

Um Guia Prático para Matching de Impressões Digitais

Letícia Torres¹, Tamires Paulino¹
José Maria Monteiro¹, Javam Machado¹

¹ Departamento de Ciência da Computação – Universidade Federal do Ceará (UFC)
Campus do Pici, Bloco 910 – Fortaleza, CE – Brasil

leticia.torres@lsbd.ufc.br, tamirespaulino19@alu.ufc.br

jose.monteiro@lsbd.ufc.br, javam.machado@lsbd.ufc.br

Abstract. *Fingerprint biometric recognition is widely used due to the uniqueness of fingerprint patterns. Despite being a well-established field, beginners and developers still face challenges arising from the lack of clear guidelines, the fragmentation of available documentation, and the limited readability of some reference works. To address these issues, this paper presents a practical and structured guide to the workflow of a minutiae-based Automated Fingerprint Identification System (AFIS). The proposed pipeline comprises four main stages: image acquisition, preprocessing for noise reduction, minutiae extraction, and matching against a fingerprint database. In addition, compatibility limitations between widely used reference tools, such as the MINDTCT software and the Minutiae Cylinder-Code (MCC) algorithm, are discussed, along with the current availability of public fingerprint databases. The proposed framework aims to reduce the learning curve and facilitate the development of new biometric systems, supporting applications such as the identification of missing persons, refugees, fugitives, undocumented individuals, and people experiencing homelessness, as well as fraud prevention in social welfare programs and access to public healthcare services.*

Resumo. *O reconhecimento biométrico por impressões digitais é amplamente utilizado devido à unicidade dessas estruturas. Apesar de ser uma área consolidada, iniciantes e desenvolvedores ainda enfrentam dificuldades decorrentes da ausência de diretrizes claras, da dispersão da documentação e da baixa legibilidade de parte dos trabalhos de referência. Para mitigar esse problema, este trabalho apresenta um guia prático e estruturado sobre o fluxo de funcionamento de um Sistema Automatizado de Identificação de Impressões Digitais (AFIS) baseado em minúcias. O pipeline metodológico compreende quatro etapas: aquisição de imagens, pré-processamento para redução de ruídos, extração de minúcias e comparação (matching) com uma base de dados. Também são discutidas limitações de compatibilidade entre ferramentas de referência, como o software MINDTCT e o algoritmo Minutiae Cylinder-Code (MCC), além da disponibilidade de bases de dados públicas. A estrutura proposta busca reduzir a curva de aprendizado e facilitar o desenvolvimento de novos sistemas biométricos, contribuindo para aplicações como identificação de pessoas desaparecidas, refugiadas, foragidas, sem documentação ou em situação de rua, combate a fraudes em programas sociais e acesso a serviços de saúde pública.*

1. Introdução

O reconhecimento biométrico refere-se ao uso de características físicas e comportamentais para a verificação e identificação de indivíduos. Há diversas características que podem ser utilizadas na implementação de sistemas biométricos, dentre elas: a face, a íris, a geometria da mão, a impressão palmar, as veias da mão, a assinatura e as impressões digitais [Maltoni et al. 2009]. Entre essas modalidades, o reconhecimento por impressões digitais destaca-se por suas propriedades de unicidade e persistência ao longo da vida [Martins et al. 2024], sendo amplamente utilizado em investigações forenses e aplicações governamentais [Cappelli e Ferrara 2012].

De acordo com [Maltoni et al. 2022b], uma impressão digital consiste na representação externa das estruturas presentes na superfície dos dedos, compostas por cristas e vales, formados ainda durante o desenvolvimento fetal. As digitais apresentam características permanentes e únicas em cada indivíduo. Na literatura, essas características são divididas em dois grupos principais: globais e locais. Os atributos globais são definidos pelas formações delta, laço e espiral. Já os locais são definidos pelas minúcias, as quais são determinadas pelas terminações e bifurcações das cristas [Maltoni et al. 2009].

Há diversos estudos voltados ao reconhecimento de indivíduos utilizando correspondências globais; tais abordagens, apesar de proporcionarem bons resultados, tendem a ser computacionalmente caras e sensíveis a ruídos e deformações [Peralta et al. 2017]. Portanto, métodos baseados em minúcias tornaram-se amplamente utilizados em sistemas automáticos de reconhecimento de impressões digitais [Maltoni et al. 2009], uma vez que possuem maior robustez a ruídos, a variação de rotação e translação, além da possibilidade de paralelismo [Peralta et al. 2017].

Atualmente, até mesmo técnicas de aprendizado de máquina e *deep learning* vêm sendo exploradas nesse campo de estudo [Peng e Huang 2025; Singh et al. 2025]. Pode-se perceber, portanto, que esse campo de pesquisa não é recente e continua sendo amplamente estudado. Todavia, a extensa literatura disponível encontra-se distribuída em diferentes fontes e, muitas vezes, concentra-se na avaliação de métodos específicos, dedicando pouca atenção à apresentação de fluxos completos de implementação. Como consequência, iniciantes na área frequentemente encontram dificuldades decorrentes da falta de diretrizes claras sobre os conceitos, técnicas, conjuntos de dados e as etapas necessárias para sua integração em um sistema funcional.

Nesse contexto, este trabalho apresenta um guia prático (*guideline*) para o desenvolvimento de sistemas de identificação de impressões digitais baseado em minúcias. A proposta organiza, de forma estruturada, as principais etapas do pipeline de um Sistema Automatizado de Identificação de Impressões Digitais (AFIS), consolidando conceitos básicos, técnicas, ferramentas e conjuntos de dados frequentemente apresentados de forma dispersa. Além disso, são discutidos aspectos práticos observados durante a utilização de ferramentas amplamente empregadas na área, com o objetivo de auxiliar pesquisadores e desenvolvedores na compreensão e implementação desses sistemas.

O restante do trabalho está organizado da seguinte maneira: na Seção 2 são apresentados os principais trabalhos relacionados à área de identificação por impressões digitais; na Seção 3 são apresentadas e discutidas as etapas que compõem o guia prático para

o desenvolvimento de sistemas de identificação por meio de impressões digitais; e, por fim, na Seção 4 são apresentadas as discussões e conclusões.

2. Trabalhos Relacionados

Sistemas Automatizados de Identificação de Impressões Digitais (AFIS) já são amplamente utilizados por diversas organizações em vários países. Em [Gibb e Riemen 2023], os autores apresentam aspectos que impactam esses sistemas, tais como fatores humanos, organizacionais e técnicos. Ademais, discutem maneiras de mitigar esses fatores com base no fluxo de trabalho da Polícia Nacional dos Países Baixos (NPN), considerado um padrão de excelência por apresentar estratégias voltadas à mitigação de erros e vieses nesses sistemas.

Em [Vibert et al. 2023], é apresentada uma análise comparativa de algoritmos para reduzir o número de minúcias em *templates* de impressões digitais. O objetivo do estudo é identificar o subconjunto de minúcias que cause a menor degradação no desempenho de reconhecimento. Foram avaliados sete algoritmos de seleção de minúcias em três bases de dados, além de três algoritmos de comparação. Os autores concluem que a distribuição espacial das minúcias é um fator decisivo para o sucesso da redução. Por fim, na fase de cadastro, o método que apresentou o melhor resultado foi o MRGA; já na fase de verificação, o método do Baricentro apresentou o melhor custo-benefício para o problema.

Para realizar o reconhecimento de impressões digitais, em [Martins et al. 2024] apresentam uma abordagem baseada em minúcias. Os diferenciais do trabalho estão no uso da técnica de fecho convexo (*convex hull*) na extração de minúcias, auxiliando na definição da região de interesse (ROI) e na representação de cada minúcia por meio de polígonos de n vértices formados por seus vizinhos, substituindo a tradicional triangulação na etapa de extração de características. O método apresentou bons resultados, com taxa de erro de 0,03% no *dataset* FVC 2000 e de 7,8% no FVC 2002, além de se mostrar robusto a rotações e translações.

O processo de identificação apresenta elevada complexidade devido ao número de comparações realizadas no banco de dados. Em [Peralta et al. 2017], o trabalho apresenta uma metodologia genérica de decomposição para realizar o procedimento de *matching* em larga escala baseado em minúcias. No estudo, o método decompõe as impressões digitais em conjuntos de estruturas locais, permitindo o cálculo paralelo de *scores* parciais e a detecção precoce de não correspondências. Foram utilizados dois algoritmos distintos de comparação, Minutia-Cylinder Code e Jiang, executados em duas estruturas de código aberto para Big Data: Apache Hadoop e Apache Spark. A abordagem apresentou eficiência no reconhecimento de impressões digitais em uma base de 400.000 *templates* (SFinGe), com um tempo médio de 0,1661 segundos para realizar uma busca completa na versão otimizada do algoritmo de Jiang no Apache Spark e 0,2005 segundos no Apache Hadoop.

Em [Bakheet et al. 2022b], foi proposta a criação de uma estrutura automatizada para a extração e correspondência de minúcias em impressões digitais invisíveis. No estudo, as imagens de digitais latentes são submetidas a um pré-processamento e, em seguida, aplica-se um detector SIFT para extrair e identificar um conjunto potencial de estruturas confiáveis para a identificação de minúcias. A fase de *matching* utiliza um

algoritmo de força bruta e um filtro de limiar para eliminar falsos positivos. O estudo apresentou bons resultados, alcançando uma taxa de erro igual (ERR) de 0,0201 em testes realizados com o banco de dados público FVC2004.

3. Um Guia Prático para o Desenvolvimento de Sistemas de Identificação por meio de Impressões Digitais

Esta seção aborda o *pipeline* de reconhecimento de impressões digitais utilizando minúcias.

3.1. Visão Geral

Nesta seção, apresentamos uma visão geral do processo de reconhecimento de impressões digitais. Como ilustrado na Figura 1, esse complexo processo pode ser dividido em quatro grandes etapas. A primeira refere-se ao processo de aquisição da imagem a ser reconhecida, por meio de sensores e de diferentes técnicas. Uma vez adquirida, essa imagem pode chegar aos sistemas em diversos formatos e qualidades; por isso, logo após a aquisição, realiza-se uma etapa de pré-processamento para realçar os pontos de interesse. Em seguida, ocorrem as etapas de extração de minúcias e de *matching*. Nesta última etapa, buscam-se, no banco de dados, as imagens mais semelhantes àquela fornecida como entrada. Por fim, são exibidas ao usuário as imagens mais similares à impressão digital fornecida como entrada.



Figura 1. Visão macro de um *pipeline* de reconhecimento de impressões digitais.

3.2. Aquisição das Imagens

A qualidade da imagem é um fator crucial para o bom desempenho em sistemas de reconhecimento de impressões digitais e a forma como as imagens são obtidas impacta diretamente essa qualidade [Mohamed Abdul Cader et al. 2023]. De maneira geral, as imagens podem ser adquiridas de forma *off-line*, em que as impressões digitais possuem uma representação física, geralmente em papel e tinta, posteriormente digitalizada, ou *live-scan*, em que são adquiridas por meio de sensores que escaneiam diretamente a impressão digital [Maltoni et al. 2009].

3.2.1. Aquisição *Off-line*

Historicamente, o processo de obtenção de impressões digitais foi realizado de maneira muito manual, com técnicas que utilizavam tinta e papel para a captura das impressões digitais [Yu et al. 2023]. Essas técnicas, chamadas *ink-technique* (técnica de

tinta), são aquelas nas quais o dedo é pressionado contra uma tinta, geralmente preta, e posteriormente pressionado e rolado sobre um papel, sendo, em seguida, digitalizado [Maltoni et al. 2022a], como mostrado na Figura 2.



Figura 2. Exemplos de impressões digitais coletadas de forma *off-line*. Fonte: [Maltoni et al. 2022a].

Outros cenários em que esse tipo de coleta ocorre incluem cenas de crime [Martins et al. 2024]. Nesse contexto, a coleta dessas impressões digitais não ocorre da mesma forma que em cenários de identificação civil (como a emissão de carteiras de identidade), por depender da superfície onde essas digitais se encontram. Segundo [Win et al. 2020], essas superfícies podem ser categorizadas em dois tipos: absorventes, nas quais técnicas com uso de produtos químicos e até mesmo fotos podem ser utilizadas para a coleta, ou não-absorventes, nas quais técnicas com uso de pó ou gel para aquisição podem ser utilizadas.

3.2.2. Aquisição *Live-Scan*

Neste tipo de coleta, a impressão digital é adquirida em tempo real, sem necessidade de digitalização posterior, por meio de um sensor de captura [Maltoni et al. 2022a]. A Figura 3 apresenta dois exemplos de captura por sensores. Sensores de impressão digital são utilizados em uma variedade de contextos, como desbloqueio de celulares, controle de acesso e pagamentos digitais [Yu et al. 2023]. Esses sensores podem ser categorizados quanto à tecnologia utilizada para coleta: ópticos, capacitivos, ultrassônicos, térmicos e por pressão [Mohamed Abdul Cader et al. 2023], ou quanto à quantidade de digitais coletadas, ou seja, se permitem a coleta de um único dedo ou múltiplos [Maltoni et al. 2022a].

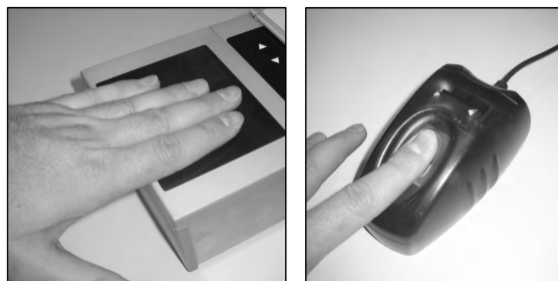


Figura 3. Exemplos de captura de impressões digitais via sensor. Fonte: [Maltoni et al. 2009].

Entretanto, por mais que o uso dessas tecnologias tenha melhorado a qualidade das imagens capturadas [Yu et al. 2023], problemas como dedos secos ou molhados ainda podem afetar fortemente a coleta da impressão digital [Mohamed Abdul Cader et al. 2023]. Ademais, sensores com pequenas áreas de contato dificultam o processo de

identificação, uma vez que a imagem coletada pode sofrer com a perda de informações [Maltoni et al. 2022a].

3.3. Pré-processamento

A imagem de uma impressão digital consiste em uma representação digital obtida por meio de algum método de coleta. Atualmente, a principal forma de coleta ocorre por meio de sensores [Maltoni et al. 2009]. Na prática, uma quantidade significativa de imagens apresenta problemas de baixa qualidade, seja por dificuldades técnicas dos sensores, como a presença de sujeira, umidade ou outros fatores, ou por dificuldades que decorrem do próprio indivíduo durante a coleta, como a aplicação inadequada de pressão sobre o sensor ou a presença de alterações na pele, por exemplo [Bakheet et al. 2022a; Bakheet et al. 2022b].

Em ambos os casos, a presença de ruídos nessas imagens compromete o processo de reconhecimento, uma vez que as etapas de extração e *matching* de minúcias dependem da boa qualidade destas imagens [Martins et al. 2024]. Nesse cenário, algumas técnicas de aprimoramento de imagem e de redução de ruído, como mostradas na Figura 4, podem ser aplicadas para mitigar o problema. Entre elas, podem ser mencionados a binarização, os filtros de mediana [Raghavan e John Singh 2024], a segmentação da imagem, a equalização de histograma, a normalização, o filtro de Gabor, a transformada de Fourier [Bakheet et al. 2022a] e até mesmo redes neurais convolucionais (CNN) [Maltoni et al. 2022b]. Entretanto, o *trade-off* entre precisão e eficiência permanece como um fator importante para a escolha da melhor técnica a ser aplicada [Maltoni et al. 2022b].

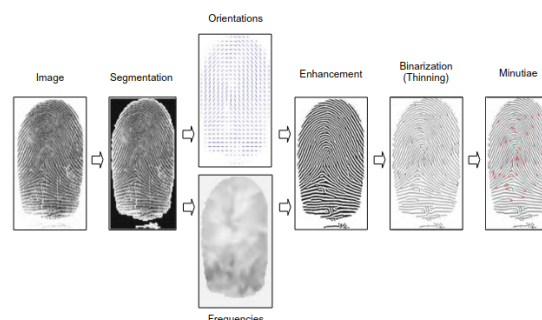


Figura 4. Exemplos de técnicas de pré-processamento aplicadas a uma impressão digital para extração de minúcias. Fonte: [Maltoni et al. 2022a].

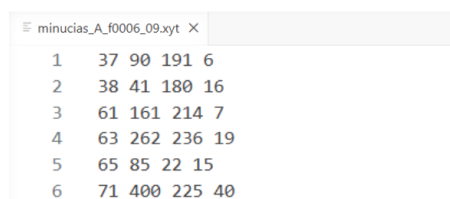
3.4. Extração de Minúcias

Uma vez concluída a etapa anterior, as imagens são então submetidas a algoritmos que realizam a extração de minúcias. Segundo [Maltoni et al. 2022b], essas podem ser definidas como características locais das impressões digitais, que estão relacionadas à forma como as estruturas de cristas podem ser descontinuadas.

Na literatura, diversos algoritmos foram propostos para a extração de minúcias, tais como Crossing-Numbers (CN) [Martins et al. 2024], SIFT [Bakheet et al. 2022b] e até mesmo redes neurais, como a FingerNet [Tang et al. 2017]. Além desses, uma ferramenta comumente utilizada é o **MINDTCT** [Vibert et al. 2023; Liu et al. 2024; Schuch et al. 2018].

Desenvolvido pelo *National Institute of Standards and Technology* (NIST), um órgão vinculado ao Departamento de Comércio dos Estados Unidos, responsável pelo desenvolvimento de diversos padrões para sistemas de reconhecimento de impressões digitais, o **MINDTCT** [Watson et al. 2007] é um *software* de detecção de minúcias. O **MINDTCT** pertence ao pacote *NIST Biometric Image Software* (NBIS), desenvolvido na linguagem C. Nos testes experimentais realizados para o desenvolvimento deste guia prático, sua utilização só foi possível em sistemas operacionais Linux.

Após a extração, as minúcias são armazenadas em *templates*, arquivos nos quais, para o **MINDTCT**, por exemplo, cada linha representa uma minúcia contendo as coordenadas (x, y) , a direção da crista (θ) e um *score* de qualidade da minúcia [Watson et al. 2007]. Para outros algoritmos, informações podem ser adicionadas ou removidas do *template*.



	1	2	3	4	5	6
1	37	90	191	6		
2	38	41	180	16		
3	61	161	214	7		
4	63	262	236	19		
5	65	85	22	15		
6	71	400	225	40		

Figura 5. Exemplo de arquivo de minúcias gerado pelo **MINDTCT**.

3.5. Matching de Minúcias

Minúcias constituem uma das estruturas mais utilizadas para a realização de *matching* de digitais, principalmente por sua estabilidade [Maltoni et al. 2022b; Peralta et al. 2017]. A imagem de uma impressão digital pode conter, dependendo de sua qualidade, em média de 10 a 200 minúcias [Martins et al. 2024] e, por suas características, somente uma pequena quantidade delas é necessária para realizar o reconhecimento do indivíduo [Maltoni et al. 2022b].

Algoritmos de *matching* são aqueles que comparam dois *templates* de impressões digitais e retornam um grau de similaridade ou uma decisão binária [Maltoni et al. 2022a]. Em cenários reais, uma das digitais é fornecida como entrada e a outra está armazenada em um conjunto de dados (repositório de imagens) [Bakheet et al. 2022a].

Dois algoritmos se destacam nesta atividade: **BOZORTH3** [Watson et al. 2007], do NIST, e o **Minutiae Cylinder-Code (MCC)**, desenvolvido por [Cappelli et al. 2010]. O primeiro pertence ao pacote NBIS, também tendo sido desenvolvido em C. Feito para ser integrado com o extrator do pacote, permite comparações 1:1 e 1: N , sendo N um conjunto de *templates*. Além disso, é classificado como item de exportação controlada pela lei americana devido à sua associação com práticas de controle de crimes e de segurança, possibilitando o acesso completo somente via CD-ROM para pessoas com acesso liberado [Watson et al. 2007].

O MCC, por sua vez, apresenta-se como uma das técnicas mais robustas e eficientes, possuindo invariância a rotação e translação, além de tolerância a distorções na pele e até mesmo erros de extração de minúcias [Maltoni et al. 2022b]. Ademais, consegue tornar a comparação mais eficiente ao utilizar técnicas de *hashing* e de indexação para buscar as digitais mais semelhantes. Todavia, ao testar sua utilização, foi possível notar que ele não pode ser utilizado em sistemas operacionais Linux, somente em Windows.

Dessa forma, já que os algoritmos de extração e de *matching* mais eficientes citados e utilizados na literatura, o MINDTCT e o MCC, são executados exclusivamente em sistemas operacionais distintos, é possível notar, então, a existência de incompatibilidade entre eles, tornando o desenvolvimento desses sistemas bem mais complexo. Ademais, para soluções comerciais, o uso do MCC ocasiona um aumento no custo de desenvolvimento, uma vez que se trata de uma solução proprietária e sua versão gratuita está disponível somente para fins de pesquisa [Biometric System Laboratory 2026].

Por mais robustos que sejam os métodos baseados em minúcias, a forte dependência da qualidade da imagem constitui uma desvantagem para essas abordagens [Martins et al. 2024]. Em contrapartida, por seu modo de funcionamento ser semelhante ao trabalho manual, esses métodos tornam-se mais confiáveis e passíveis de uso em aplicações judiciais [Peng e Huang 2025; Martins et al. 2024].

3.5.1. Conjuntos de Dados de Impressões Digitais

Em sistemas de identificação por impressões digitais, utilizam-se mecanismos de busca e comparação para retornar as imagens armazenadas mais semelhantes à imagem de entrada. Nos contextos reais, como os sistemas de emissão da Carteira de Identidade Nacional (CIN), os conjuntos de dados contêm milhares de instâncias, o que torna esse processo significativamente mais complexo.

Diversos conjuntos de dados com imagens de impressões digitais podem ser encontrados na literatura. Entretanto, a dificuldade de acesso a esses repositórios torna o desenvolvimento e o teste desses sistemas uma tarefa desafiadora. A seguir, destacamos algumas dessas bases de dados:

- Bases NIST: Bases de dados contendo grandes quantidades de amostras, como a NIST SD4, que contém 4000 instâncias, além de dados de diferentes tipos e qualidades. Foram descontinuadas em 2018 e não estão mais disponíveis para *download*.
- Bases *Fingerprint Verification Competition* (FVC): São bases organizadas pelo Laboratório de Sistemas Biométricos (BioLab) ¹ da Universidade de Bolonha. São bases de referência utilizadas para *benchmarks* de sistemas biométricos de identificação baseados em impressões digitais. No total, quatro bases estão disponíveis: FVC 2000 [Maio et al. 2002a], FVC 2002 [Maio et al. 2002b], FVC 2004 [Maio et al. 2004], FVC 2006 [Cappelli et al. 2007]. Por fim, uma desvantagem dessas bases é a pequena quantidade de amostras. A maior delas, FVC 2006, possui 1800 imagens.

4. Discussão e Conclusão

Este trabalho apresenta um guia prático para o desenvolvimento de sistemas de identificação baseados em impressões digitais. O guia proposto é composto por quatro etapas principais: aquisição de imagens, pré-processamento, extração de minúcias e *matching*.

¹<https://biolab.csr.unibo.it/home.asp>

Entende-se, com base em revisões da literatura, que a identificação por meio de impressões digitais é uma área antiga e com conhecimentos bem consolidados. Entretanto, poucos trabalhos apresentam informações bem estruturadas sobre o tema. As informações são esparsas e, muitas vezes, os trabalhos de referência são pouco legíveis. Ademais, do ponto de vista prático, há pouca documentação disponível. Assim, a curva de aprendizado para quem deseja desenvolver aplicações inovadoras baseadas em impressões digitais é bastante elevada.

Por fim, sistemas com uso real enfrentam desafios relacionados à segurança, à presença de digitais latentes e à necessidade de indexação dos *templates* de minúcias para acelerar o processo de busca em bases com milhares de instâncias. Como trabalho futuro, pretende-se detalhar o *guideline* apresentado com orientações voltadas à mitigação desses desafios.

Agradecimentos

Este trabalho foi realizado com apoio da Lenovo Tecnologia (Brasil) Ltda. e dentro do escopo do projeto Cientista Chefe Segurança Pública.

Uso de Inteligência Artificial

A Inteligência Artificial foi utilizada como apoio à revisão textual, à organização de seções e à geração inicial de trechos de código; todas as saídas foram revisadas, verificadas e ajustadas pelas autoras.

Referências

- [Bakheet et al. 2022a] Bakheet, S., Al-Hamadi, A., e Youssef, R. (2022a). A fingerprint-based verification framework using harris and surf feature detection algorithms. *Applied Sciences*, 12(4):2028.
- [Bakheet et al. 2022b] Bakheet, S., Alsubai, S., Alqahtani, A., e Binbusayyis, A. (2022b). Robust fingerprint minutiae extraction and matching based on improved sift features. *Applied Sciences*, 12(12):6122.
- [Biometric System Laboratory 2026] Biometric System Laboratory (2026). Research activities. <https://biolab.csr.unibo.it/research.asp?organize=Activities&select=&selObj=82&pathSubj=111%7C%7C8%7C%7C82&Req=>. Accessed: 2026-05-26.
- [Cappelli e Ferrara 2012] Cappelli, R. e Ferrara, M. (2012). A fingerprint retrieval system based on level-1 and level-2 features. *Expert Systems with Applications*, 39(12):10465–10478.
- [Cappelli et al. 2007] Cappelli, R., Ferrara, M., Franco, A., e Maltoni, D. (2007). Fingerprint verification competition 2006. *Biometric Technology Today*, 15(7-8):7–9.
- [Cappelli et al. 2010] Cappelli, R., Ferrara, M., e Maltoni, D. (2010). Minutia cylinder-code: A new representation and matching technique for fingerprint recognition. *IEEE transactions on pattern analysis and machine intelligence*, 32(12):2128–2141.
- [Gibb e Riemen 2023] Gibb, C. e Riemen, J. (2023). Toward better afis practice and process in the forensic fingerprint environment. *Forensic Science International: Synergy*, 7:100336.
- [Liu et al. 2024] Liu, X., Raja, K., Wang, R., Qiu, H., Wu, H., Sun, D., Zheng, Q., Liu, N., Wang, X., Huang, G., et al. (2024). A latent fingerprint in the wild database. *IEEE Transactions on Information Forensics and Security*, 19:3703–3718.
- [Maio et al. 2002a] Maio, D., Maltoni, D., Cappelli, R., Wayman, J. L., e Jain, A. K. (2002a). Fvc2000: Fingerprint verification competition. *IEEE transactions on pattern analysis and machine intelligence*, 24(3):402–412.

- [Maio et al. 2002b] Maio, D., Maltoni, D., Cappelli, R., Wayman, J. L., e Jain, A. K. (2002b). Fvc2002: Second fingerprint verification competition. In *2002 International conference on pattern recognition*, volume 3, pages 811–814. IEEE.
- [Maio et al. 2004] Maio, D., Maltoni, D., Cappelli, R., Wayman, J. L., e Jain, A. K. (2004). Fvc2004: Third fingerprint verification competition. In *International conference on biometric authentication*, pages 1–7. Springer.
- [Maltoni et al. 2022a] Maltoni, D., Maio, D., Jain, A. K., e Feng, J. (2022a). Fingerprint sensing. *Handbook of fingerprint recognition*, pages 63–114.
- [Maltoni et al. 2022b] Maltoni, D., Maio, D., Jain, A. K., e Feng, J. (2022b). *Handbook of Fingerprint Recognition*. Springer Cham, Cham, Switzerland, 3 edition.
- [Maltoni et al. 2009] Maltoni, D., Maio, D., Jain, A. K., e Prabhakar, S. (2009). *Handbook of fingerprint recognition*. Springer.
- [Martins et al. 2024] Martins, N., Silva, J. S., e Bernardino, A. (2024). Fingerprint recognition in forensic scenarios. *Sensors*, 24(2):664.
- [Mohamed Abdul Cader et al. 2023] Mohamed Abdul Cader, A. J., Banks, J., e Chandran, V. (2023). Fingerprint systems: sensors, image acquisition, interoperability and challenges. *Sensors*, 23(14):6591.
- [Peng e Huang 2025] Peng, A. e Huang, R. (2025). Research progress on the application of deep learning in fingerprint recognition. *Pattern Recognition*, page 112216.
- [Peralta et al. 2017] Peralta, D., García, S., Benítez, J. M., e Herrera, F. (2017). Minutiae-based fingerprint matching decomposition: methodology for big data frameworks. *Information Sciences*, 408:198–212.
- [Raghavan e John Singh 2024] Raghavan, R. e John Singh, K. (2024). An enhanced and hybrid fingerprint minutiae feature extraction method for identifying and authenticating the patient's noisy fingerprint. *International Journal of System Assurance Engineering and Management*, 15(1):84–97.
- [Schuch et al. 2018] Schuch, P., Schulz, S., e Busch, C. (2018). Survey on the impact of fingerprint image enhancement. *IET Biometrics*, 7(2):102–115.
- [Singh et al. 2025] Singh, R., Singh, R., Tripathi, R. K., e Agarwal, P. (2025). Fingerprint recognition using artificial neural networks. *Proceedings of the National Academy of Sciences, India Section A: Physical Sciences*, 95(2):127–135.
- [Tang et al. 2017] Tang, Y., Gao, F., Feng, J., e Liu, Y. (2017). Fingernet: An unified deep network for fingerprint minutiae extraction. In *Biometrics (IJCB), 2017 IEEE International Joint Conference on*. IEEE.
- [Vibert et al. 2023] Vibert, B., Le Bars, J.-M., Charrier, C., e Rosenberger, C. (2023). Comparative study of minutiae selection methods for digital fingerprints. *Frontiers in Big Data*, 6:1146034.
- [Watson et al. 2007] Watson, C. I., Garris, M. D., Tabassi, E., Wilson, C. L., McCabe, R. M., Janet, S., e Ko, K. (2007). User's guide to nist biometric image software (nbis).
- [Win et al. 2020] Win, K. N., Li, K., Chen, J., Viger, P. F., e Li, K. (2020). Fingerprint classification and identification algorithms for criminal investigation: A survey. *Future Generation Computer Systems*, 110:758–771.
- [Yu et al. 2023] Yu, Y., Niu, Q., Li, X., Xue, J., Liu, W., e Lin, D. (2023). A review of fingerprint sensors: Mechanism, characteristics, and applications. *Micromachines*, 14(6):1253.