Reconhecimento de impressões digitais falsas*

1st Igor Augusto de Carvalho
Processamento Digital de Imagens
IFSP - Instituto Federal de São Paulo
Birigui, Brasil
igor.carvalho@aluno.ifsp.edu.br

2nd João Vitor Ribeiro da Luz
Processamento Digital de Imagens
IFSP - Instituto Federal de São Paulo
Birigui, Brasil
j.luz@aluno.ifsp.edu.br

3rd Lucas Alves de Souza
Processamento Digital de Imagens
IFSP - Instituto Federal de São Paulo
Birigui, Brasil
lucas.alves@aluno.ifsp.edu.br

***Abstract*—Este artigo aborda o funcionamento do reconhecimento de impressões digitais falsas com base em processamento digital de imagens, utilizando métodos como o método Baseado em Padrão de Transpiração, método Baseado em Estatísticas de Poros e o método Baseados em Estatísticas de Primeira Ordem dos Tons de Cinza.**

O projeto resulta em uma detecção de spoofing em impressões digitais ao comparar as bordas de duas imagens: uma imagem presumivelmente real e outra potencialmente falsa (spoof). A detecção é baseada na análise da diferença entre as imagens de bordas, usando um limiar predefinido para identificar possíveis manipulações. O resultado final indica se a impressão digital é considerada autêntica ou se há suspeitas de spoofing.

***Index Terms*—*Processamento Digital de Imagem*, *Padrão de Transpiração*, *Estatísticas de Poros*, *Estatísticas de Primeira Ordem dos Tons de Cinza*.**

I. Introdução

Nos últimos anos, a ascensão da tecnologia biométrica transformou a forma como interagimos com o mundo digital, promovendo uma revolução na autenticação e segurança. Entre as diversas modalidades biométricas, as impressões digitais emergiram como uma das formas mais difundidas e confiáveis de identificação pessoal. A biometria, essencialmente, fundamenta-se na singularidade de características físicas ou comportamentais para estabelecer a identidade de um indivíduo de maneira única e intransferível.

As impressões digitais, consideradas há muito tempo como marcadores infalíveis de identidade, têm sido amplamente adotadas em sistemas de segurança, controle de acesso e autenticação biométrica. No entanto, à medida que a tecnologia avança, novos desafios surgem, e a área do Reconhecimento de Impressões Digitais enfrenta agora uma ameaça significativa: a falsificação biométrica. Este fenômeno, que envolve a criação e utilização de impressões digitais falsas para burlar sistemas de segurança, coloca em xeque a confiabilidade e a segurança dos métodos biométricos.

Esta revisão crítica aborda inicialmente o conceito de biometria, delineando a sua evolução e a importância crescente no cenário contemporâneo. Em seguida, explora a especificidade das impressões digitais como um dos principais modos de autenticação biométrica, destacando a sua ubiquidade e eficácia percebida. No entanto, o foco principal deste artigo concentra-se nos desafios emergentes relacionados ao Reconhecimento de Impressões Digitais falsas, examinando as técnicas utilizadas por fraudadores para contornar sistemas de segurança baseados nessa tecnologia aparentemente infalível. Ao compreender os riscos associados à falsificação biométrica, podemos fortalecer os sistemas existentes e promover avanços na pesquisa em segurança biométrica, garantindo assim a continuidade do uso confiável e seguro das impressões digitais como meio de identificação pessoal.

II. Objetivos

Este artigo visa aprofundar o entendimento sobre as falsificações biométricas de impressões digitais, analisando as técnicas empregadas por fraudadores e avaliando criticamente a eficácia dos sistemas existentes. Propõe-se desenvolver soluções e aprimoramentos para fortalecer a segurança biométrica, considerando implicações éticas e legais. Além disso, busca explorar inovações tecnológicas que possam prevenir tais falsificações e promover conscientização, destacando riscos e melhores práticas. Validar os resultados por meio de estudos de caso é essencial para embasar conclusões e, assim, contribuir para o avanço contínuo da pesquisa em segurança biométrica.

III. Referencial Teórico

A. Biometria

A biometria é uma disciplina científica que se concentra na análise e estudo de características únicas, sejam elas físicas, fisiológicas ou comportamentais, em seres humanos e outros organismos. O termo ”biometria” deriva do grego, com ”bio” referindo-se à vida e ”metron” à medida. Essa abordagem prática utiliza características distintivas para identificar indivíduos de maneira única.

No âmbito físico, as características biométricas incluem impressões digitais, retina, íris, formato do rosto, geometria da mão e a estrutura da orelha. As características fisiológicas estão relacionadas às funções corporais, como a voz, assinatura da escrita, dinâmica de digitação e até mesmo a forma como alguém caminha. Além disso, as características comportamentais envolvem padrões de comportamento, como a maneira como uma pessoa digita, assina seu nome ou interage com dispositivos eletrônicos.

Amplamente aplicada em sistemas de segurança, controle de acesso e autenticação, a biometria oferece uma abordagem mais confiável e conveniente em comparação com métodos tradicionais baseados em senhas ou cartões. O Reconhecimento de Impressões Digitais é um exemplo difundido dessa

aplicação, utilizando as características únicas das impressões digitais para identificar e verificar a identidade de um indivíduo.

B. Impressões Digitais

Uma impressão digital é uma representação única e distintiva dos padrões de sulcos e cristas encontrados na superfície das extremidades dos dedos humanos. Essas características únicas são utilizadas para identificação pessoal, especialmente em tecnologias de segurança biométrica, onde a impressão digital serve como uma assinatura única e exclusiva de cada indivíduo.

Fig. 1. Representação de Impressão Digital [**?**]

São padrões formados pelos sulcos e cristas presentes na pele das extremidades dos dedos humanos, como nas pontas dos dedos, polegares e palmas das mãos. Esses padrões são únicos para cada pessoa, mesmo entre gêmeos idênticos, e permanecem inalterados ao longo da vida, o que torna as impressões digitais uma forma altamente confiável de identificação biométrica.

A pele dos dedos possui glândulas que secretam óleos e suor, formando padrões distintos quando tocamos em superfícies. As partes mais altas da pele, chamadas de cristas, formam padrões salientes, enquanto as depressões entre elas, conhecidas como sulcos, criam um design único. As impressões digitais são geralmente classificadas em três tipos principais: arco, presilha e espiral, cada um com características específicas.

Devido à singularidade e estabilidade desses padrões, as impressões digitais são amplamente utilizadas em sistemas de identificação e autenticação, como em aplicativos de segurança, controle de acesso e até mesmo em dispositivos eletrônicos, oferecendo uma forma eficaz e segura de verificar a identidade de uma pessoa. O processo de coleta e análise de impressões digitais é chamado de dactiloscopia, e sua aplicação prática tem sido uma ferramenta valiosa em áreas como aplicação da lei, forense e segurança.

IV. Materiais e Métodos

O projeto em Python utiliza a biblioteca OpenCV (cv2), a biblioteca NumPy (np), a biblioteca Pillow (Image do PIL) e a biblioteca Matplotlib (plt) para realizar a detecção de spoofing em impressões digitais. Spoofing é uma técnica em que tenta-se enganar um sistema biométrico usando uma reprodução (spoof) em vez de uma amostra biométrica real. Comparando duas imagens para verificar se há evidências de spoofing.

V. Desenvolvimento

O desenvolvimento do projeto baseado em uma abordagem de pesquisa e aplicação, uma vez que o objetivo proposto se explica como o estudo de uma dentre as diversas aplicações do processamento digital de imagem no cotidiano das pessoas.

Inicialmente, com a escolha do tema, ”Reconhecimento de impressões digitais falsas”, fora realizada uma pesquisa na internet a respeito de projetos e artigos que utilizassem processamento digital de imagem para reconhecimento de impressões digitais falsas. Com bases de conhecimento já estabelecidas a respeito do tema proposto inicia-se a implementação, a partir de com um código base feito pelos integrantes do grupo, fora realizado a analise e estudo de como funciona o reconhecimento de impressões digitais falsas . [**?**]

A biblioteca utilizada foi OpenCV (cv2), a biblioteca NumPy (np), a biblioteca Pillow (Image do PIL) e a biblioteca Matplotlib (plt) para realizar a detecção de spoofing em impressões digitais.

Fig. 2. Ilustração Impressão Digital

Com isto, fora aplicada um código, que em questão realiza a detecção de spoofing em impressões digitais utilizando técnicas de processamento de imagem. Ele emprega as bibliotecas OpenCV, NumPy, Pillow (PIL), e Matplotlib para realizar diversas operações. A detecção de spoofing é feita comparando as bordas de duas imagens, uma presumivelmente real e outra potencialmente uma reprodução falsa (spoof).

A função para detectar bordas(imagem) é responsável por converter uma imagem colorida para escala de cinza e, em seguida, aplicar o detector de bordas Canny, que destaca as características de transição de intensidade na imagem. O resultado é uma imagem contendo apenas as bordas identificadas.

A função principal, para verificar spoofing com os parâmetros de imagem real e de imagemspoof, utiliza a função anterior para obter as imagens de bordas das imagens real e spoof fornecidas como entrada. Em seguida, as imagens de bordas são exibidas lado a lado usando Matplotlib. O código calcula a diferença absoluta entre essas imagens de bordas, considerando um limiar para identificar pixels significativamente diferentes. Se o número de pixels diferentes exceder um limite predefinido, o código conclui que a impressão digital é falsa (spoofing); caso contrário, é considerada autêntica.

Por fim, o código carrega duas imagens (que, atualmente, são iguais, mas deveriam ser diferentes para fins de comparação) e chama a função de verificação de spoofing. O resultado é impresso na tela, indicando se a impressão digital é considerada autêntica ou se há suspeitas de spoofing.

Fig. 3. Impressão íntegra

VI. Resultados

O desfecho deste projeto resultou em uma detecção de spoofing em impressões digitais ao comparar as bordas de duas imagens: uma imagem presumivelmente real e outra potencialmente falsa (spoof). A detecção é baseada na análise da diferença entre as imagens de bordas, usando um limiar predefinido para identificar possíveis manipulações. O resultado final indica se a impressão digital é considerada autêntica ou se há suspeitas de spoofing.

Fig. 4. Impressão Falsa

VII. Conclusão

Em conclusão, este projeto explorou eficazmente o emprego de técnicas avançadas de processamento digital de imagem para o reconhecimento de impressões digitais falsas, um desafio crucial na segurança biométrica. Ao aplicar o detector de bordas Canny e analisar a diferença entre imagens autênticas e potenciais reproduções falsas, alcançamos um método robusto para identificar padrões suspeitos. A abordagem proposta destaca-se pela sua capacidade de discernir entre impressões digitais reais e falsas, fornecendo uma contribuição significativa para a segurança de sistemas biométricos. Essa aplicação inovadora de técnicas de processamento de imagem oferece uma promissora linha de pesquisa para aprimorar a autenticidade e confiabilidade em sistemas biométricos, contribuindo assim para a contínua evolução da segurança digital.

O foco deste artigo reside na exploração e implementação de técnicas avançadas de processamento digital de imagem com o objetivo específico de detectar impressões digitais falsas. A pesquisa concentrou-se em aprimorar a segurança biométrica, empregando o detector de bordas Canny e uma análise detalhada da discrepância entre impressões digitais autênticas e possíveis reproduções fraudulentas. Ao destacar a capacidade do método proposto em distinguir com precisão entre padrões reais e simulados, o artigo contribui para o avanço da segurança em sistemas biométricos, apresentando uma abordagem inovadora e promissora para a detecção de spoofing. Este enfoque visa fortalecer a autenticidade e confiabilidade dos sistemas biométricos, oferecendo uma valiosa perspectiva para futuras pesquisas e desenvolvimentos no campo da segurança digital.

Os principais objetivos deste artigo foi aprofundar a compreensão das falsificações biométricas de impressões digitais, investigando as técnicas empregadas por fraudadores e avaliando criticamente a eficácia dos sistemas biométricos existentes. Além disso, busca-se desenvolver soluções e aprimoramentos que fortaleçam a segurança biométrica, considerando implicações éticas e legais associadas. A pesquisa visa explorar inovações tecnológicas capazes de prevenir tais falsificações e promover a conscientização, destacando os riscos envolvidos e propondo melhores práticas. A validação dos resultados por meio de estudos de caso é considerada essencial para fundamentar conclusões e contribuir para o avanço contínuo da pesquisa em segurança biométrica, proporcionando insights valiosos para a comunidade científica e profissional.

No âmbito deste projeto em Python, os materiais empregados incluem a biblioteca OpenCV (cv2) para manipulação e processamento de imagens, a biblioteca NumPy (np) para realizar operações eficientes em arrays multidimensionais, a biblioteca Pillow (Image do PIL) para operações relacionadas a imagens, e a biblioteca Matplotlib (plt) para criar visualizações gráficas. Os métodos adotados envolvem a detecção de spoofing em impressões digitais, uma técnica que visa enganar sistemas biométricos por meio de reproduções falsas em vez de amostras biométricas reais. A abordagem se baseia na comparação direta de duas imagens, utilizando funcionalidades do OpenCV, para verificar a presença de evidências de spoofing. Este método proporciona uma análise visual das bordas das imagens e utiliza limiares predefinidos para identificar potenciais discrepâncias, formando assim uma estratégia eficaz para a detecção de falsificações em sistemas biométricos.

O desenvolvimento do projeto seguiu uma abordagem de pesquisa e aplicação, concentrando-se no estudo de uma das diversas aplicações do processamento digital de imagem no cotidiano. Inicialmente, a escolha do tema ”Reconhecimento de impressões digitais falsas” foi fundamentada por uma pesquisa na internet, explorando projetos e artigos relacionados ao uso de processamento digital de imagem para essa finalidade. Com um entendimento prévio do tema, o grupo de pesquisa iniciou a implementação, partindo de um código base desenvolvido pelos integrantes. A análise e estudo do funcionamento do reconhecimento de impressões digitais falsas foram realizados, buscando compreender as nuances do processo. A implementação utilizou as bibliotecas OpenCV (cv2), NumPy (np), Pillow (Image do PIL), e Matplotlib (plt) para realizar a detecção de spoofing em impressões digitais.

Essa escolha de bibliotecas destacou-se como fundamental para as etapas de processamento de imagem e análise visual das bordas, contribuindo para a eficácia do método proposto.

Os resultados deste projeto culminaram em uma eficiente detecção de spoofing em impressões digitais, realizada por meio da comparação das bordas de duas imagens distintas: uma presumivelmente real e outra potencialmente falsa (spoof). A abordagem adotada fundamentou-se na análise da diferença entre as imagens de bordas, com a aplicação de um limiar predefinido para identificar possíveis manipulações. O desfecho final do processo oferece uma conclusão decisiva sobre a autenticidade da impressão digital, indicando se é considerada autêntica ou se existem suspeitas de spoofing. Esses resultados destacam a eficácia do método implementado, fornecendo uma contribuição valiosa para a detecção confiável de falsificações em sistemas biométricos.

REFERENCES

[1] Kaspersky, Kaspersky. Impressões digitais: por quê somos únicos?, 2021. Doi:https://www.kaspersky.com.br/resource-center/definitions/biometrics Disponível em: https://www.kaspersky.com.br/resource-center/definitions/biometrics. Acesso em: 1 de dezembro de 2023.

[2] SILVA, Fernando. O que é biometria?, 2015. Doi:https://www.ufmg.br/espacodoconhecimento/impressoes-digitais-por-que-somos-unicos/ Disponível em: https://www.ufmg.br/espacodoconhecimento/impressoes-digitais-por-que-somos-unicos/. Acesso em: 1 de dezembro de 2023.

[3] HID, Global. Biometria por impressão digital, 2023. Doi:https://www.hidglobal.com/pt/solutions/fingerprint-biometrics Disponível em: https://www.hidglobal.com/pt/solutions/fingerprint-biometrics. Acesso em: 1 de dezembro de 2023.

[4] SILVA, Murilo Varges da. Detecção de impressões digitais falsas no reconhecimento biométrico de pessoas. 2015. 99 f. Dissertação (mestrado) - Universidade Estadual Paulista Julio de Mesquita Filho, Instituto de Biociências, Letras e Ciências Exatas, 2015.