um sistema de validação facial.

Podemos concluir que o sistema validou corretamente a maioria dos casos tendo como problema somente uma rejeição maior do que o esperado, dificultando a usabilidade mas mantendo a segurança muito elevada, já que não validou ninguém não autorizado.

Para as verificações de foto com WSQ obtivemos o seguinte relatório: Foram executados 902 verificações 1:1 entre fotos e WSQs obtendo-se 829 não correspondências de um total de 810 esperadas, possuindo uma incidência de 102,34% de não correspondência, ou seja, novamente recusando mais do que deveria, além de 73 correspondências de um total esperado 92 o que representa um acerto de 79,34%, número acima do

resultado anterior, o que comprova que a base de qualidade maior dos WSQs é impactante. As taxas obtidas são calculadas a partir de uma ocorrência de zero falsas aceitações, 19 falsas rejeições, 73 aceitações verdadeiras e 810 rejeições verdadeiras que levam a uma taxa de FAR de 0% (pelo score o FAR deve ser de 0,001%), FRR de 2,10%, TAR de 79,34%, TRR de 100% e EER de 1,05% e por fim totalizando um acerto geral de 97,89% das comparações. Novamente os valores obtidos podem ser considerados bons, já que a base de imagens (fotos de smartphones) possui uma baixa qualidade de NFIQ, o que impacta diretamente na verificação, causando uma diminuição da aceitação de usuários.

Por fim está o relatório de verificação entre os WSQs, neste relatório todas as 484 verificações conseguiram ter exatamente o resultado esperado, comprovando a qualidade da base, extrator e matcher envolvidos no teste. As taxas obtiveram os melhores valores possíveis, sendo 0% para FAR e FRR, ou seja, não houve falsas verificações, e 100% do TAR e TRR, ou seja, todas as verificações foram verdadeiras, o que resulta em um EER de 0% que é o melhor valor possível. Cabe ainda destacar que a execução de todas as etapas de teste e geração dos relatórios leva em média três minutos, o que é um tempo muito bom já que estão sendo realizados mais de 3600 comparações e mais de 60 processamentos.

Por fim é possível comprovar que o método sugerido é eficaz para resolver a demanda proposta com uma taxa média aproximada de FAR de 0,001%, TAR de 77% e EER de 1% (considerados excelentes pelo NIST), e que mesmo com a base de imagens estando composta por quase metade das biometrias com baixa qualidade o resultado foi bem expressivo e aceitável dentro dos parâmetros internacionais. Vale ressaltar que a base de imagens foi obtida sem muito esforço e com um método simples, caso esta seja melhorada será obtido um resultado melhor ainda, pois é possível averiguar que os baixos NFIQs são os provenientes dos resultados incorretos na verificação.

Para confirmar que os baixos NFIQs impactam negativamente o resultado das comparações, foi executada uma segunda bateria de testes com a utilização somente dos dados com NFIQ menor ou igual a 3. Com isso o resultado obtido foi melhorado drasticamente, aumentando o TAR de verificações entre fotos de 76,97% para 84,21% e melhorando em poucas casas decimais as outras taxas, além de aumentar o TAR de verificações entre WSQs de 79,34% para 83,63% e melhorando também em poucas casas decimais os valores das outras taxas.

Portanto é possível assegurar todas as perguntas que motivaram os testes, sendo o método proposto eficaz (capaz de identificar um indivíduo corretamente), seguro (tem um nível de qualidade de comparação aceito internacionalmente), performático, aplicável a qualquer fim e muito fácil de utilizar com a API desenvolvida.

## 6. Conclusões e Trabalhos futuros

Nos últimos anos observou-se uma tendência cada vez maior no uso de identificação biométrica, aliado ao crescimento do uso dos smartphones. Ainda neste período houve o início de uma pandemia global, onde as pessoas foram forçadas a descobrir maneiras de não entrarem em contato umas com as outras, o que voltou os olhares para métodos de autenticação biométrica seguros que não necessitassem de contato.

O levantamento do estado da arte realizado neste trabalho demonstrou que ainda não existe nenhum meio seguro e eficaz para identificar as pessoas sem necessitar de contato. Existem alguns modelos propostos para cobrir essa lacuna, porém todos carecem de alguns detalhes importantes e principalmente são difíceis de serem aplicados em larga escala, possuindo um valor de implantação elevado.

Por conta disso, o objetivo geral deste trabalho foi apresentar um modelo de identificação biométrica para validação das impressões digitais sem que haja a necessidade de contato, para isso foi utilizado a câmera presente nos smartphones. Para atender este objetivo, alguns objetivos específicos foram perseguidos, que são: Extração de impressões digitais a partir de uma foto processada, validação da qualidade das biometrias obtidas bem como níveis de FAR e TAR obtidos independente do método de obtenção da biometria e desenvolvimento de uma API REST que disponibilize de maneira fácil a utilização do modelo desenvolvido.

Este trabalho apresentou um método proposto para executar uma verificação biométrica por impressões digitais obtidas a partir de uma simples foto de smartphone, de maneira a evitar o contato das pessoas com uma leitora e diminuir o custo para a validação da biometria.

O trabalho pode ser dividido em três partes principais. A primeira delas consiste na revisão dos fundamentos teóricos para o desenvolvimento do método proposto, assim como a revisão do estado da arte das verificações biométricas sem contato. Sendo esta uma parte crucial para o entendimento do objetivo e definição da proposição final deste trabalho.

A segunda parte abrange o desenvolvimento da aplicação que realiza todo o processamento necessário para atingir o resultado esperado. Buscou-se utilizar métodos simples e fáceis de serem implementados para que a execução se realizasse em um tempo baixo. Foram necessários vários micro testes para a obtenção dos algoritmos de processamento parciais, assim como o algoritmo final.

E a terceira parte do trabalho consiste na criação, execução e validação dos testes. Nessa etapa procurou-se exibir os dados de uma maneira simples e que fosse capaz de validar que o método proposto é capaz de validar corretamente uma verificação biométrica dentro dos padrões internacionais. Desta maneira alcançou-se o objetivo proposto para o projeto.

De acordo com os objetivos definidos para este trabalho, pode-se listar várias contribuições como um detalhamento de como funciona o processo de identificação biométrica, análise de minúcias e tratamento de imagens. Também foi possível desenvolver um método capaz de processar fotos obtidas através



de smartphones, ou qualquer câmera comum, extraí-las em um template biométrico e realizar uma comparação 1:1 de fotos com WSQs ou outras fotos, mantendo a qualidade e taxa de FAR dentro de 0.001% que é considerado ótimo internacionalmente.

Cabe ressaltar que o método sugerido é eficaz para resolver a demanda proposta com uma taxa média aproximada de FAR de 0,001%, TAR de 77% e EER de 1% (considerados excelentes pelo NIST), e que mesmo com a base de imagens estando composta por quase metade das biometrias com baixa qualidade o resultado foi bem expressivo e aceitável dentro dos parâmetros internacionais. Considerando somente biometrias com NFIQ 1 a 3 os valores obtidos foram de FAR de 0,001%, TAR de 83% e EER de 1%.

Além disso foi realizada uma revisão dos trabalhos relacionados na área, mostrando as principais diferenças entre cada trabalho, bem como a utilização de maneiras não tradicionais no processamento das imagens e o desenvolvimento de uma API REST para o método de verificação proposto, a fim de tornar simples a utilização por qualquer pessoa. Diferentemente dos outros trabalhos na área, este levou em consideração NFIQ e fez uma validação completa das taxas de qualidade, além de também focar em como obter as biometrias.

Como continuação deste trabalho, pode ser realizada uma busca por algoritmos de tratamento de imagens, junto com a busca de novos filtros que possam realçar mais as minúcias da foto tirada, independente das condições, facilitando a extração da digital. Buscar por uma boa implementação do filtro de Gabor, que possua um filtro de estimativa de orientação das elevações da impressão digital, assim como um filtro de estimativa de frequência dessas elevações.

Também para ajudar no processamento de biometrias e testes, realizar uma longa sessão de coleta, armazenando várias biometrias com diferentes índices de qualidade (extraídas pelos sensores tradicionais) e várias fotos de outros smartphones e câmeras, as quais serão posteriormente processadas. Assim como a coleta de biometrias de mais pessoas, a fim de compor uma base realmente vasta e completa. Implementar uma forma de testes automatizados considerando toda a nova base, levantando relatórios mais completos que os dispostos aqui. Ainda no ramo da coleta, é possível estudar as melhores maneiras de obtenção da foto e até mesmo o desenvolvimento de um APP que detecta a zona de interesse dos dedos e faz um recorte automático da área, auxiliando na captura, e ainda fazendo com que a imagem seja automaticamente redimensionada para conter 500 ppi na zona de interesse. Para facilitar ainda mais a coleta o ideal seria tirar apenas a foto da mão e a partir desta executar um recorte em cada dedo.

Outra melhoria a ser realizada seria a utilização de um novo algoritmo de segmentação, pois o algoritmo utilizado não se mostrou capaz de funcionar em qualquer cenário, demorando consideravelmente para imagens grandes e detalhadas. Por fim criar uma forma de validação de prova de vida, já que a prova de vida de um dedo depende fortemente

de confiança no dispositivo utilizado para a captura (leitoras medem radiação infravermelha) e no acompanhamento de um terceiro confiável. Para desenvolver essa validação poderia ser utilizado uma coleta com mais frames e IA para detectar o movimento do dedo e fazer uma captura "3D" com aproximação e afastamento do dedo, com o objetivo de provar que é uma pessoa de fato viva.

## Referências

- [1] CERTISIGN. *Qual é a relação entre a impressão digital e a sua personalidade?* 2017. <https://blog.certisign.com.br/qual-e-a-relacao-entre-a-impressao-digital-e-a-sua-personalidade/>. Acesso em 20 jul. 2022.
- [2] MARCONDES, J. S. *Biometria, Sistema Biométrico: O que é, Como Funciona?* 2020. Blog Gestão de Segurança Privada <https://gestaodesegurancaprivada.com.br/biometria-sistema-biometrico-o-que-e-como-funciona/>. Acesso em 19 jul. 2022.
- [3] GOGONI, R. *O que é biometria? Os 6 tipos mais usados na tecnologia.* 2019. <https://tecnoblog.net/responde/o-que-e-biometria-tecnologia/>. Acesso em 21 jul. 2022.
- [4] HANSEN, L. *Is Biometric Technology Worth the Cost?* 2021. <https://www.cioinsight.com/infrastructure/biometric-technology/#:~:text=How%20Much%20Does%20Biometric%20Security,little%20as%20%2420%20per%20device>. Acesso em 20 jul. 2022.
- [5] NEUROTECHNOLOGY. *NEUROtechnology.* 2022. <https://www.neurotechnology.com/>. Acesso em: 01 mar. 2022.
- [6] NEC. *How is biometric data stored?* 2022. <https://www.nec.co.nz/market-leadership/publications-media/how-is-biometric-data-stored/>. Acesso em 20 jul. 2022.
- [7] DRULLIS, G. *Serpro abre edital para solução de captura de digitais com câmera do celular.* 2022. <https://www.mobiletime.com.br/noticias/25/07/2022/serpro-abre-edital-para-solucao-de-captura-de-digitais-com-camera-do-celular>. Acesso em 20 nov. 2022.
- [8] ONESPAN. *Autenticação biométrica: Definição, tendências, prós e contras, casos de uso e mitos.* 2022. <https://www.onespan.com/pt-br/topics/autenticacao-biometrica#:~:text=A%20autentic%C3%A7%C3%A3o%20biom%C3%A9trica%20%C3%A9%20um,e%20outros%20recursos%20de%20rede>. Acesso em 20 jul. 2022.
- [9] MARY, C. *Minutiae Based Extraction in Fingerprint Recognition.* 2022. Bayometric. <https://www.bayometric.com/minutiae-based-extraction-fingerprint-recognition/>. Acesso em 20 jul. 2022.
- [10] STROMBERG, J. *Adermatoglyphia: The Genetic Disorder Of People Born Without Fingerprints.* 2014.



- <https://www.smithsonianmag.com/science-nature/adermatoglyphia-genetic-disorder-people-born-without-fingerprints-1809493032>). Acesso em 20 jul. 2022.
- [11] WATSON, S. *How Fingerprinting Works*. 2008. <https://science.howstuffworks.com/fingerprinting3.htm>). Acesso em 20 jul. 2022.
- [12] MÁRCICO, J. E. *Papiloscopia*. 2022. <http://www.papiloscopia.com.br/historia.html>). Acesso em 20 jul. 2022.
- [13] BANSAL, R.; SEHGAL, P.; BEDI, P. *Minutiae Extraction from Fingerprint Images - a Review*. 2011. <https://arxiv.org/ftp/arxiv/papers/1201/1201.1422.pdf>). Acesso em 21 jul. 2022.
- [14] NIST. *NFIQ 2*. 2021. <https://www.nist.gov/services-resources/software/nfiq-2>). Acesso em 20 jul. 2022.
- [15] LIBERT, J.; ORANDI, S.; GRATHAM, J. *Comparison of the WSQ and JPEG 2000 Image Compression Algorithms On 500 ppi Fingerprint Imagery*. 2012. <https://www.govinfo.gov/content/pkg/GOVPUB-C13-cc24a731f16cb865d9164f88def784ee/pdf/GOVPUB-C13-cc24a731f16cb865d9164f88def784ee.pdf>). Acesso em 21 jul. 2022.
- [16] KHANDELWAL, S. *Hacker Clones German Defense Minister's Fingerprint Using Just her Photos*. 2014. The Hacker News <https://thehackernews.com/2014/12/hacker-clone-fingerprint-scanner.html>). Acesso em 01 mar. 2022.
- [17] VIANA, R. *Deepfakes: como vídeos falsos são usados para burlar sistemas de segurança*. 2022. <https://www.combateafraude.com/post/deepfakes-videos-falsos-seguranca>). Acesso em 21 jul. 2022.
- [18] SUPREMA. *Suprema's Live Finger Detection Technology*. 2016. [http://kb.supremainc.com/knowledge/doku.php?id=en:tc\\_whitepaper\\_suprema\\_live\\_finger\\_detection](http://kb.supremainc.com/knowledge/doku.php?id=en:tc_whitepaper_suprema_live_finger_detection)). Acesso em 31 dez. 2022.
- [19] MARY, C. *Biometric Glossary: Technical Terms and Definitions*. Bayometric. 2022. Bayometric. <https://www.bayometric.com/biometric-glossary-terms-definitions/>). Acesso em 20 jul. 2022.
- [20] MAJHI, B.; AL. et. *Machine Learning for Biometrics: Concepts, Algorithms and Applications*. 2022. <https://www.sciencedirect.com/book/9780323852098/machine-learning-for-biometrics>). Acesso em 22 jul. 2022.
- [21] INNOVATRICS. *Equal Error Rate (EER)*. 2022. <https://www.innovatrics.com/glossary/equal-error-rate-eer/#:~:text=A%20statistic%20used%20to%20show,accuracy%20of%20the%20biometric%20system>). Acesso em 20 mar. 2023.
- [22] MARY, C. *False Acceptance Rate (FAR) and False Recognition Rate (FRR) in Biometrics*. 2022. Bayometric. <https://www.bayometric.com/false-acceptance-rate-far-false-recognition-rate-frr/>). Acesso em 20 jul. 2022.
- [23] ANDRESS, J. *Basics of Information Security (Second Edition)*. 2014. <https://www.sciencedirect.com/topics/computer-science/false-acceptance-rate>). Acesso em 22 jul. 2022.
- [24] NEUROTECHNOLOGY. *Technology Awards*. 2023. Bayometric. <https://www.neurotechnology.com/megamatcher-abis-awards.html>). Acesso em 31 mar. 2023.
- [25] FVC-ONGOING. *Published Results: Fingerprint Verification*. 2023. <https://biolab.csr.unibo.it/fvcongoing/UI/Form/PublishedAlgs.aspx#&&rURsNOBN92xHvjxPZGC6ijhPFRM/3jvSgQW4k4kb2N6WSmFNBeVjER/ctEmy/LeYAsEnQJS7YXm2S1n0FG6OE4di3+jYBjmpFdvXB3dvT1n2z6HIFGmNiFluVZ3bAC1enEVaTMxzFy28IIGYD>). Acesso em 02 fev. 2023.
- [26] NICE, K.; WILSON, T. V.; GUREVICH, G. *How Digital Cameras Work*. 2006. <https://electronics.howstuffworks.com/cameras-photography/digital/digital-camera.htm>). Acesso em 22 jul. 2022.
- [27] SONY. *Qual é a diferença entre pontos por polegada (DPI) e Pixels por polegada (PPI)?* 2015. <https://science.howstuffworks.com/fingerprinting3.htm>). Acesso em 02 fev. 2023.
- [28] IPSISPRO. *Aprenda tudo sobre lentes fotográficas agora*. 2019. <https://blog.ipsispro.com.br/tudo-sobre-lentes-fotograficas>). Acesso em 22 jul. 2022.
- [29] OPENCV. *Histograms - 2: Histogram Equalization*. 2022. [https://docs.opencv.org/4.x/d2/d74/tutorial\\_js\\_histogram\\_equalization.html](https://docs.opencv.org/4.x/d2/d74/tutorial_js_histogram_equalization.html)). Acesso em 21 nov. 2022.
- [30] GIOVANINI, A. *Filtro Passa Alta?* 2022. <https://adenilsongiovanini.com.br/blog/filtro-passa-alta-o-que-e-e-para-que-serve/>). Acesso em 30 jul. 2022.
- [31] SOUZA, G. de M. *Laplaciano do Gaussiano*. 2016. <https://melosgabriel.github.io/pdi/6.Filtro-Espacial/#:~:text=Como%20vimos%20nas%20aulas%20da,suavizante%2C%20para%20eliminarmos%20os%20ru%C3%ADdos>). Acesso em 20 jul. 2022.
- [32] DATAGEN. *Image Segmentation: The Basics and 5 Key Techniques*. 2022. <https://datagen.tech/guides/image-annotation/image-segmentation/>). Acesso em 04 jan. 2023.
- [33] OTSU. *A threshold selection method from gray-level histograms*. 1979. IEEE Trans. Systems, Man, and Cybernetics, 9(1), p. 62–66 (1979). Acesso em 30 jul. 2022.
- [34] ADOBE. *How to switch up your color scheme*. 2022. <https://www.adobe.com/creativecloud/photography/discover/invert-colors.html>). Acesso em 04 jan. 2023.

- [35] THAI, R. *Fingerprint Image Enhancement and Minutiae Extraction*. 2003. <https://www.peterkovesi.com/studentprojects/raymondthai/RaymondThai.pdf>. Acesso em 21 jul. 2022.
- [36] KUMAR, A.; KWONG, C. *Towards Contactless, Low-Cost and Accurate 3D Fingerprint Identification*. 2015. IEEE Transactions on Pattern Analysis and Machine Intelligence, v. 37, n. 3, p. 681-696, 1 March 2015, doi: 10.1109/TPAMI.2014.2339818. Acesso em 30 jul. 2022.
- [37] CHOI, H.; CHOI, K.; KIM, J. *Mosaicing Touchless and Mirror-Reflected Fingerprint Images*. 2010. IEEE Transactions on Information Forensics and Security, v. 5, n. 1, p. 52-61, Mar. 2010, doi: 10.1109/TIFS.2009.2038758. Acesso em 30 jul. 2022.
- [38] CHOWDHURY, A. M. M.; IMTIAZ, M. H. *Contactless Fingerprint Recognition Using Deep Learning - A Systematic Review*. 2021. <https://www.researchgate.net/publication/363385196-Contactless-Fingerprint-Recognition-Using-Deep-Learning-A-Systematic-Review>. Acesso em 20 jul. 2022.
- [39] RAGHAVENDRA, R.; BUSCH, C.; YANG, B. *Scaling-robust fingerprint verification with smartphone camera in real-life scenarios*. 2013. IEEE Sixth International Conference on Biometrics: Theory, Applications and Systems (BTAS), 2013, p. 1-8, doi: 10.1109/BTAS.2013.6712736. Acesso em 30 jul. 2022.
- [40] GUPTA, S.; ANAND, S.; RAI, A. *Efficient Fingerprint Extraction and Matching Using Smartphone Camera*. 2017. <https://www.researchgate.net/publication/318899084-Fingerprint-Extraction-Using-Smartphone-Camera>. Acesso em 21 jul. 2022.
- [41] FIUMARA, G. *Releases: usnistgov/NFIQ2*. 2021. <https://github.com/usnistgov/NFIQ2/releases>. Acesso em 31 dez. 2022.