Aspectos de segurança no reconhecimento facial

B.V. Costa, G.B. Oliveira e G.E. Sgarbi.
Departamento de Ciência da Computação, UNIP, São Jose do RioPreto – SP, Brasil.

ABSTRACT: Facial recognition plays a crucial role in our lives, from surveillance systems to security issues like unblocking devices, allowing purchases and access to banking accounts. For security reasons most mobiles manufactures don't say much about their technology involving face recognition. The goal of this work is to try to gather information regarding what elements are used in the facial recognition process to allow for better security and prevent cheating for mobile phones. Our findings show that modern mobile phone use data from infrared sensor along with image for better security, functions that are not commonly found in image recognition algorithms. Without such functions facial recognition can easily be cheated.

1. INTRODUÇÃO

A biometria é muito utilizada nos dias atuais pela sua facilitação de identificação de pessoas no geral, é baseada em métodos de reconhecimento a partir de características físicas de indivíduos. Como cada pessoa é única, esses aspectos físicos permitem um reconhecimento exclusivo a partir do cadastro realizado, sendo a impressão digital um bom exemplo disso.

O reconhecimento facial lida com a identificação de faces a partir de imagens, existem aproximadamente 80 pontos nodais na face de uma pessoa e esses nós são as variáveis que nos tornam únicos. É a distância entre os olhos, curvatura, espessura dos lábios, cicatrizes, marcas de expressão, e até mesmo o comprimento do nariz, entre outras dezenas de características.

O processo de reconhecimento de face converte informações analógicas (face) em um conjunto de informações digitais (dados) com base nas características faciais de uma pessoa. A análise do seu rosto se torna basicamente uma fórmula matemática. O código digital é chamado de impressão digital facial. Assim como as impressões digitais são únicas, todos têm suas próprias impressões digitais faciais.

Atualmente, o reconhecimento facial tem se tornado muito importante por ser uma tecnologia cada vez mais utilizada em protocolos de segurança. Um bom exemplo de uso dela é o desbloqueio de aparelhos digitais, onde ela acaba substituindo o uso da senha. Além das aplicações como controles de acesso e câmeras de monitoramento para identificação de terroristas ou pessoas procuradas em câmeras de aeroporto, reconhecimento de usuários em caixas de banco, acesso a locais restritos, entre outros. Deste modo, o reconhecimento facial é um ponto de segurança que está em constante crescimento. Além de diferentes algoritmos de reconhecimento facial conhecidos, empresas como Apple, Xiaomi, Samsung e outros produtores de aparelhos eletrônicos também possuem sua própria segurança para reconhecimento facial, utilizando tecnologias e algoritmos próprios a fim de aumentar a segurança de seus usuários.

O propósito desse artigo é encontrar os padrões utilizados em alguns dos algoritmos anteriormente citados, e assim descobrir os principais métodos e focos de interesse a partir da informação captada de um rosto.

2. TRABALHO RELACIONADOS

Para o reconhecimento facial, citamos dois artigos relacionados ao tema: 1 – As informações de segurança de reconhecimento facial sobre a Apple. 2 – Apresentação das evoluções de tecnologias relacionadas ao reconhecimento facial.

2.1 SOBRE TECNOLOGIA AVANÇADA EM FACE ID DA APPLE

A Apple afirma que utiliza um dos mais avançados softwares e hardwares para possibilitar o Face ID. O código usa dados capturados pela câmera projetando e analisando pontos invisíveis que criam um mapa de profundidade do rosto bem como capturam imagem infravermelha – esses dados são transformados em uma representação matemática que é comparada a representação contida no banco, ambos protegidos por criptografia. De acordo com dados da marca, a probabilidade de um usuário aleatório desbloquear seu celular é de 1 em 1.000.000 usando ou não uma máscara. A restrição ou sugestão aqui é que crianças abaixo de 13 anos ou quem possuem irmão gêmeo utilize outro tipo

de identificação já que nessas situações as características faciais podem não ser distinguíveis ou ter se desenvolvido plenamente. [1][2]

2.2 UMA REVISÃO SOBRE TECNOLOGIAS DE RECONHECIMENTO FACIAL

O reconhecimento fácil é uma subdivisão do problema de reconhecimento de padrão visual. O reconhecimento fácil está relacionado a tecnologias que foram construídas para um sistema de reconhecimento facial, incluindo detecção da face, sua posição, reconhecimento de identidade, processamento de imagem, entre outros. Dentro do desenvolvimento histórico da evolução de algoritmos de reconhecimento facial, podemos iniciar citando o PCA ou Análise de Componente Principal, implementado em 1991 pelo MIT. O PCA é normalmente utilizado em pré-processamento de imagem para redução de informação e barulho. O LDA, por sua vez, é usado para reconhecimento de dados com labels, sendo sua principal função o uso de classificação. Em 1995 o SVM ou Máquina de Suporte de Vetor foi proposta se tratando de um algoritmo de solução para reconhecimento facial de alta dimensão. A partir de seu desenvolvimento temos o algoritmo do Adaboos proposto por Schapire usado para detecção facial e também, o algoritmo de pequenas amostras aumentando efetivamente a retenção de informação da imagem enquanto reduz o impacto de barulho bem como melhorando a capacidade de reconhecimento. Por fim, o Deep Learning que é um ramo de machine learning, possibilitando a detecção das características necessárias para a classificação automática no processo de treinamento, transformando completamente o campo de reconhecimento facial. [3]

3. TESTES E RESULTADOS

Para os testes realizados, foram utilizados três smartphones diferentes com seus algoritmos próprios e uma máquina para utilização do algoritmo implementado.

- Smartphone I: Celular pessoal, Apple, Iphone, modelo XS, 64 GB Versão IOS: 16.1

- Smartphone II: Celular pessoal, Xiaomi, modelo Mi 11 Lite 128 GB Versão Android: 12 Número versão: SKQ1.210909.001

- Smartphone III: Celular pessoal Motorola moto g (60)s 128gb versão do Android 11 número da versão RRLS31.Q2X-70-39-5

- Máquina para implementação do algoritmo: Computador pessoal, Intel(R) Core (TM) i5-7400 CPU @ 3.00GHz, 8,00 GB de Memória RAM, Sistema operacional de 64 bits, processador baseado em x64, placa de vídeo GT 1030 2GB GDDR5 Versão do driver 512.15, versão Python 3.9.5 e Visual Studio Code version 1.72.

De modo geral, podemos dizer que algoritmos de reconhecimento facial possuem três fases: detecção de face que consiste em localizar um rosto a partir de uma imagem complexa contendo vários elementos e individualizar o rosto; normalização – padronização da imagem para que possam ser comparados os mesmos parâmetros contidos no banco de dados; reconhecimento - avaliação da imagem a ser reconhecida comparando-a com imagens do banco de dados. Nesta fase temos variações de metodologias e se trata da fase em que os usuários terão acesso e poderão tentar quebrar o reconhecimento.

Com base no objetivo do trabalho, alguns dos principais algoritmos de reconhecimento facial foram testados. A princípio testamos a funcionalidade padrão, sem cobrir nada, para verificar se o algoritmo funcionava perfeitamente. Após esse veredito, omitimos elementos passo a passo, a fim de testar a segurança do reconhecimento e buscar padrões entre os dispositivos.

Dentre esses elementos presentes na face: olhos, nariz, testa, boca, orelhas, queixo, escondendo os elementos. Também foi utilizado óculos escuros para o teste.

A partir dos testes realizados, encontramos um padrão entre eles. A área de interesse dos algoritmos de reconhecimento de imagem, se inicia com o triângulo do rosto, olhos, nariz e alguns deles a boca, a partir disso eliminando áreas não reconhecidas, e localizando as conhecidas do banco de imagens. Na tabela 1 abaixo apresenta esses resultados.

TABELA 1 - RESULTADO DOS TESTES REALIZADOS

MÉTODOS:	APPLE	XIAOMI	MOTOROLA	ALGORITMO
OLHOS FECHADOS	0%	0%	0%	100%
COBRINDO TESTA E ORELHA	100%	100%	100%	100%
COBRINDO SOMENTE TESTA	100%	100%	100%	100%
COBRINDO SOMENTE ORELHA	100%	100%	100%	100%
COBRINDO SOMENTE NARIZ	70%	80%	80%	80%
COBRINDO SOMENTE QUEIXO	100%	100%	100%	100%
COBRINDO SOMENTE BOCA	100%	100%	0%	100%
COBRINDO BOCA E QUEIXO	100%	100%	0%	100%
COBRINDO NARIZ, BOCA, QUEIXO E ORELHA	70%	90%	33,33%	66,66%
UTILIZANDO ÓCULOS ESCURO	100%	0%	100%	100%

Foi realizada uma comparação entre os diferentes algoritmos, e com isso foi possível analisar diversos padrões e a precisão de cada um.

A partir do pensamento de buscar padrões, foi decidido esconder essas partes. Cobrindo pontos laterais da face, o extremo superior (testa), extremo lateral (orelhas), extremo inferior (queixo), esses extremos por si só não altera a validade do reconhecimento como um todo.

Após isso, a parte inferior e superior central do rosto foram escondidas a fim de encontrar quais são os elementos faciais que o algoritmo utiliza. Realizando a omissão da parte superior total olhos e nariz, foi detectado que o algoritmo não reconhece de maneira alguma, partindo dessa linha de raciocínio, o inverso foi testado, a parte inferior apenas boca e queixo, detectando assim um padrão, o triângulo principal: olhos e nariz. Em um caso especifico (Motorola) ele necessita ao menos do lábio superior da boca.

Os óculos escuros foram importantes para detectar também qual seria a próxima etapa de detecção de elementos, o olho estando com a opacidade reduzida o algoritmo iria comparar qual outro elemento. Esse tipo de padrão de dados implica que os pontos extremos (queixo, testa e orelha) são levados em consideração apenas caso não seja obtido a validade do reconhecimento com os pontos centrais.

O código implementado não possui a principal característica entre os mais utilizados métodos de reconhecimento facial, como detecção de profundidade através do uso de câmeras infravermelho, apesar disso, consegue detectar a face de modo equivalente aos outros algoritmos utilizados nos smartphones testados. Abaixo é apresentada imagem do algoritmo em funcionamento, onde com o usuário cadastrado no banco de dados, ele é reconhecido e identificado com nome.

Figura 1 – Usuário sendo reconhecido pelo algoritmo

O algoritmo utilizado em uma imagem colorida impressa, a esquerda de um usuário cadastrado onde ele é identificado com o nome, e a direita um usuário não cadastrado é identificado como desconhecido pelo algoritmo.

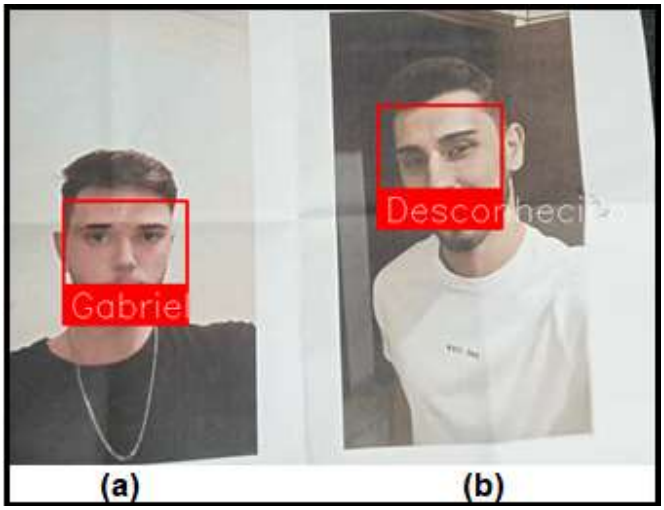

Figura 2 – Exemplo da aplicação do algoritmo: (a) Usuário reconhecido pelo algoritmo, (b) Usuário não reconhecido pelo algoritmo

4. CONCLUSÃO

Nesse artigo, foram realizados diferentes métodos para a leitura facial na tentativa de burlar o sistema de reconhecimento. Com base nisso, identificamos que orelha e o queixo são itens menos levados em conta. Já os olhos para Apple e Xiaomi é um dos elementos mais importantes, pois é visto primeiramente o olho e depois o resto dos componentes do rosto. No iphone,

utilizando alguns óculos escuros, ele buscará pelo triângulo superior olho-testa-nariz. Caso isso não esteja disponível, ele passará a procurar o olho, óculos escuros e o triângulo inferior.

O reconhecimento facial nos principais celulares, não utiliza apenas câmeras simples, ao menos utilizam o infravermelho para reconhecimento de profundidade. Com esses dados obtidos é realizado uma transformação em uma regra matemática. Assim ele contrasta com aquilo na qual foi implementado, onde o algoritmo não apresenta nenhum tipo de segurança nesse sentido de distância, estando vulnerável a trapaças com imagens impressas ou digitais.

Um dos padrões mais seguros que deve se ressaltar, é que nos dispositivos testados ao menos um olho deve estar aberto, caso contrário, o algoritmo nem cogita realizar a leitura da face, a partir disso pode-se entender que é uma medida de segurança aplicada contra violência de privacidade. O olho é um ponto central de testes, caso ele não seja identificado o algoritmo não cogita, de forma alguma validar a face. Após os olhos validados, o nariz é verificado formando o triângulo superior, caso não identificado ou seja difícil de identificar, são utilizados outros elementos (extremos) secundários como a testa, orelha e queixo.

Diante os testes realizados, concluímos que o algoritmo implementado possui diversas falhas de segurança, na qual é facilmente enganado quando é utilizado uma imagem do usuário, seja de forma impressa, por meio da tela de qualquer celular, ou até mesmo pela tela de um computador, ele consegue realizar a leitura facial normalmente. Enquanto os dispositivos utilizados são bem mais precisos em relação ao algoritmo implementado, implicando que não somente as diferenças entre as imagens podem ser validadas, mas também a profundidade e distância entre elementos.

5. REFERÊNCIAS

[1] APPLE, **About Face ID advanced technology.** Disponível em: < https://support.apple.com/en-us/HT208108 >. Acesso em: 10 de outubro de 2022.

[2] AWS, **O que é reconhecimento facial.** Disponível em: < https://aws.amazon.com/pt/what-is/facial-recognition/ >. Acesso em: 27 de setembro de 2022.

[3] LIXIANG LI, XIAOHUI MU, SIYING LI, HAIPENG PENG, **A Review of Face Recognition.** Disponível em: < https://www.researchgate.net/publication/343118558_A_Review_of_Face_Recognition_Technology >. Acesso em: 22 de outubro de 2022.

[4] KASPERSKY, **O que é reconhecimento facial – definição e explicação.** Disponível em: < https://www.kaspersky.com.br/resource-center/definitions/what-is-facial-recognition >. Acesso em: 12 de outubro de 2022.

[5] PONTOTEL, **Entenda como funciona a biometria facial no controle de ponto e confira as vantagens.** Disponível em: < https://www.pontotel.com.br/biometria-facial/ >. Acesso em: 15 de outubro de 2022.

[6] SERASA EXPERIAN, **Biometria Facial Processo de identificação ágil, eficiente e sem atrito.** Disponível em: < https://www.serasaexperian.com.br/solucoes/biometria-facial/ >. Acesso em: 12 de outubro de 2022.

[7] STAN Z. LI, ANIL K. JAIN, **Handbook of Face Recognition.** Disponível em: < https://link.springer.com/book/10.1007/978-0-85729-932-1 >. Acesso em: 20 de outubro de 2022.

[8] TOM SIMONITE, **How Face Recognition Can Destroy Anonymity.** Disponível em: < https://www.wired.com/story/how-face-recognition-destroy-anonymity/ >. Acesso em: 22 de outubro de 2022