Fundação Universidade Federal do ABC
Pró reitoria de pesquisa
Av. dos Estados, 5001, Santa Terezinha, Santo André/SP, CEP 09210-580
Bloco L, 3ºAndar, Fone (11) 3356-7617
iniciacao@ufabc.edu.br

Projeto de Iniciação Científica submetido
para avaliação no Edital: 01/2024

**Título do projeto:** Avaliação de abordagens de ajuste de hiperparâmetros em dinâmica da digitação

**Palavras-chave do projeto:** biometria; aprendizado de máquina; ajuste de hiperparâmetros

**Área do conhecimento do projeto:** Ciências Exatas e da Terra; Ciência da Computação; Metodologia e Técnicas da Computação

## Resumo

O uso de biometria para autenticação de usuários, em oposição a métodos tradicionais baseados em senhas estáticas, têm sido atrativo em razão da maior segurança que um sistema biométrico pode proporcionar. Os usuários podem ser reconhecidos com base em características físicas ou comportamentais ao invés de precisarem se lembrar de uma senha ou a ter em mãos um cartão inteligente ou *token*. Dentre as diversas modalidades biométricas existentes, há a *dinâmica de digitação*, que reconhece as pessoas com base em seu ritmo de digitação. Diversos algoritmos de classificação podem ser usados nesse contexto. Esses algoritmos possuem hiperparâmetros, que precisam ser ajustados adequadamente. O ajuste de hiperparâmetros pode ser realizado para cada usuário individualmente ou pode ser global, isso é, os hiperparâmetros assumirão o mesmo valor para todos os usuários. O objetivo deste projeto é explorar diferentes abordagens de ajuste de hiperparâmetros em algoritmos para classificação para dinâmica de digitação.

# Sumário

# 1 Introdução

Nos últimos anos, a popularização de serviços oferecidos única e exclusivamente pela da Internet tem crescido de forma extraordinária. Muitas pessoas realizam pagamentos em sites de lojas diretamente de suas casas e gerenciam suas contas bancárias sem a necessidade de irem até os bancos (TERADA, 2008). Dessa forma, surge a necessidade sistemas de autenticação e identificação cada vez mais sofisticados.

Entretanto, na perspectiva de Ryu et al. (2023), a maioria dos sistemas de autenticação comumente usados são baseados em senhas estáticas, ou uma combinação entre uma senha e um cartão inteligente ou *tokens*. Peacock, Ke e Wilkerson (2004) destacam que essa abordagem possui uma série de limitações. Por exemplo, senhas compostas por palavras comuns, sequências numéricas ou alfanuméricas simples que sejam passíveis de memorização são consideradas "fracas" no que se refere ao nível de segurança que elas oferecem, pois podem ser descobertas por ataques do tipo "força bruta".

Peacock, Ke e Wilkerson (2004) ainda afirmam que é recomendado que os usuários criem senhas maiores e compostas por uma combinação de números, letras e caracteres especiais para serem menos vulneráveis a ataques. Em adição a isso, as senhas deveriam ser diferentes para cada conta nos sites em que acessam. Todavia, muitas vezes os usuários ainda optam pela utilização de uma mesma senha para todas as suas contas, o que gera um risco de segurança: se apenas um dos sistemas for invadido e tiver os seus dados roubados, o acesso aos dados do indivíduo em todos os outros serviços estará comprometido.

Segundo Jain, Ross e Pankanti (2006), muitas dessas limitações associadas ao uso de senhas podem ser contornadas pela incorporação de métodos de autenticação melhores. Nesse sentido, a biometria, como uma forma de estabelecer a identidade por meio de características físicas ou comportamentais dos indivíduos, surge como uma alternativa. Há diversas modalidades biométricas (JAIN; NANDAKUMAR; ROSS, 2016) que podem ser usadas tanto para identificação quanto para a verificação de usuários.

Neste projeto, será dado o enfoque na vertente física, em particular, na biometria através de impressões digitais. Essa modalidade biométrica se baseia nos padrões de pequenas elevações e depressões na pele da pontas dos dedos (JAIN; FLYNN; ROSS,

2007). Os usuários são então reconhecidos com base nas diferenças nesses padrões.

Conforme definido em (JAIN; ROSS; PRABHAKAR, 2004), sistemas biométricos são sistemas de reconhecimento de padrões que extraem características de dados biométricos e então comparam as características extraídas com uma referência biométrica em um banco de dados. Nesse sentido, Maltoni et al. (2022) explica que, para a autenticação através de digitais, a representação das características extraídas das imagens é um problema fundamentação da verificação de digitais.

Como não há a garantia de que as imagens da digital de um mesmo dedo nunca serão exatamente iguais em termos de intensidade de pixel, orientação e formato, há a necessidade de se extrair características a partir das quais seja possível diferenciar diferentes digitais com uma boa acurácia e que sejam invariantes para uma dada digital. Somente assim o uso de digitais em sistemas de autenticação se tornariam viáveis.

O objetivo deste trabalho é avaliar diferentes algoritmos e técnicas de extração de características de imagens de digitais e formas de representação. Sua avaliação será feita com base na sua performance em um cenário de verificação de usuários.

As demais seções do projeto estão organizadas da seguinte forma: na Seção 2, são introduzidos conceitos sobre digitais e as diferentes representações que podem ser extraídas delas; na Seção 3, são apresentados os objetivos; na Seção 4, é descrita a metodologia; na Seção 5, a viabilidade do projeto é discutida; e, na Seção 6, é apresentado o cronograma deste projeto.

# 2 Fundamentação teórica

Esta seção apresenta alguns conceitos importantes para este projeto de pesquisa envolvendo biometria através de impressões digitais.

## 2.1 Biometria por Impressão Digital

O termo "Impressão Digital"no contexto de biometria por digitais se refere ao padrão de pequenos cumes e vales que podem ser observados na ponta dos dedos das pessoas (JAIN; FLYNN; ROSS, 2007). Ao longo da evolução da raça humana o desenvolvimento de digitais está relacionado à capacidade de segurar objetos com as mãos, e o padrão específico de cumes e vales, assim como outras características do corpo, é definido por fatores genéticos e ambientais.

O reconhecimento de que as impressões impressões digitais são únicas para cada dedo de cada pessoa ocorreu em 1880 com base em observações experimentais de Henry Fauld (MOENSSENS, 1971). Em 1993 a unicidade de impressões digitais foi reconhecida por entidades governamentais do Reino Unido, e foi determinado que as digitais de criminosos seriam coletadas no momento da prisão. Dessa forma, os especialistas em investigação forense poderiam identificar criminosos com base em manchas de impressões digitais deixadas na cena de crime, chamadas de impressões digitais latentes. A partir disso, órgãos de segurança pública investiram intensamente em pesquisas sobre impressões digitais e no treinamento de especialistas em reconhecimento de digitais (SCOTT, 1951).

Conforme explica Maltoni et al. (2022), apesar dos esforços para tornar mais eficiente o processo manual de identificação por impressões digitais, o aumento da demanda tornou esse método inviável. O sistema de classificação manual era ineficiente, o treinamento de novos profissionais capazes de empregá-lo era demorado e a comparação visual de impressões digitais era cansativa e lenta. Por isso, os órgãos de segurança pública começaram a investir em soluções eletrônicas e automatizadas, o que levou ao desenvolvimento dos *Automated Fingerprint Identification Systems* (AFIS) ou Sistemas Automatizados de Identificação de Impressões Digitais.

Inicialmente usados por forças de segurança, esses sistemas hoje também são aplica-

dos em diversas áreas não forenses devido ao aumento das preocupações com segurança e fraudes de identidade. Nesse contexto, as digitais são coletadas com sensores especializados que geram imagens das digitais, que são processadas a fim de se obter uma forma de representação que pode ser usada para verificação. *Internet Banking* e autenticação de usuários em dispositivos móveis são exemplos (JAIN; FLYNN; ROSS, 2007).

## 2.2 Formas de representação de impressões digitais

Maltoni et al. (2022) enfatiza que uma boa representação de uma impressão digital deve conter informações que possibilitem a distinção entre duas amostras, deve ser extraída de forma rápida e fácil e ser compacta para poder armazenada em sistemas biométricos com pouca capacidade. Representações baseadas em imagens, apesar normalmente em escalas de cinza, normalmente não são adequadas dadas variações de iluminação, resolução, qualidade e ruídos provocados pela presença de cicatrizes e outras injurias nos dedos das pessoas, principalmente as que realizam algum tipo de trabalho manual com frequência.

O autor supracitado divide os atributos que podem ser extraídos de uma impressão digital em três níveis diferentes:

- Nível 1: também chamado de nível global, há atributos como o padrão das curvaturas das linhas nas imagens, delimitadas pelos cumes e vales da impressão digital. A partir dela podem ser determinados os "pontos singulares", que são os centros das curvaturas dessas linhas (LEVI; SIROVICH, 1972). As imagens de orientação e frequência e o formato da digital (que serão definidos posteriormente) também são considerados atributos de escopo global;

- Nível 2: são as características de escopo local, que exigem uma análise em uma escala menor da impressão digital. Dentre elas as que são mais facilmente observadas em sensores convencionais são as *bifurcações de cume*, onde um cume se divide em dois, e *terminações de cume*, onde um cume termina em um vale. Tais características são chamadas de *minúcias*, e são normalmente definidas pela sua posição na impressão digital e orientação (ângulo);

- Nível 3: são atributos dos próprios cumes em si, como o seu formato, largura, contorno e poros excretores de suor. Tais características são altamente distintivas, mas só podem ser extraídas de impressões digitais de alta resolução (acima de 1000 dpi).

## 2.3 Extração de características de ditais

Para a verificação de usuários através de suas impressões digitais é necessário um processamento das imagens para a extração de características, sendo que em cada faze é gerada uma nova imagem que contém apenas as informações relevantes para o estágio seguinte, até que finalmente é possível determinar as posições e outras informações distintivas das minúcias (MALTONI et al., 2022). A seguir serão descritos brevemente os estágios de processamento e algumas técnicas que podem ser utilizadas em cada um deles.

### 2.3.1 Segmentação

A segmentação normalmente é o estágio inicial do processamento de impressões digitais. Nele, a porção da imagem que corresponde à impressão digital em si é separada no restante, que não possui informações relevantes para a distinção de digitais.

Diversos métodos baseados em aprendizado de máquina foram elaborados e avaliados para segmentação, principalmente técnicas de Aprendizado Profundo, muito comum no processamento de imagens. Vale mencionar Zhu et al. (2017), que treinaram quatro redes neurais convolucionais (CNNs) utilizando blocos de imagem em múltiplas escalas e combinaram as pontuações de saída correspondentes com o objetivo de aprimorar a precisão da segmentação.

Em (EZEOBIEJESI; BHANU, 2017) foi usada uma pilha de máquinas de Boltzmann restritas (RBMs) para construir um modelo generativo de aprendizado de características. Para cada bloco da impressão digital, as características extraídas são repassadas a um classificador binário simples, que realiza a classificação.

Diferente dos métodos anteriores, Nguyen, Cao e Jain (2018) integram redes neurais totalmente convolucionais com técnicas baseadas em detecção para analisar toda a imagem

de entrada de uma só vez, ao invés de realizar um processamento por janelas (porções retangulares da imagem). Além disso, um mecanismo de atenção visual foi desenvolvido especificamente para concentrar o processamento apenas nas regiões onde há impressões digitais latentes.

### 2.3.2 Orientação local dos cumes

A orientação local dos cumes é definida como o ângulo de uma linha da impressão digital em um pixel da imagem. Normalmente é associado um mesmo ângulo para uma pequena janela da imagem já segmentada.

Dentre as técnicas utilizadas para estimar a orientação dos cumes podem ser citadas as propostas por Zhu et al. (2006) e Schuch, Schulz e Busch (2017), que utilizaram redes neurais artificiais para estimar as orientações e compararam com métodos tradicionais baseados em gradientes.

### 2.3.3 Detecção de minúcias

A detecção de minúcias é um dos estágios mais importantes do processamento de impressões digitais, visto que diversos algoritmos de verificação de impressões digitais com boa acurácia são baseados na comparação das minúcias.

Dada a importância desse estágio para a verificação de digitais há uma pesquisa por métodos de extração de minúcias das imagens. Tang, Gao e Feng (2017) trataram a extração de minúcias como um problema de detecção de objetos. Nesse método, uma CNN é utilizada para converter impressões digitais brutas em um mapa de pontuação de minúcias, com uma posição analisada a cada bloco de $16x16$ pixels. As posições com pontuação acima de um determinado limiar são consideradas candidatas a minúcias. Em seguida, as regiões vizinhas são refinadas por uma segunda CNN que compartilha os mesmos níveis convolucionais, a qual também estima a orientação da minúcia.

Tang et al. (2017) propuseram uma Rede Neural Profunda, o FingerNet, que combina conhecimento especializado do domínio de impressões digitais com treinamento de ponta a ponta para aumentar a precisão da extração de características. Especificamente, o modelo

é inicialmente construído convertendo etapas tradicionais de extração de características — extração de orientação e detecção de minúcias — em camadas convolucionais com pesos fixos. Em seguida, essas camadas básicas são estendidas com novas camadas, e todos os pesos da rede são ajustados. Para treinar o modelo, é utilizada uma função de perda composta que aproveita rótulos fracos, fortes e verdadeiros relacionados à orientação, segmentação e minúcias.

## 2.4 Verificação de impressões digitais

Conforme explica Maltoni et al. (2022) um algoritmo de verificação de impressões digitais compara duas imagens de digitais e retorna um pontuação entre 0 e 1, em que 1 indica a maior similaridade possível, ou uma resposta binária. Poucas técnicas de verificação operam diretamente nas imagens em escala de cinza. A maioria deles opera em representações intermediárias, discutidas na Sessão 2.2.

O autor afirma que as principais dificuldades na verificação de digitais estão relacionadas com a coleta das imagens, que estão sujeitas a ruídos causados por condições adversas na pele, rotação dos dedos ao encostar no sensor, parte do dedo pode ficar fora da área do sensor, etc. Dos diversos algoritmos de verificação de digitais propostos na literatura, a grande maioria tem um bom desempenho quando utilizados em imagens de boa qualidade.

# 3 Breve descrição dos objetivos e metas

Este projeto tem o objetivo de **comparar diferentes abordagens para ajuste de hiperparâmetros de algoritmos de classificação em dinâmica da digitação**. Para isso, será avaliado o ajuste de hiperparâmetros de forma individual e global. Além disso, diferentes técnicas de ajuste de hiperparâmetros podem ser investigadas nesse contexto.

A princípio, o foco do projeto será na dinâmica de digitação de *texto fixo*, em que todos os indivíduos digitam a mesma expressão. O desempenho será avaliado por métricas como FMR, FNMR e acurácia balanceada, descritas na Seção 4.2.

Os objetivos específicos do projeto são:

- Selecionar algoritmos de classificação usados em dinâmica da digitação;
- Definir abordagens de ajuste de hiperparâmetros que possam ser aplicadas em dinâmica da digitação (por exemplo: ajuste individual, ajuste global);
- Realizar experimentos comparando as diferentes abordagens de ajuste;
- Avaliar desempenho obtido pelos algoritmos com cada abordagem.

# 4 Metodologia

Este projeto irá comparar técnicas para ajuste de hiperparâmetros de algoritmos de classificação em dinâmica da digitação. Para isso, serão utilizados conjuntos de dados disponíveis publicamente, conforme descrito na Seção 4.1. Esses dados serão divididos entre treino e teste, sendo que as amostras usadas para treinamento serão referentes a dados mais antigos em comparação com os dados usados para teste. Na Seção 4.2, são descritas métricas que serão usadas para avaliação de desempenho neste trabalho.

## 4.1 Conjuntos de dados

Grande parte dos trabalhos que realizaram experimentos com dados de dinâmica da digitação não disponibilizaram os dados coletados (**??**). Esse fato dificulta a reprodutibilidade de estudos na área. Este projeto irá utilizar dados publicamente disponíveis. Alguns conjuntos de dados que podem ser usados são descritos a seguir:

- CMU (**??**): Este conjunto de dados [1] possui dados de 51 indivíduos que digitaram a senha ".tie5Roanl" em oito sessões de captura, com 50 amostras em cada sessão. No total, cada indivíduo digitou a senha 400 vezes.

- KeyRecs (**??**): O conjunto de dados KeyRecs [2] envolveu a captura de dinâmica da digitação de texto fixo e de texto livre. A princípio, o foco deste projeto será em texto fixo, portanto apenas essa parte do conjunto de dados deve ser utilizada. Para texto fixo, de acordo com a descrição do conjunto de dados, 99 indivíduos digitaram uma mesma senha em duas sessões, com 100 amostras em cada sessão, totalizando 200 amostras por indivíduo. Ao realizar o download da versão disponível, entretanto, observou-se que alguns usuários tem menos do que 200 amostras.

Além desses conjuntos de dados, o projeto pode eventualmente usar outros conjuntos de dados como, por exemplo, os conjuntos de dados GREYC (**??**) e também o disponibilizado por **??**).

[1] <https://www.cs.cmu.edu/~keystroke/>
[2] <https://zenodo.org/records/7886743>

## 4.2 Métricas

Esta seção descreve algumas métricas usadas na literatura que serão usadas para avaliação dos resultados nos experimentos realizados neste projeto de pesquisa. Essas métricas são: FMR, FNMR e acurácia balanceada (**????**). Uma breve descrição dessas métricas é apresentadas a seguir:

- FMR (*False Match Rate*, Taxa de falsa correspondência): percentual de tentativas de impostores que foram aceitas como genuínas, definida como

$$FMR = \frac{numero\ de\ tentativas\ de\ impostores\ aceitas}{total\ de\ tentativas\ de\ impostores}. \quad (1)$$

  Uma taxa relacionada é a FAR (*False Acceptance Rate*), que tem significado similar, mas considera também taxa em que o sistema biométrico falha ao obter uma amostra biométrica. Essa taxa é conhecida como FTA (*Failure to Acquire Rate*).

- FNMR (*False Non-match Rate*, Taxa de falsa não-correspondência): percentual de tentativas genuínas que foram rejeitadas como impostoras pelo sistema, definida como

$$FNMR = \frac{numero\ de\ tentativas\ genuinas\ rejeitadas}{total\ de\ tentativas\ de\ usuarios\ genuinos}. \quad (2)$$

  Uma métrica relacionada é a FRR (*False Rejection Rate*), que tem um significado similar, mas considera também a FTA.

- Acurácia balanceada: média do acerto para cada classe (genuíno e impostor). Essa métrica pode ser obtida a partir da o cálculo da (HTER - *Half Total Error*, Metade do erro total)

$$HTER = \frac{FNMR + FMR}{2}, \quad (3)$$

  definida como a média entre FNMR e FMR (**??**). A partir da HTER, então é obtida a acurácia balanceada, definida como

$$BAcc = 1 - HTER. \tag{4}$$

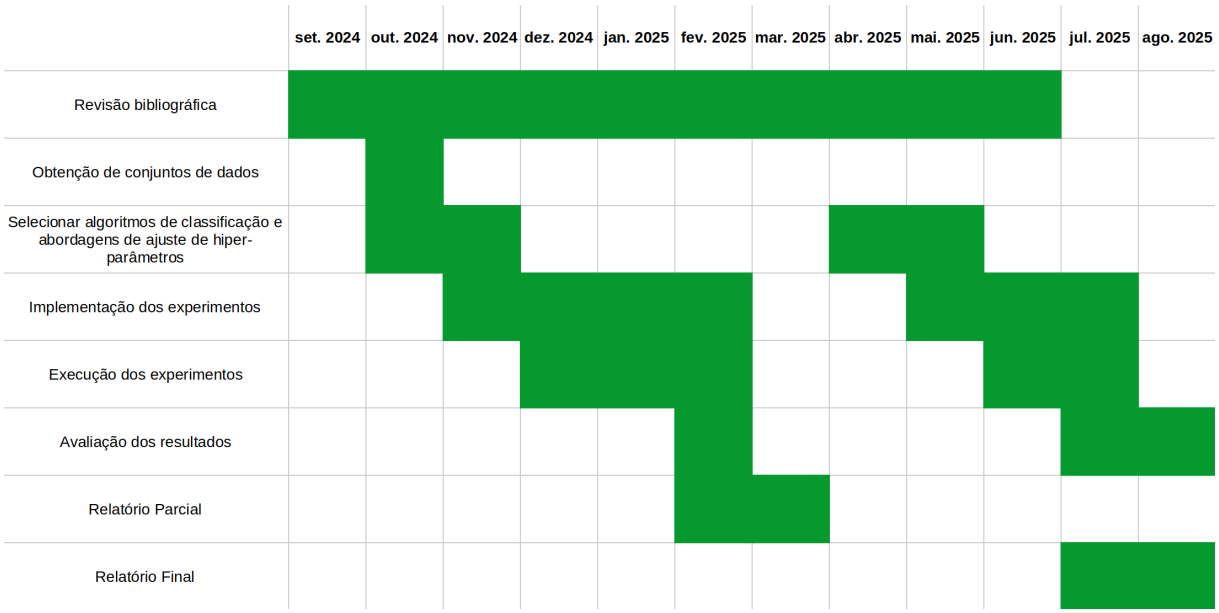
# 5 Descrição da viabilidade da execução do projeto

Para a realização da pesquisa bibliográfica neste projeto, será necessário acesso a artigos científicos. O Portal de Periódicos da CAPES disponível pela rede da UFABC pode ser utilizado para isso. Com relação aos experimentos, há conjuntos de dados de dinâmica da digitação disponíveis publicamente, conforme apresentado na Seção 4.1. Além disso, para a implementação e execução dos experimentos, um computador/notebook é suficiente. Sobre as atividades do projeto, o cronograma para condução desta pesquisa é descrito na próxima seção.

# 6 Cronograma

O cronograma do projeto, dividido em 12 meses, é apresentado na Figura 1.

Figura 1 – Cronograma do projeto.




As tarefas do cronograma são brevemente descritas a seguir:

- *Revisão bibliográfica*: pesquisa de trabalhos relacionados a dinâmica da digitação e ajuste de hiperparâmetros;
- *Selecionar algoritmos de classificação e abordagens de ajuste de hiperparâmetros*: definir quais algoritmos de aprendizado de máquina serão utilizados na classificação dos dados de dinâmica da digitação, assim como as abordagens de ajuste de hiperparâmetros que serão avaliadas;
- *Obtenção de conjuntos de dados*: obtenção de conjuntos de dados para os experimentos. Alguns conjuntos de dados que podem ser utilizados são mencionados na Sessão 4.1;
- *Implementação dos experimentos*: implementação do código para realizar os experimentos;
- *Execução dos experimentos*: execução dos experimentos com diferentes abordagens de ajuste de hiperparâmetros;

- *Avaliação dos resultados*: avaliação dos resultados obtidos nos experimentos;
- *Relatório Parcial*: elaboração do relatório parcial;
- *Relatório Final*: elaboração do relatório final.

Além das atividades descritas no cronograma, artigos científicos poderão ser escritos e submetidos.

# Referências


EZEOBIEJESI, J.; BHANU, B. Latent fingerprint image segmentation using deep neural network. In: _____. *Deep Learning for Biometrics*. Cham: Springer International Publishing, 2017. p. 83–107. ISBN 978-3-319-61657-5. Disponível em: <https://doi.org/10.1007/978-3-319-61657-5_4>.

JAIN, A.; ROSS, A.; PANKANTI, S. Biometrics: a tool for information security. *IEEE Transactions on Information Forensics and Security*, v. 1, n. 2, p. 125–143, 2006.

JAIN, A.; ROSS, A.; PRABHAKAR, S. An introduction to biometric recognition. *IEEE Transactions on Circuits and Systems for Video Technology*, IEEE, v. 14, n. 1, p. 4–20, 2004. ISSN 1051-8215.

JAIN, A. K.; FLYNN, P.; ROSS, A. A. *Handbook of Biometrics*. Berlin, Heidelberg: Springer-Verlag, 2007. ISBN 038771040X.

JAIN, A. K.; NANDAKUMAR, K.; ROSS, A. 50 years of biometric research: Accomplishments, challenges, and opportunities. *Pattern Recog. Letters*, Elsevier, v. 79, p. 80 – 105, 2016. ISSN 0167-8655.

LEVI, G.; SIROVICH, F. Structural descriptions of fingerprint images. *Information Sciences*, v. 4, n. 3, p. 327–355, 1972. ISSN 0020-0255. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0020025572800203>.

MALTONI, D.; MAIO, D.; JAIN, A. K.; FENG, J. Book. *Handbook of fingerprint recognition: Third edition*. [s.n.], 2022. 1 - 522 p. Cited by: 42. Disponível em: <https://www.scopus.com/inward/record.uri?eid=2-s2.0-85159134415&doi=10.1007%2f978-3-030-83624-5&partnerID=40&md5=20c90152518eac119f092021f0fe4dfa>.

MOENSSENS, A. *Fingerprint Techniques*. Chilton Book Company, 1971. (Inbau law enforcement series). ISBN 9780801955273. Disponível em: <https://books.google.com.br/books?id=aF6qQgAACAAJ>.

NGUYEN, D.-L.; CAO, K.; JAIN, A. K. *Automatic Latent Fingerprint Segmentation*. 2018. Disponível em: <https://arxiv.org/abs/1804.09650>.

PEACOCK, A.; KE, X.; WILKERSON, M. Typing patterns: a key to user identification. *IEEE Security Privacy*, IEEE, v. 2, n. 5, p. 40–47, 2004.

RYU, R.; YEOM, S.; HERBERT, D.; DERMOUDY, J. The design and evaluation of adaptive biometric authentication systems: Current status, challenges and future direction. *ICT Express*, v. 9, n. 6, p. 1183–1197, 2023. ISSN 2405-9595.

SCHUCH, P.; SCHULZ, S.-D.; BUSCH, C. Deep expectation for estimation of fingerprint orientation fields. In: *2017 IEEE International Joint Conference on Biometrics (IJCB)*. [S.l.: s.n.], 2017. p. 185–190.

SCOTT, W. *Fingerprint Mechanics: A Handbook; Fingerprints from Crime Scene to Courtroom*. Thomas, 1951. Disponível em: <https://books.google.com.br/books?id=zMA1AAAAIAAJ>.

TANG, Y.; GAO, F.; FENG, J. Latent fingerprint minutia extraction using fully convolutional network. In: *2017 IEEE International Joint Conference on Biometrics (IJCB)*. IEEE Press, 2017. p. 117–123. Disponível em: <https://doi.org/10.1109/BTAS.2017.8272689>.

TANG, Y.; GAO, F.; FENG, J.; LIU, Y. Fingernet: An unified deep network for fingerprint minutiae extraction. In: *2017 IEEE International Joint Conference on Biometrics (IJCB)*. IEEE Press, 2017. p. 108–116. Disponível em: <https://doi.org/10.1109/BTAS.2017.8272688>.

TERADA, R. *Segurança de Dados*. [S.l.]: Blucher, 2008. ISBN 9788521215400.

ZHU, E.; YIN, J.; ZHANG, G.; HU, C. Fingerprint ridge orientation estimation based on neural network. p. 158–164, 01 2006.

ZHU, Y.; YIN, X.; JIA, X.; HU, J. Latent fingerprint segmentation based on convolutional neural networks. In: *2017 IEEE Workshop on Information Forensics and Security (WIFS)*. [S.l.: s.n.], 2017. p. 1–6.