UNIVERSIDADE FEDERAL DA BAHIA

DEPARTAMENTO DE CIÊNCIA DA COMPUTAÇÃO

PROGRAMA DE GRADUAÇÃO

ADEILSON ANTÔNIO DA SILVA

DETECÇÃO DE FRAUDES NA AUTENTICAÇÃO FACIAL MULTIMODAL

Salvador - BA, Brasil

25 de julho de 2019

Adeilson Antônio da Silva

Detecção de fraudes na autenticação facial multimodal

Monografia apresentada para obtenção do Grau de Bacharel em Ciência da Computação pela Universidade Federal da Bahia.

Universidade Federal da Bahia

Departamento de Ciência da Computação

Programa de Graduação

Orientador: Maurício Pamplona Segundo

Salvador - BA, Brasil

25 de julho de 2019

Adeilson Antônio da Silva
Detecção de fraudes na autenticação facial multimodal/ Adeilson Antônio da Silva. – Salvador - BA, Brasil, 25 de julho de 2019-
31 p. : il. (algumas color.) ; 30 cm.

Orientador: Maurício Pamplona Segundo

Monografia – Universidade Federal da Bahia
Departamento de Ciência da Computação
Programa de Graduação, 25 de julho de 2019.

1. reconhecimento facial. 2. infravermelho. 2. padrões binários locais. 3. autenticação contínua. I. Maurício Pamplona Segundo. II. Universidade Federal da Bahia. III. Departamento de Ciência da Computação. IV. Autenticação Facial Contínua usando Imagens de Infravermelho

Adeilson Antônio da Silva

Detecção de fraudes na autenticação facial multimodal

Monografia apresentada para obtenção do Grau de Bacharel em Ciência da Computação pela Universidade Federal da Bahia.

Trabalho aprovado. Salvador - BA, Brasil, 15 de setembro de 2017:

Maurício Pamplona Segundo
Orientador

Rubisley de Paula Lemes
Avaliador

Ivan do Carmo Machado
Avaliador

Salvador - BA, Brasil
25 de julho de 2019

Agradecimentos

Reservo este parágrafo à família, e assim sendo, inicio agradecendo a meus pais, Mary Márcia da Silva e Adilson Santos da Silva, por todo apoio e confiança durante todos esses anos. Eles são a base de tudo que sou e jamais chegaria até aqui não fosse pelo esforço deles, que dedicaram suas vidas para que eu me tornasse um ser humano melhor. Agradeço também a pessoas que foram essenciais para minha entrada e permanência na universidade, através de seus conselhos e palavras de incentivo. Sônia Santos da Silva, minha tia e segunda mãe, e Caroline Ferraz Silva, amiga e companheira de todas as horas. Agradeço também a todos meus familiares por todas as palavras de conforto e de carinho, privilégio que nem todos nesse mundo podem ter. As reuniões familiares que faltei, os almoços que não compareci, as festas em que fiquei pouco tempo, tudo isso culpando a faculdade, não foram em vão.

Reservo este parágrafo aos professsores e mestres. Começo agradecendo a meu orientador, Maurício Pamplona Segundo, que me abriu as portas da ciência na universidade e me ajudou a entender como funciona todo processo de construção do conhecimento. Por ser também um grande ponto de inspiração, por todo conhecimento que possui e que não mede esforços para compartilhar. Agradeço os conselhos e também as risadas que compartilhamos. Registro também aqui a admiração que tenho pelos outros professsores do Departamento de Ciência da Computação da UFBA, que me ajudaram a perceber quão grande é o mundo da computação. Apesar de toda dificuldade de se fazer ciência no Brasil eles seguem firmes, fazendo de tudo para levar o nome do DCC-UFBA à frente.

Reservo este parágrafo aos amigos e colegas de curso. Não posso deixar de agradecer a todos os membros da InfoJr UFBA, espaço de aprendizado e de crescimento, onde tive a honra de me desenvolver como pessoa, como líder e que me deu retorno por cada segundo de trabalho investido nos últimos três anos. Sem a InfoJr UFBA não teria me desenvolvido tanto e conquistado tanta coisa dentro da universidade. Tive a honra de liderar pessoas, organizar eventos, virar noites desenvolvendo projetos, faltar consultas médicas para fazer reuniões com clientes e passar diversas horas fazendo reuniões para definir o futuro de pessoas que sequer conhecia. Tudo isso com o enorme prazer de poder dizer que fazia (e farei enquanto possível) parte da primeira Empresa Júnior de Informática do Nordeste! Agradeço também a todos os amigos de laboratório por todo companheirismo e toda colaboração para o andamento de todos os projetos que tive a chance de participar.

Gostaria de deixar registrado também o nome do Instituto Cultural Steve Biko, que através do projeto Oguntec me permitiu começar a entender, antes mesmo de sonhar em entrar na universidade, o que é ser um cientista. Foi lá que aprendi que era possível sim

para um jovem negro e de periferia entrar numa universidade pública e ocupar um espaço há tantos anos negado aos seus semelhantes. A educação é, sem dúvidas, a ferramenta mais poderosa que eles me deram.

"Eu certamente não estava buscando nenhum diploma, da forma como uma faculdade confere um símbolo de status aos seus alunos. Minha educação caseira me deu, com todos os livros adicionais que eu li, um pouco mais de sensibilidade à surdez, ao idiotismo e à cegueira que afligia a raça negra na América.".

(Malcolm X)

Resumo

Esta monografia apresenta o andamento das atividades de pesquisa realizadas num período de doze meses, cujo foco foi o levantamento de informações e a construção de um protótipo de sistema de reconhecimento de fraudes utilizando imagens coloridas. As principais informações levantadas, como métodos de detecção de fraudes, bem como projetos encontrados que já realizam estes processos serão descritos e discutidos. O sistema construído é apresentado através de uma descrição de suas etapas, como a detecção da face, normalização de pose e extração de características. Os resultados do protótipo construído foram satisfatórios, chegando a apresentar uma taxa de acerto de 99.6% em um dos experimentos realizados.

Palavras-chave: Detecção de fraudes, biometria, visão computacional.

Abstract

This monograph reports the progress of a twelve month research that focused on information gathering and building a prototype of a antispoofing system using color images. The main information gathered, as antispoofing detection methods, just as projects available with the same focus will be analysed and discussed. The built system is presented through a description of its stages, such as face detection, pose normalization and feature extraction. The results of the built prototype were satisfactory, with a 99.6% success rate in one of the experiments.

Keywords: antispoofing, biometrics, computer vision.

Lista de ilustrações

Lista de tabelas

Lista de abreviaturas e siglas

3DMAD	3D Mask Attack Database
LBP	Local Binary Pattern
SVM	Support Vector Machines

Sumário

1 Introdução

Sistemas de identificação de indivíduos que utilizam biometria têm sido cada vez mais utilizados atualmente. Esses sistemas geralmente oferecem um nível maior de segurança em relação a sistemas comuns de autenticação, pois utilizam características físicas ou comportamentais de indivíduos (*e.g.* face, íris, voz, impressão digital) para verificar a identidade (BOLLE et al., 2003). Apesar desse nível maior de segurança, é possível burlar sistemas biométricos. As vulnerabilidades conhecidas podem ser as mesmas encontradas em sistemas computacionais de outros tipos, como exposição a ataques de negação de serviço, ataques à base de dados com a intenção de vazamento de informações, reconstrução de perfil de usuário a partir dos seus padrões biométricos armazenados, dentre outros (JAIN; NANDAKUMAR; ROSS, 2016). Jain *et. al* (JAIN; NANDAKUMAR; ROSS, 2016) aponta para a tentativa de fraude em sistemas biométricos como um dos maiores problemas de segurança especificamente ligados a este tipo de sistema. A intenção de uma fraude é de obter acesso a um sistema ao simular a característica biométrica de outra pessoa sem o consentimento dela. Num sistema convencional isso seria equivalente a ter acesso a dados sensíveis, como nome de usuário e senha.

Um sistema totalmente protegido contra fraudes ainda não existe nos dias atuais (PARVEEN et al., 2015). Apesar disso, existem estudos que buscam criar mecanismos de proteção contra a maioria das formas de fraude já conhecidos. Dentre as fraudes mais comuns, é possível citar o uso de dedos artificiais no caso de sistemas baseados no reconhecimento de impressões digitais, gravações de áudio em sistemas que utilizam reconhecimento de voz, e fotos, vídeos e máscaras no caso de sistemas que utilizam reconhecimento facial (PARVEEN et al., 2015; ERDOGMUS; MARCEL, 2013).

Em trabalhos passados (SILVA; SEGUNDO, 2015), observamos essa necessidade de se analisar a ocorrência de fraudes no reconhecimento facial utilizando fotografias convencionais, também chamadas de imagens coloridas. Nesse contexto, o objetivo desse trabalho foi o levantamento de trabalhos relacionados e a construção de um protótipo de sistema de reconhecimento de fraudes utilizando imagens coloridas. Esta monografia apresenta o andamento atual desse projeto, discute os resultados encontrados até então, e expõe projeções para o futuro da aplicação.

2 Referencial Teórico

Dentro da literatura é possível encontrar estudos sobre diversos tipos diferentes de fraudes a sistemas de reconhecimento facial. Alguns trabalhos dedicam-se a analisar a vivacidade da face apresentada ao sistema, detectando movimentos simples de cabeça, o piscar dos olhos, ou expressões faciais. Um contraponto a esse tipo de estudo é que é possível fazer uma simulação da vivacidade utilizando sequências de vídeo ou até mesmo a movimentação de fotografias impressas. A partir disso, desdobraram-se estudos com foco na análise do impacto da reprodução de imagens faciais utilizando fotografias impressas e até mesmo a reprodução dessas imagens em monitores digitais de computador (TAN et al., 2010) (PEIXOTO; MICHELASSI; ROCHA, 2011).

Peixoto *et. al* (PEIXOTO; MICHELASSI; ROCHA, 2011) dedicou-se a entender se condições de iluminação mais baixas poderiam de alguma forma impactar na detecção de fraudes. A partir disso, reconstruiu uma base de dados para simular os ataques utlizando fotografias de faces mostradas em uma tela LCD e produziu uma extensão de um método apresentado em Tan *et. al* (TAN et al., 2010) para lidar com características de iluminação diferentes. Essa extensão melhorou os resultados da detecção de fraude, reduzindo bastante a taxa de erro durante o processo de classificação.

Määttä *et. al* (MAATTA; HADID; PIETIKAINEN, 2011) propõe a análise da textura das imagens coloridas de faces utlizando variações de padrões binários locais (LBP - Local Binary Patterns) (AHONEN; HADID; PIETIKÄINEN, 2004) e a combinação dessas variações como entrada para um classificador de máquina de vetores de suporte (SVM - Support Vector Machines). Neste trabalho a intenção é de construir um classificador para distinguir entre face real e face impressa em papel. Segundo o autor, a combinação de diferentes abordagens de LBP resulta numa maior discriminabilidade por questões relacionadas as diferenças de absorção e reflexão da luz numa imagem verdadeira e numa tentativa de intrusão, principalmente em regiões mais específicas do rosto como as bochechas. O método proposto atingiu uma taxa de acerto de 0.99, melhorando o estado da arte até então.

André *et. al* (ANJOS; MARCEL, 2011) apresenta resultados relativos análise de imagens impressas em sistemas de reconhecimento facial com imagens 2D. A abordagem proposta utiliza um algoritmo com base em movimento. A intensidade relativa de movimento entre a face e o plano de fundo é levada em consideração, isto é, a quantidade de movimento que acontece em determinada região de interesse na imagem. Por conta da natureza dessa abordagem, o processo de decisão do classificador é dado em função do tempo. Isto significa que determinada quantidade de frames são analisados em um intervalo

de tempo para determinar a quantidade de movimento relativo. Utilizando um limiar do valor de movimento para classificar aquele intervalo como real ou fraude, várias janelas de tempo são avaliadas e então a média das classificações dessas janelas é dada como o resultado da sequência de imagens avaliada. Caso a média seja maior que 0.5, conclui-se que a sequência de imagens é de um acesso real. Caso contrário, são fraudulentas. São avaliados também dois tipos de ataques diferentes, um mantendo as imagens de fraude fixas num suporte e o outro mantendo as imagens sendo seguradas pelo atacante com as mãos. O classificador construído teve melhor performance contra ataques onde a foto é segurada pelo atacante. Segundo o autor, isto se deve à maior quantidade total de energia de movimento e da forma como essa energia é distribuída ao longo do tempo.

Outros trabalhos propuseram-se a estudar o problema da fraude utilizando máscaras 3D que tendem a simular o modelo facial de usuários de uma determinada base de dados (KOSE; DUGELAY, 2013) (ERDOGMUS; MARCEL, 2013). Erdogmus *et. al* (ERDOGMUS; MARCEL, 2013) propõe-se a estudar as diferenças entre variações do método de descrição de textura padrões binários locais (LBP - Local Binary Patterns) (AHONEN; HADID; PIETIKÄINEN, 2004) e a combinação desses processos de descrição com outros métodos de classificação como máquinas de vetores de suporte (SVM - Support Vector Machines), análise de discriminante linear (LDA - Linear Discriminant Analysis) e comparação de histogramas usando qui-quadrado.

3 Sistema

O protótipo desenvolvido é composto por cinco etapas: (1) aquisição de imagens, responsável pela leitura das imagens da base de dados; (2) detecção de faces e olhos, que utiliza classificadores em cascata para encontrar a posição da face e dos olhos nas imagens de entrada; (3) normalização de iluminação e pose, onde a localização da face e dos olhos são utilizadas para alinhar a face em uma posição padrão de forma que as variações na posição do rosto tenham o menor impacto possível no reconhecimento, e então as variações de brilho e contraste da imagem são normalizadas utilizando equalização de histograma para amenizar variações de iluminação do ambiente; (4) extração de características faciais, onde Padrões Binários Locais (LBP, *Local Binary Patterns*) (OJALA; PIETIKAINEN; HARWOOD, 1994) são utilizados para a representação da textura da face; e por fim a (5) classificação entre fraude e não-fraude, etapa onde a textura da face de entrada é analisada para decidir se essa é uma fraude ou não através de uma Máquina de Vetores de Suporte (SVM, *Support Vector Machine*) (CORTES; VAPNIK, 1995). A Figura 1 ilustra estas etapas, e mais detalhes são dados nas seções seguintes.

Figura 1 – Ilustração das etapas do sistema de reconhecimento de fraudes.

3.1 Aquisição de imagens

Nesta etapa, utilizamos as imagens da base de dados *3D Mask Attack Database* (3DMAD) (ERDOGMUS; MARCEL, 2013). Esta base foi construída utilizando gravações de 17 usuários diferentes capturadas por um sensor Microsoft Kinect. As gravações foram realizadas em três sessões, com cinco vídeos de 300 quadros de cada usuário. Nas duas primeiras sessões, as imagens são de um acesso real do usuário num ambiente controlado, com visão frontal e expressões faciais neutras. Na terceira sessão o usuário simula uma fraude utilizando uma máscara 3D. No total, são 76500 quadros com resolução de 640×480 pixels, cada quandro contendo uma imagem colorida e uma imagem de profundidade. A Figura 2 mostra um exemplo de imagens da 3DMAD. É válido salientar que, para a construção das máscaras 3D, os autores da base utilizaram o site *ThatsMyFace.com* utilizando uma foto frontal e duas de perfil de cada um dos 17 colaboradores da base de dados. Através dessa plataforma, foram solicitadas máscaras vestíveis de tamanho real feitas a partir de um composto de resina, com buracos nos olhos e nas narinas, como visualizado na Figura 3.

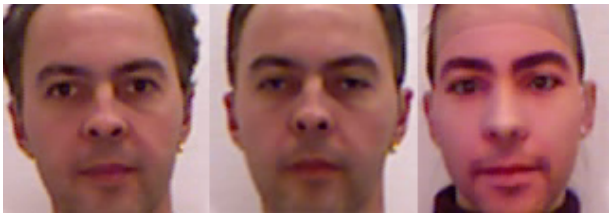

Figura 2 – Exemplo de imagens da 3DMAD de um mesmo usuário: à esquerda, imagem da primeira sessão (*i.e.* acesso real); ao centro, imagem da segunda sessão (*i.e.* acesso real); à direita, imagem da terceira sessão (*i.e.* fraude com máscara).

Figura 3 – Exemplo de máscaras da 3DMAD construídas através do website *ThatsMyFace.com*. Imagem de Erdogmus e Marcel (ERDOGMUS; MARCEL, 2013).

3.2 Detecção da face e dos olhos

Após a aquisição das imagens, o próximo passo é a detecção da face. Para esta finalidade, a aplicação de um classificador em cascata em uma imagem utilizando janelas de busca com tamanho variável é suficiente para classificar as diferentes regiões de uma imagem de entrada entre face e não-face (BAGGIO et al., 2012; VIOLA; JONES, 2004). Após isso, nas regiões identificadas como face, utilizamos um outro classificador em cascata para detectar os olhos. A localização dos olhos é fundamental para a fase seguinte, onde essas informações serão empregadas para realizar a normalização de pose, como ilustrado na Figura 4.

Figura 4 – Exemplo de resultado de detecção da face e dos olhos em um dos quadros. Um recorte da face é realizado e a posição dos olhos é guardada.

3.3 Normalização de pose e iluminação

Com a posição da face e dos olhos conhecida, realizamos o alinhamento dessas características para uma posição padrão, de forma a garantir que as comparações entre duas imagens sempre serão realizadas entre as mesmas partes do rosto (BAGGIO et al., 2012). É possível visualizar esse processo na Figura 5.

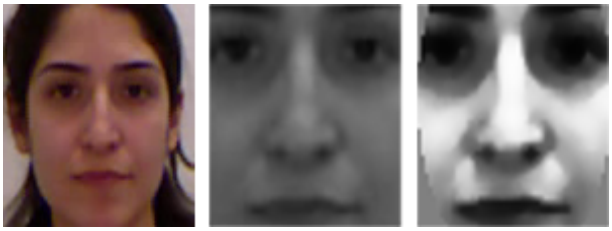

Figura 5 – Ilustração do processo de normalização. Imagem de entrada (esquerda), imagem após transformações geométricas (centro), imagem após equalização de histograma e recorte elíptico ao redor da face (direita).

Inicialmente nós rotacionamos a face para que os olhos fiquem horizontalmente alinhados. Após isso, redimensionamos a imagem de forma a manter uma distância específica entre os olhos. Em seguida, realizamos uma translação para posicionar os olhos numa posição predeterminada da imagem de saída. Por fim, realizamos um corte na

imagem para remover informações desnecessárias ao propósito do sistema, como cabelo, orelhas e plano de fundo.

Após a normalização de pose, realizamos uma normalização de brilho e contraste na imagem. Essa etapa é importante pois, num ambiente não controlado, a iluminação do rosto costuma variar por conta da posição do rosto em relação às fontes de luz. Para reduzir o impacto dessas variações, utilizamos a equalização de histograma nos lados esquerdo e direito da face de forma separada, e depois aplicamos novamente a equalização de histograma em toda a face já contendo as regiões laterais equalizadas. Dessa forma é possível garantir melhores resultados, pois as diferenças de iluminação entre as regiões laterais da face, por já estarem normalizadas, não terão um impacto tão grande na normalização global. A Figura 6 mostra o resultado da normalização de pose e iluminação para as faces mostradas na Figura 2.

Figura 6 – Exemplos de imagens de um mesmo usuário normalizadas: à esquerda e ao centro, duas imagens de acessos reais; à direita, imagem de tentativa de fraude com máscara.

3.4 Extração de Características

Após a normalização da face, realizamos a extração de características LBP (OJALA; PIETIKAINEN; HARWOOD, 1994; AHONEN; HADID; PIETIKÄINEN, 2004). Esse descritor foi escolhido por apresentar os melhores resultados na literatura em termos de extração e representação de informação de textura em imagens coloridas (PARVEEN et al., 2015; ERDOGMUS; MARCEL, 2013).

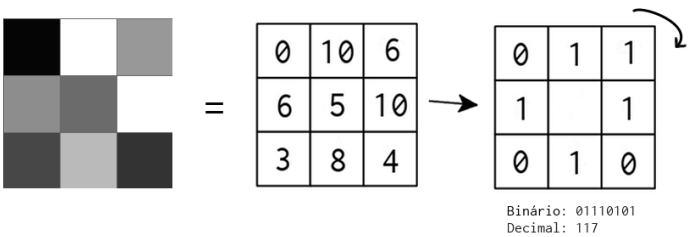

Figura 7 – Ilustração da ideia básica do LBP com vizinhança fixa 3x3.

Na ideia original do LBP, cada pixel da imagem é comparado com seus vizinhos. Caso o valor do pixel vizinho seja maior ou igual ao valor do pixel corrente, o valor

1 é atribuído a esse vizinho, caso contrário, o valor 0 é atribuído. Para cada pixel um número em formato binário é obtido através da concatenação dos valores atribuídos aos seus vizinhos. O operador básico ilustrado na Figura 7 pode ser extendido para utilizar diferentes valores de vizinhos e de raio para o círculo da vizinhança. Aumentar o número de vizinhos ou do raio podem criar a necessidade de realizar interpolações durante o cálculo do lbp, nos casos em que a coordenada de um ponto não possuir correspondência direta com uma coordenada da imagem. No sistema proposto utilizamos raio 1 e 8 vizinhos.

Figura 8 – Divisão da imagem de entrada em subregiões e geração dos histogramas locais que, concatenados, formam o histograma geral da imagem.

Após obter esses números binários, gera-se um histograma que pode ser utilizado como descrição das variações de textura na imagem. É válido salientar que a imagem de entrada é dividida em subregiões, como exemplificado na Figura 8. Dessa forma é possível codificar mais informações espaciais. Cada subregião possui um histograma local e a concatenação dos histogramas locais gera o histograma geral da imagem. Neste trabalho as imagens são divididas em 8x8 subregiões. Os histogramas gerais são utilizados neste trabalho tanto para o treinamento de um classificador quanto para a classificação da ocorrência de fraudes. Dois exemplos do resultado do LBP são apresentados na Figura 9.

Figura 9 – Diferenças entre imagens antes de depois do pré-processamento (esquerda superior e inferior, respectivamente) e as imagens LBP geradas a partir delas.

3.5 Classificação

Na fase de classificação entre fraude e não fraude, utilizamos o SVM. A escolha por esse método se deu novamente pelos resultados apresentados na literatura para imagens coloridas (ERDOGMUS; MARCEL, 2013).

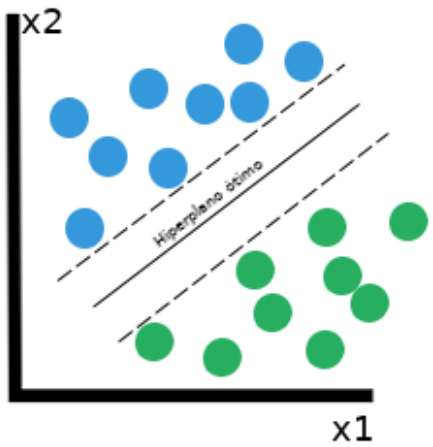

Figura 10 – Ilustração da ideia básica de máquinas de vetores de suporte.

O SVM busca separar duas classes contidas em um conjunto de dados de treino por meio de hiperplanos em espaços multidimensionais. Tomando como exemplo um cenário de duas dimensões, como o da Figura 10, em que os dados são representados pelas elipses coloridas, o SVM tenta encontrar o hiperplano (*i.e.* uma reta nesse caso) que fornece a melhor separação entre os pontos pertencentes a classes distintas, e consequentemente maximizar as diferenças entre as classes contidas no treino. Podem existir diferentes hiperplanos que consigam realizar a separação entre as classes, porém a busca é hiperplano ótimo, pois ele consegue maximizar as distâncias entre as classes utilizadas para treino, tornando o classificador menos sensível a ruído (CORTES; VAPNIK, 1995). Neste trabalho utilizamos a implementação SVM da biblioteca OpenCV (BAGGIO et al., 2012). O kernel escolhido foi o Linear e foi utilizado um método fornecido pela biblioteca para que alguns parâmetros da função do kernel fossem estimados durante o treino.

Uma vez que se encontra a melhor maneira de separar as classes de treino, os vetores de suporte obtidos formam um classificador para o problema. Este pode então ser aplicado em uma nova imagem de entrada (*i.e.* imagem não contida no conjunto de treino) e obtém-se o grau de semelhança dela com cada classe treinada. Na classificação, utilizamos a classe mais similar como a classe estimada para a imagem de entrada, como ilustrado na Figura 11.

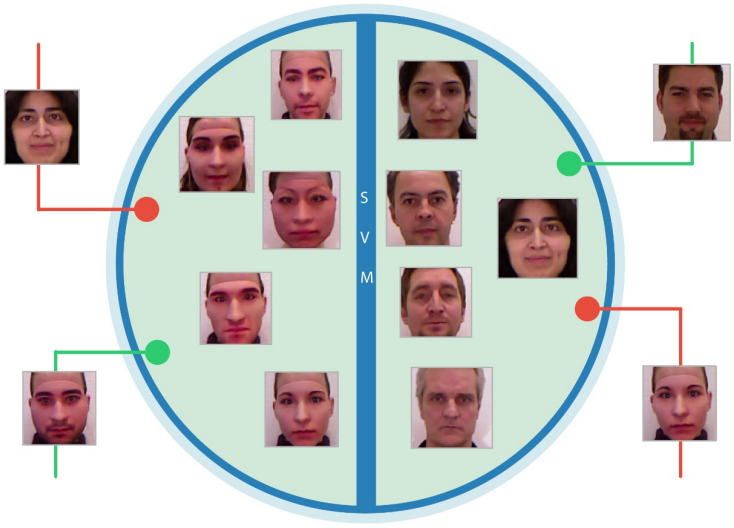

Figura 11 – Ilustração da classificação de fraudes utilizando SVM.

4 Resultados obtidos

O protótipo desenvolvido tem foco na detecção de fraudes utilizando máscaras em imagens coloridas. O sistema detecta faces utilizando classificadores em cascata, normaliza as faces detectadas em relação à pose e iluminação utilizando os métodos descritos em (BAGGIO et al., 2012), extrai características utilizando padrões binários locais e classifica as faces entre fraude e não-fraude utilizando máquinas de vetores de suporte. Os classificadores em cascata utilizados, bem como os métodos de extração do LBP e o método de classificação do SVM são fornecidos pela biblioteca OpenCV.

A base de dados é dividida em três conjuntos diferentes: treino, desenvolvimento e teste. Cada um dos grupos possui, respectivamente, as imagens de sete, cinco e cinco dos usuários. Para os experimentos descritos aqui, foi seguida a recomendação dos autores da base de que o conjunto de teste seja utilizado unicamente para estudos de performance e que os conjuntos de treino e de desenvolvimento sejam utilizados para a construção de classificadores e otimização de parâmetros. Os resultados apresentados neste trabalho foram obtidos sem a utilização do conjunto de desenvolvimento.

Para a avaliação da efetividade do modelo SVM treinado e do método de normalização, dois testes foram realizados: um deles utilizando as imagens obtidas pela detecção facial, sem nenhum tipo de pré-processamento, e o outro utilizando as imagens obtidas após a fase de normalização. Essa separação foi realizada porque, durante os testes, surgiu a suspeita de que o método de normalização, por conta do recorte realizado (ver Figura 6), poderia descartar informações importantes e assim perder poder de descrição, levando a resultados inferiores. Além disso, algumas diferenças de textura foram visualizadas no resultado das imagens LBP, como visto na figura 12.

As três sessões de gravação do subconjunto de treino foram aproveitadas em nossos

Figura 12 – Diferenças entre imagens LBP de face real (esquerda) e de face com máscara (direita), ambas sem o processo de normalização. Algumas diferenças são mais visíveis nessa etapa, como a linha de contorno da máscara na região da testa, por exemplo.

experimentos. Houve apenas uma separação simples entre imagens reais (as duas primeiras sessões) e imagens de máscara (última sessão). Essa separação foi mapeada em duas classes, sendo a classe 1 equivalente às imagens de face real e a classe 2 equivalente às imagens de fraude com máscara. Posteriormente, o classificador SVM foi treinado de forma a separar as imagens dessas duas classes, tendo como dados de entrada os histogramas LBP das imagens utilizadas. A seguir são apresentados os resultados com e sem a etapa de pré-processamento (normalização de iluminação e pose).

4.1 Detecção de fraude sem pré-processamento na imagem da face

No primeiro experimento, não utilizamos o processo de normalização. Para cada vídeo contido na base, as faces foram detectadas e recortadas, as características foram extraídas com o LBP, e as imagens finais foram passadas para o classificador, que retornava o número equivalente à classe de maior confiança do classificador.

Nas imagens de face real, 15000 quadros foram avaliados (*i.e.* 5 vídeos com 300 quadros de cada usuário por sessão, 5 usuários diferentes, 2 sessões). O sistema detectou faces em 14673 quadros, classificou as faces corretamente em 14615 quadros e classificou as faces incorretamente como máscara em 58 quadros, levando a uma taxa de acerto de 99.60% para faces reais.

Figura 13 – Exemplos de faces classificadas. Na linha superior, faces classificadas incorretamente como máscara (esquerda) e como face real (direita). Na linha inferior, exemplos de imagens classificadas corretamente como face real (esquerda) e máscara (direita).

No cenário de teste para imagens de máscara, foram avaliados 7500 quadros (*i.e.* 5 vídeos com 300 quadros de cada usuário por sessão, 5 usuários diferentes, 1 sessão). Foram detectadas faces em 7458 quadros, sendo que 230 foram classificadas incorretamente como faces reais e 7228 foram classificadas como máscaras, o que significa uma taxa de acerto

de 96.91% para fraudes com máscaras. Na figura 13 é possível visualizar algumas imagens e suas classificações.

4.2 Detecção de fraude utilizando pré-processamento na imagem da face

No segundo experimento adicionamos uma etapa de pré-processamento da face para alinhá-la a uma posição padrão e remover variações de iluminação, após a detecção utilizando um classificador em cascata. Após isso as características foram extraídas com o LBP e as imagens finais foram passadas para o classificador, que retornava um número inteiro (1 ou 2) equivalente à classe de confiança do classificador.

Nas imagens de face real, os mesmos 15000 quadros do experimento anterior foram avaliados. O sistema detectou faces e olhos em 14670 quadros, classificou as faces corretamente em 14443 quadros e classificou as faces incorretamente como máscara em 227 quadros, levando a uma taxa de acerto de 98.45% para faces reais.

Figura 14 – Exemplos de faces classificadas. Na linha superior, faces classificadas incorretamente como máscara (esquerda) e como face real (direita). Na linha inferior, exemplos de imagens classificadas corretamente como face real (esquerda) e máscara (direita).

No cenário de teste para imagens de máscara, foram avaliados os mesmos 7500 quadros do experimento anterior. Foram detectadas faces e olhos em 7441 quadros, sendo que 233 foram classificadas incorretamente como faces reais e 7208 foram classificadas como máscaras, o que significa uma taxa de acerto de 96.86% para fraudes com máscaras. Na figura 14 é possível visualizar algumas imagens e suas classificações.

Apesar deste resultado ser ligeiramente inferior ao resultado do experimento anterior, ele é mais confiável por se basear apenas na informação de textura, uma vez que não há artefatos relacionados à forma como as máscaras foram confeccionadas afetando

a classificação (*e.g.* limite entre máscara e testa na Figura 9). Com isso, mesmo se as máscaras cobrirem uma região maior da face, os resultados com pré-processamento provavelmente serão mantidos, enquanto não se pode garantir o mesmo no experimento sem pré-processamento.

5 Conclusão e Trabalhos Futuros

5.1 Conclusao

A base de dados 3DMAD mostrou-se uma boa fonte para o estudo do problema proposto. A quantidade de imagens é adequada e a qualidade delas é alta. Os problemas encontrados foram a falta de variações intensas de pose e iluminação, que podem representar um problema na aplicação desse sistema em ambientes reais.

Foi possível observar que a técnica utilizada para detecção da face e dos olhos foi eficaz para as imagens coloridas durante os testes realizados, localizando a face e ambos os olhos em 98.27% da imagens testadas. Além disso, a combinação de LBP e SVM mostrou-se adequada para a descrição e classificação nesse problema específico (*i.e.* fraudes por máscara em imagens capturadas pelo Microsoft Kinect), alcançando 97.92% de classificação correta nas imagens normalizadas pela etapa anterior. Observamos também que a técnica utilizada para normalização de pose e iluminação diminuiu o desempenho da classificação, mas acreditamos que ela aumenta o poder de generalização do protótipo desenvolvido, pois se baseia apenas nas diferenças de textura que existem entre faces e máscaras, e não em características específicas das máscaras fabricadas. Como visto na tabela 1, a diferença nos resultados com e sem normalização é considerável.

Tabela 1 – Tabela de comparação de resultados

Método	**# imagens**	**# corretas**	**# incorretas**	**Taxa de acerto**
Reais sem normalização	14673	14615	58	99.60%
Reais com normalização	14670	14443	227	98.45%
Falsas sem normalização	7458	7228	230	96.91%
Falsas com normalização	7441	7208	233	96.86%

5.2 Trabalhos Futuros

Como trabalho futuro, pretendemos ampliar o campo de estudo das técnicas de detecção de fraude, incluindo imagens de infravermelho e de profundidade, bem como ampliar os tipos de fraudes considerados para alcançar uma solução mais genérica para o problema.

Atualmente, a utilização de imagens de infravermelho já vem sendo explorada, utilizando imagens impressas para simular faces reais, com a intenção de burlar um sistema de reconhecimento facial. O estudo de fraudes utilizando imagens desse tipo ainda é pouco

explorado na literatura, sendo necessária a construção de uma base de dados própria para dar suporte ao estudo deste problema.

Até então não obtivemos sucesso na tentativa de enganar as aplicações que temos acesso. Como visto na figura 15, uma face real na imagem de infravermelho e a face da fotografia impressa em papel a4 possuem diferenças grandes, o que influencia no resultado do reconhecimento.

Figura 15 – Exemplo de diferenças entre as imagens de infravermelho de acesso real (esquerda) e de fraude utilizando papel a4 (direita).

Outro problema encontrado foi durante a tentativa de utilização de papel fotográfico, como visto na figura 16. A luz emitida pelo Microsoft Kinect é totalmente refetida pelo papel, fazendo com que a face não seja exibida. O comportamento foi o mesmo tanto no papel fotográfico convencional quanto no papel fotográfico fosco. Por conta disso, a aplicação de papel fotográfico foi abandonada.

Figura 16 – Problema encontrado ao utilizar papel do tipo fotográfico. Imagem recapturada colorida (esquerda) e imagem recapturada infravermelho (direita).

Apesar das adversidades encontradas até aqui, ainda acreditamos na possibilidade de fraudar um sistema de reconhecimento facial que utiliza imagens de infravermelho e, por isso, novos materiais serão testados com a intenção de evidenciar tal vulnerabilidade.

Referências

AHONEN, T.; HADID, A.; PIETIKÄINEN, M. Face recognition with local binary patterns. In: _____. *Computer Vision - ECCV 2004: 8th European Conference on Computer Vision, Prague, Czech Republic, May 11-14, 2004. Proceedings, Part I*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2004. p. 469–481. ISBN 978-3-540-24670-1. Disponível em: <https://doi.org/10.1007/978-3-540-24670-1_36>. Citado 3 vezes nas páginas 15, 16 e 20.

ANJOS, A.; MARCEL, S. Counter-measures to photo attacks in face recognition: A public database and a baseline. In: *2011 International Joint Conference on Biometrics (IJCB)*. [S.l.: s.n.], 2011. p. 1–7. Citado na página 15.

BAGGIO, D. L. et al. *Mastering OpenCV with Practical Computer Vision Projects*. [S.l.]: Packt Publishing, Limited, 2012. ISBN 9781849517829. Citado 3 vezes nas páginas 19, 22 e 24.

BOLLE, R. et al. *Guide to Biometrics*. [S.l.]: SpringerVerlag, 2003. ISBN 0387400893. Citado na página 14.

CORTES, C.; VAPNIK, V. Support-vector networks. *Mach. Learn.*, Kluwer Academic Publishers, Hingham, MA, USA, v. 20, n. 3, p. 273–297, set. 1995. ISSN 0885-6125. Disponível em: <https://doi.org/10.1023/A:1022627411411>. Citado 2 vezes nas páginas 17 e 22.

ERDOGMUS, N.; MARCEL, S. Spoofing in 2d face recognition with 3d masks and anti-spoofing with kinect. In: *2013 IEEE Sixth International Conference on Biometrics: Theory, Applications and Systems (BTAS)*. [S.l.: s.n.], 2013. p. 1–6. Citado 6 vezes nas páginas 9, 14, 16, 18, 20 e 22.

JAIN, A. K.; NANDAKUMAR, K.; ROSS, A. 50 years of biometric research: Accomplishments, challenges, and opportunities. *Pattern Recognition Letters*, v. 79, p. 80 – 105, 2016. ISSN 0167-8655. Disponível em: <http://www.sciencedirect.com/science/article/pii/S0167865515004365>. Citado na página 14.

KOSE, N.; DUGELAY, J. L. Shape and texture based countermeasure to protect face recognition systems against mask attacks. In: *2013 IEEE Conference on Computer Vision and Pattern Recognition Workshops*. [S.l.: s.n.], 2013. p. 111–116. ISSN 2160-7508. Citado na página 16.

MAATTA, J.; HADID, A.; PIETIKAINEN, M. Face spoofing detection from single images using micro-texture analysis. In: *Proceedings of the 2011 International Joint Conference on Biometrics*. Washington, DC, USA: IEEE Computer Society, 2011. (IJCB '11), p. 1–7. ISBN 978-1-4577-1358-3. Disponível em: <http://dx.doi.org/10.1109/IJCB.2011.6117510>. Citado na página 15.

OJALA, T.; PIETIKAINEN, M.; HARWOOD, D. Performance evaluation of texture measures with classification based on kullback discrimination of distributions. In: *Proceedings of 12th International Conference on Pattern Recognition*. [S.l.: s.n.], 1994. v. 1, p. 582–585 vol.1. Citado 2 vezes nas páginas 17 e 20.

PARVEEN, S. et al. Face anti-spoofing methods. *Current Science*, v. 108, n. 8, p. 1491–1500, 2015. Citado 2 vezes nas páginas 14 e 20.

PEIXOTO, B.; MICHELASSI, C.; ROCHA, A. *Face liveness detection under bad illumination conditions*. 2011. 3557-3560 p. Citado na página 15.

SILVA, A. A.; SEGUNDO, M. P. Reconhecimento facial 2d para autenticação contínua. In: *Proceedings of the 28th Conference on Graphics, Patterns and Images (SIBGRAPI) – Workshop of Undergraduate Works*. [S.l.: s.n.], 2015. Citado na página 14.

TAN, X. et al. Face liveness detection from a single image with sparse low rank bilinear discriminative model. In: *Proceedings of the 11th European Conference on Computer Vision: Part VI*. Berlin, Heidelberg: Springer-Verlag, 2010. (ECCV'10), p. 504–517. ISBN 3-642-15566-9, 978-3-642-15566-6. Disponível em: <http://dl.acm.org/citation.cfm?id=1888212.1888251>. Citado na página 15.

VIOLA, P.; JONES, M. J. Robust real-time face detection. *International Journal of Computer Vision*, v. 57, n. 2, p. 137–154, May 2004. ISSN 1573-1405. Disponível em: <https://doi.org/10.1023/B:VISI.0000013087.49260.fb>. Citado na página 19.