

Tiago de Freitas Pereira

ESTUDO COMPARATIVO DE TÉCNICAS DE DETECÇÃO DE ATAQUES DIRETOS À SISTEMAS DE  
AUTENTICAÇÃO DE FACE

Campinas  
2012



Universidade Estadual de Campinas  
Faculdade de Engenharia Elétrica e de Computação

Tiago de Freitas Pereira

ESTUDO COMPARATIVO DE TÉCNICAS DE DETECÇÃO DE ATAQUES DIRETOS À SISTEMAS DE  
AUTENTICAÇÃO DE FACE

Qualificação de Mestrado apresentada na Faculdade de Engenharia Elétrica e de Computação como parte dos requisitos exigidos para a obtenção do título de Mestre em Engenharia Elétrica.  
Área de concentração: Computação

Orientador: Professor Doutor José Mario De Martino

Este exemplar corresponde a versão final do exame de qualificação apresentado pelo aluno, e orientado pelo Prof. Dr. José Mario De Martino

---

Campinas  
2012



# Resumo

Resumo

Palavras-chave:



# Abstract

Abstract

Key-words:



# Sumário

<b>1</b>	<b>Introdução</b>	<b>11</b>
1.1	Contextualização e motivação . . . . .	11
1.1.1	Ataque de <i>replay</i> . . . . .	13
1.1.2	Ataque na referência biométrica . . . . .	14
1.1.3	Ataque <i>man-in-the-middle</i> . . . . .	14
1.1.4	Ataque de spoofing . . . . .	15
1.2	Objetivos, Hipóteses e Resultados esperados . . . . .	15
1.3	Organização do trabalho . . . . .	15
<b>2</b>	<b>Revisão da literatura</b>	<b>17</b>
2.1	Bases de dados de referência . . . . .	18
2.2	Spoofing em reconhecimento de face . . . . .	18
2.2.1	Presença de vitalidade . . . . .	19
2.2.2	Características da cena . . . . .	20
2.2.3	Discrepância relativa à qualidade da imagem . . . . .	21
2.3	Considerações Finais . . . . .	23
<b>3</b>	<b>Metodologia</b>	<b>25</b>
<b>4</b>	<b>Conclusões e Perspectivas</b>	<b>27</b>
	<b>Bibliografia</b>	<b>28</b>



# Introdução

## 1.1 Contextualização e motivação

Em uma sociedade moderna, o processo de autenticação é uma tarefa importante para proteger dados e recursos sejam ele físicos ou digitais. Consistindo da confirmação de uma identidade requerida, o processo de autenticação é o primeiro e o mais crítico na cadeia de segurança restringindo acesso a usuários não autorizados.

Para a tarefa de confirmação de uma identidade, utilizam-se elementos que devem corresponder unívocamente ao identificador associado a um determinado usuário. Estes elementos são chamados de fatores de autenticação. Centralizados no usuário que está requerendo a identidade, estes fatores podem ser utilizados isoladamente ou combinados a fim de reforçar a segurança. Os fatores de autenticação são classificados em aquilo que o usuário:

- **Sabe:** Por exemplo, uma senha ou uma frase de segurança;
- **Possui:** Por exemplo, um *token* de segurança, uma chave de cadeado ou um cartão;
- **É:** Por exemplo, uma característica física ou comportamental.

Cada um destes fatores apresentados possui um conjunto de vantagens e desvantagens. O uso mais comum de senhas, é acesso lógico a sistemas computacionais (computadores, e-mail, banco, cartão de crédito e muitos outros). A senha possui a vantagem de ser naturalmente imutável ao longo do tempo, ou seja, caso a mesma não seja mudada, ela continuará tendo o mesmo valor ao longo do tempo. Senhas contudo podem ser tão complexas quanto se queira, ficando a critério de seu detentor criar uma senha que ao mesmo tempo seja segura (de difícil adivinhação para um eventual atacante) e de fácil memorização. Estes critérios, claramente antagônicos, é o principal ponto de ataque a sistemas computacionais baseados em autenticação com senhas. Como um exemplo de vulnerabilidade no uso de senhas, em fevereiro de 2012 78 contas de e-mail de membros do governo da Síria foram invadidas divulgando informações confidenciais<sup>1</sup>. Destas 78 contas de e-mail, 33 a senha era '12345' ou '123456' incluindo a senha do próprio presidente.

---

<sup>1</sup><http://www.dailymail.co.uk/news/article-2100111/New-York-spin-doctor-coached-Syrian-dictator-Assad-swing-sympathies-US-public.html>

*Tokens* geralmente são associados a um segundo fator de autenticação. Como exemplo, um cartão de crédito é um *token* que acompanhado com a senha do cartão reforça a segurança do mesmo. Há bancos que disponibilizam para seus clientes tokens que geram um número aleatório a cada 30 segundos com a finalidade de reforçar o acesso à serviços de *internet banking*. Na Figura 1.1) pode-se observar um token em formato de chaveiro. Estes *tokens* são objetos físicos que podem ser facilmente perdidos, e uma vez perdidos a autenticação fica comprometida por parte do usuário.



Figura 1.1: Token em formato de chaveiro

Biometria é a ciência de reconhecer a identidade de uma pessoa baseada em seus atributos físicos e/ou comportamentais, tais como a face, as impressões digitais, veias da mão, voz e a íris (Li & Jain 2011). O uso da biometria como fator de autenticação possui algumas vantagens. Naturalmente, não é possível esquecer uma característica biométrica e dificilmente esta característica desaparece repentinamente (talvez em casos de acidentes graves). Características biométricas são intrínsecas a pessoa que as possui e portanto é intransferível. Como desvantagem, a biometria pode variar drasticamente ao longo do tempo. Como exemplo, a voz humana pode variar repentinamente quando estamos doentes; nossos traços faciais infelizmente envelhecem ao longo do tempo. Vale ressaltar que métodos de autenticação baseados em biometria são probabilísticos, ou seja, pode ser que o sistema de autenticação rejeite uma entrada autêntica devido à uma série de fatores externos.

As características humanas para serem utilizadas em uma método de autenticação biométrica devem satisfazer alguns requisitos, dentre eles destacam-se:

- Universalidade (toda pessoa deve possuí-la);
- Unicidade (deve permitir distinguir as pessoas);
- Estabilidade (não deve se alterar demasiadamente ao longo do tempo);
- Coletabilidade (deve poder ser medida quantitativamente);
- Desempenho (deve possibilitar um reconhecimento preciso, em tempo hábil);

- Aceitabilidade (deve ser aceitos facilmente por seus usuários);
- Circunvenção (deve dificultar a possibilidade de fraudes).

A tabela 1.1 apresenta um comparativo realizado por (Maltoni, Maio, Jain & Prabhakar 2009) entre as características biométricas mais utilizadas. É possível observar que nenhuma das biometrias apresentadas consegue atender todos estes requisitos com excelência e a escolha de qual utilizar deve levar em conta a natureza e as exigências de cada aplicação (Jain, Bolle & Pankanti 1999).

Tabela 1.1: Comparaçao das características biométricas mais utilizadas

Característica	Universalidade	Unicidade	Estabilidade	Coletabilidade	Desempenho	Aceitabilidade	Circunvenção
Face	Alta	Baixa	Média	Alta	Baixa	Alta	Baixa
Impressão Digital	Média	Alta	Alta	Média	Alta	Média	Média
Geometria das mãos	Média	Média	Média	Alta	Média	Média	Média
Veias da mão/dedo	Média	Média	Média	Média	Média	Média	Alta
Íris	Alta	Alta	Alta	Média	Alta	Baixa	Alta
Assinatura	Baixa	Baixa	Baixa	Alta	Baixa	Alta	Baixa
Voz	Média	Baixa	Baixa	Média	Baixa	Alta	Baixa

Sistemas de autenticação biométrica podem ser grosseiramente representados segundo o fluxograma da Figura ??.

Primeiramente o trato biométrico é capturado via algum tipo de **sensor**. Após esta captura, o trato biométrico capturado é **processado** a fim de extrair as características biométricas e geração da referência biométrica. Quando se está efetuando o cadastro de uma referência biométrica, estas características são **armazenadas** em uma base de dados para acessos futuros. Quando se está efetuando a **autenticação**, estas características biométricas serão utilizadas no processo de comparação com alguma identidade requerida no banco de dados. Conforme pode ser observado na figura ataques podem ser efetuados em qualquer ponto da arquitetura (?). As próximas subseções irão discorrer sobre cada um dos possíveis ataques e soluções para mitigá-los.

### 1.1.1 Ataque de *replay*

O ataque de replay consiste da utilização de dados previamente submetidos da identidade alvo para o sistema de autenticação a fim de obter o acesso não autorizado. Estes dados podem ser obtidos interceptando (*sniffing*) o canal de dados entre o sensor e a unidade de processamento de dados biométricos durante uma autenticação bem sucedida da identidade

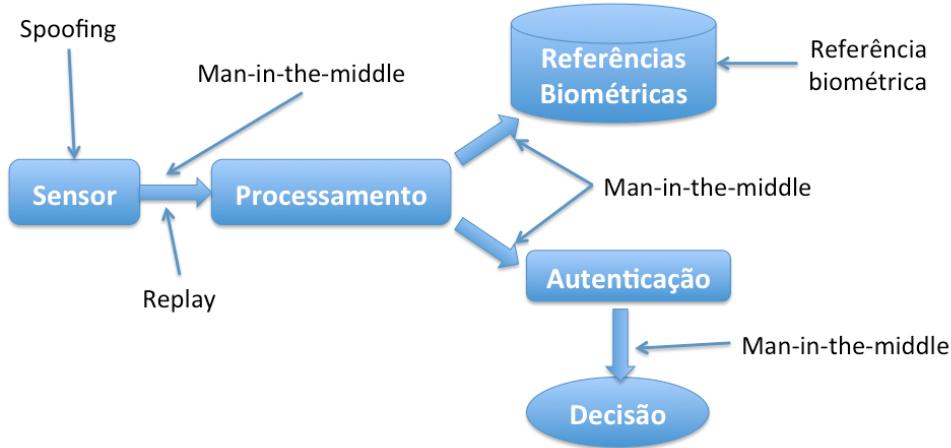


Figura 1.2: Fluxograma de um sistema de autenticação biométrica

alvo. Para deter ataques dessa natureza, o sistema de autenticação biométrica deve assegurar que o dado fornecido não foi injetado artificialmente. Uma forma de se defender deste tipo de ataque é fazer uso da característica probabilística da própria biometria. É praticamente impossível dois processos de captura independentes e em intervalos de tempo distintos gerar exatamente o mesmo dado biométrico. Se isto ocorrer é provável que este dado foi interceptado e está sendo injetado no sistema de autenticação (?).

### 1.1.2 Ataque na referência biométrica

O ataque de referências biométricas consiste em atacar o local de armazenamento das referências biométricas. Com este tipo de ataque pode-se: adicionar uma biometria falsa no sistema de armazenamento, copiar as referências biométricas armazenadas, remover alguma referência biométrica ou modificar as referências biométricas existentes (?). Dentre estas possibilidades a mais perigosa é a cópia de referências biométricas, pois as mesmas podem ser usadas, através de engenharia reversa, para gerar biometrias falsas. (?) demonstrou que é possível gerar impressões digitais falsas através do processo de engenharia reversa com referências biométricas baseadas em minúcias. Com estas impressões digitais fabricadas, foi possível violar um sistema de autenticação baseado em impressões digitais. Um outro ponto de destaque neste tipo de ataque é que uma vez violada uma referência biométrica, a mesma perde a característica da unicidade.

### 1.1.3 Ataque *man-in-the-middle*

O ataque *man-in-the-middle* ou homem do meio é uma forma de ataque em que os dados trocados entre os componentes do sistema de biometria são, de alguma forma, interceptados e alterados pelo atacante. Neste tipo de ataque o atacante pode: interceptar dados sensor, interceptar dados enviados para armazenamento e interceptar dados de decisão do sistema de

biometria. Mecanismos como encriptação dos dados antes de serem transmitidos e/ou prover canais de comunicação seguro podem mitigar este tipo de ataque.

#### 1.1.4 Ataque de spoofing

O ataque de *spoofing* em sistemas de autenticação biométrica, é um tipo de ataque em que o atacante forja o trato biométrico alvo apresentando uma biometria falsa ao sensor, burlando o sistema de autenticação. Em sistemas de autenticação baseados em biometria há duas motivações para se forjar um trato biométrico. A **primeira** motivação é o atacante obter o trato biométrico de outra pessoa a fim de tomar sua identidade. Em sistemas de autenticação baseados na voz, o atacante pode gravar a voz da identidade alvo e usar esta gravação como entrada no sistema de autenticação. Em sistemas de autenticação baseados em impressões digitais o atacante pode obter alguma impressão latente da identidade alvo e gerar um dedo artificial contento a impressão digital roubada. A saber em (?), (?) e (?) são trabalhos relacionados a ataques de *spoofing* em sistemas de autenticação baseados em impressões digitais, em (?), (?) e (?) são trabalhos relacionados a ataques de *spoofing* baseados na biometria da iris e em (?) e (?) são trabalhos relacionados a ataques de *spoofing* em sistemas de autenticação baseados na biometria da voz humana. A **segunda** motivação é um atacante gerar um trato biométrico totalmente artificial (sem se basear em uma biometria real), a fim de enganar o sistema de cadastro e autenticação biométricos. Com isso, o atacante pode compartilhar esta biometria falsa com outros atacantes.

Melhores práticas de segurança orientam utilizar mecanismos como, criptografia de dados e criação de canais seguros para mitigar ataques para a maioria dos casos citados anteriormente (?). No caso dos ataques de *spoofing*, o sensor de biometria (ponto alvo deste tipo de ataque) é o único ponto do fluxograma da Figura 1.2 em que nenhum dos mecanismos são efetivos para mitigá-los, tornando-se assim o ponto mais frágil a ataques e este será o ponto central desta dissertação.

## 1.2 Objetivos, Hipóteses e Resultados esperados

Este projeto verifica duas hipóteses:

## 1.3 Organização do trabalho



# Capítulo 2

## Revisão da literatura

Por sua natureza não intrusiva, autenticação utilizando a biometria da face é uma das áreas mais ativas e desafiadoras no campo da biometria. Apesar do significativo progresso da tecnologia de reconhecimento facial nas últimas décadas em uma série de tópicos como o envelhecimento dos indivíduos e iluminação exterior complexo ainda são desafios de pesquisa na área. Avanços na área foram amplamente relatados em (? , ?). No entanto, a tarefa de verificar se o rosto apresentado a uma câmera é realmente um rosto de uma pessoa real, e não uma tentativa de forjar uma identidade (*spoof*) tem sido quase sempre esquecido. A Figura 2.1 apresenta os fluxos da informação no caso de um acesso real e em no caso de um ataque de spoofing.

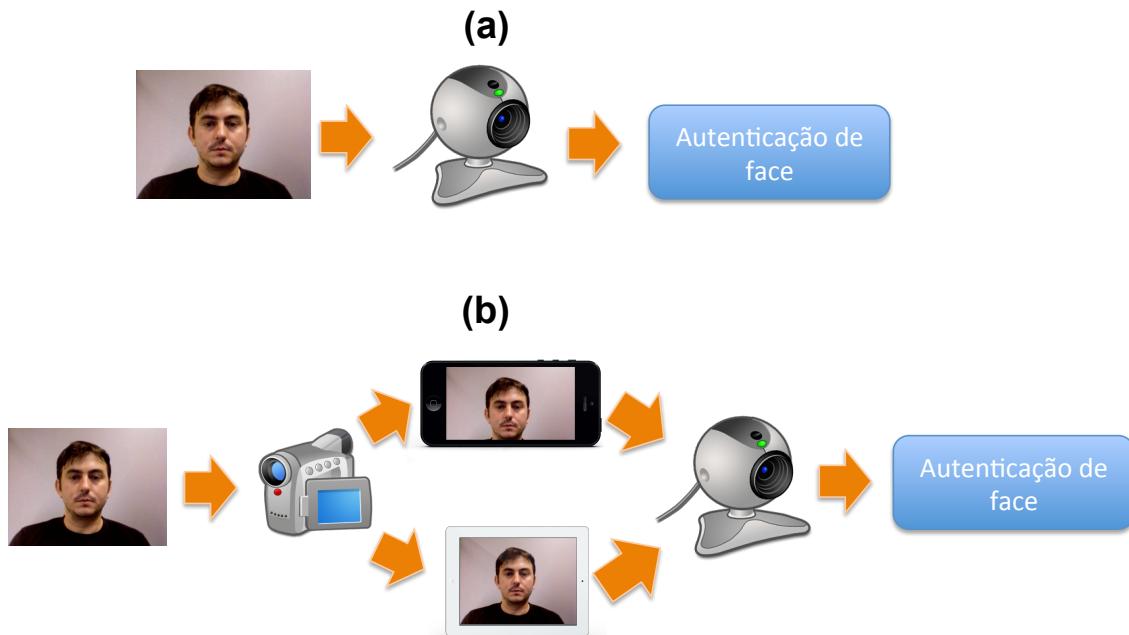


Figura 2.1: (a) Fluxo da informação em um acesso real (b) Fluxo da informação em um ataque de spoofing

Recentemente, a mídia tem documentado algumas situações de ataques em sistemas de reconhecimento de face em produção. Usando fotografias simples, um grupo de pesquisa da

Universidade de Hanói mostrou que com relativa facilidade é possível burlar os sistemas de autenticação face em produção nos laptops Lenovo, Asus e Toshiba (?). Desde o lançamento da versão *Ice Cream Sandwich*, o sistema operacional Android vêm com um sistema de autenticação de face embarcado com a finalidade de desbloquear o celular. Desde então, tem sido amplamente demonstrado em toda a web como é possível burlar esta barreira de autenticação. Como resposta, uma contramedida baseada no piscar de olhos, foi introduzida na versão mais recente do sistema operacional Android.

Deficiências contra ataques de spoofing não é exclusividade da biometria facial. Podem ser observados em (?, ?, ?) que sistemas biométricos baseados em impressões digitais sofrem de fraqueza semelhante. A mesma deficiência em sistemas de reconhecimento de íris foram diagnosticados em (?, ?). Finalmente, em (?, ?) ataques spoofing para reconhecimento de locutor são abordados.

Este capítulo está organizado da seguinte maneira: Na Seção 2.1 serão apresentados as principais bases de dados de referência para o estudo de ataques de *spoofing* em sistemas de reconhecimento facial. A Seção 2.2 apresenta uma sucinta revisão da literatura apresentando algumas estratégias para lidar com o problema. Por fim na Seção é apresentado as considerações finais do capítulo.

## 2.1 Bases de dados de referência

REPLAY, NUAA, CASIA.

## 2.2 Spoofing em reconhecimento de face

Um sistema de autenticação baseado na biometria de face pode ser forjada de diversas maneiras (?) e são elas a apresentação para a câmera de:

- Fotos com a face do usuário alvo;
- Vídeos com a face do usuário alvo;
- Máscaras construídas a partir da face do usuário alvo;
- Maquiagem na tentativa de imitar a identidade do usuário alvo;
- Cirurgia plástica na tentativa de imitar a identidade do usuário alvo.

Embora seja possível para falsificar um sistema de autenticação de face utilizando maquiagem, cirurgia plástica ou máscaras; fotografias e vídeos são provavelmente as ameaças mais comuns. Além disso, devido à crescente popularidade das redes sociais na WEB, (facebook, youtube, flickr, instagram e outros) uma grande quantidade de conteúdo multimídia, especialmente vídeos e fotografias, estão disponíveis e estes dados podem ser utilizados facilmente para atacar um sistema de autenticação de faces. Para mitigar os sucessos dos ataques dessa natureza, contramedidas eficazes deve ser pesquisadas e desenvolvidas.

Contramedidas para ataques de spoofing em reconhecimento de face podem ser classificados quanto à dependência da colaboração do usuário. Métodos que são ditos colaborativos, partem do princípio que a pessoa que está efetuando a autenticação deve favorecer o mesmo, executando alguma atividade do tipo desafio-resposta. Em (?) e (?) o usuário é orientado a falar um texto gerado automaticamente e os movimentos labiais são correlacionados com reconhecimento de fala a fim de gerar uma checagem forte acerca da presença de um usuário em frente à câmera.

Métodos que não são colaborativos, operam com imagens ou vídeos capturados por câmeras convencionais sem exigir uma interação com o usuário que está efetuando a autenticação. Uma vantagem clara nas abordagens desse tipo é que a usabilidade de sistemas de autenticação de face não é onerada, já que o usuário não toma ciência de que uma checagem de sua presença em frente a câmera está sendo efetuada. Dada a vantagem descrita métodos dessa natureza serão explorados neste trabalho.

Estratégias não colaborativas podem ser classificados em estratégias que exploram:

- Presença de vitalidade (liveness detection);
- Características da cena;
- Discrepância relativa a qualidade da imagem;

### 2.2.1 Presença de vitalidade

Presença de vitalidade ou *liveness detection* consiste na seleção de características faciais que apenas pessoas vivas conseguem reproduzir.

O piscar de olhos é uma tarefa involuntária que os seres humanos executam constantemente. Um ser humano comum pisca de forma involuntária em média uma vez a cada 2 ou 6 segundos para manter os olhos limpos e umedecidos. Este intervalo pode variar drasticamente em situações de stress aumentando este intervalo para mais de 20 segundos. Contudo, não importa a situação de stress em que se está submetido; em algum momento este movimento irá ocorrer e não há estabelecido um limite máximo estabelecido em que um ser humano consegue suportar sem piscar os olhos. Apoiado nesta hipótese, (?, ?) desenvolveram uma contramedida baseada no piscar dos olhos com o objetivo de bloquear ataques efetuados com fotografia. O sistema desenvolvido modela a piscadela utilizando cadeias escondidas de markov (HMM) mapeando os estados de olho aberto para olho fechado e olho aberto novamente. Experimentos foram conduzidos utilizando uma base de dados criada pelos autores e livremente disponível para download<sup>1</sup> mostraram uma acurácia de 95,7% contra uma taxa de falsos positivos abaixo de 0,1%.

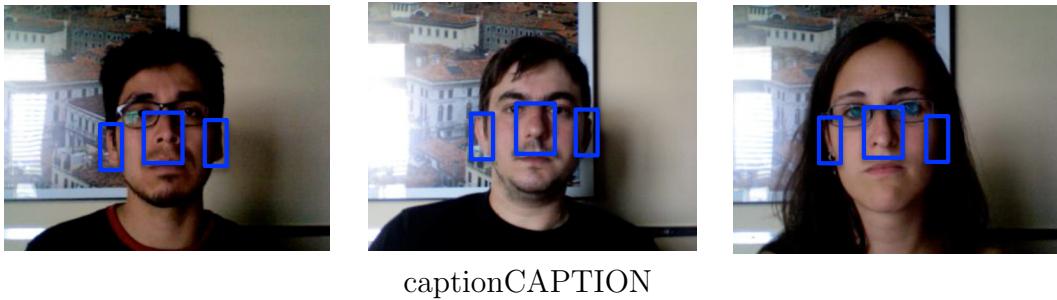
Apoiado na hipótese de que faces vivas apresentam padrões de movimento em certas regiões da face altamente descorrelacionados se comparados ataques (?) desenvolveu uma heurística baseada em fluxo ótico para explorar tal característica. Como referência foram selecionados a região do centro da face e das orelhas com pode ser observado na Figura 2.2.1.

O algoritmo pode ser summarizado como segue:

1. Detectar a face;

---

<sup>1</sup>[http://www.cs.zju.edu.cn/gpan/database/db\\_blink.html](http://www.cs.zju.edu.cn/gpan/database/db_blink.html)



2. Definir região facial está se movendo mais horizontalmente ou mais verticalmente;
3. Delimitar a região do centro da face e das orelhas; verticalmente;
4. Se a cabeça estiver se movendo mais horizontalmente, LIMIARES. TERMINAR
5. Será considerado ataque se a quantidade de movimento percebida na região do centro da face semelhante a quantidade de movimento na região das orelhas.

A performance foi avaliada utilizando uma base de dados construída sobre a base de dados de face XM2VTS. Os acessos reais foram gerados utilizando o subconjunto *Head Rotation Shot* desta base de dados e os ataques foram gerados com fotografias impressas em papel das mesmas imagens utilizadas para os acessos reais e regravados utilizando uma câmera de computador. Com esta base de dados criada um  $EER = 0,5\%$  foi obtido. Esta base de dados não foi disponibilizada publicamente pelos autores de modo que qualquer tentativa de reprodução dos resultados fica impossibilitada.

Ainda sobre a mesma hipótese dos movimentos intra-faciais, (?) também desenvolveu uma heurística utilizando fluxo ótico. Ao contrário de (?), Bao et al não detecta regiões específicas da face, mas sim as divide em quatro partes (horizontalmente e verticalmente) e avalia se ...

Com a seguinte euristica.

### 2.2.2 Características da cena

Contramedidas que buscam características da cena buscam combinar a relação das características faciais com as características de onde a face está inserida.

A contramedida proposta por (?) mede a correlação do movimento da região facial em relação ao seu fundo utilizando como medida de movimento uma simples diferença das intensidades dos pixels em quadros sucessivos. O movimento acumulado entre esta diferença ( $M_D$ ), para um determinado *RoI* e seu respectivo fundo, é calculado usando a seguinte equação:

$$M_D = \frac{1}{S_D} \sum_{(x,y) \in D} |I_t(D) - I_{t-1}(D)| \quad (2.1)$$

em que  $D$  é o *RoI*,  $S_D$  é a área do *RoI* e  $I_t$  é a intensidade de um pixel.

Para introduzir o coeficiente de movimento em um classificador, 5 medidas são computadas em uma janela de  $n$  segundos. As medidas são as seguintes: o mínimo de  $M_D$ , o máximo, a

média, o desvio padrão e a proporção  $R$  composta entre a soma de todos os componentes não-DC e DC (Direct Current) do componente em si tomadas como base o  $N$  pontos transformada de Fourier do sinal gerado por  $M_D$  (ver Equação ref eq: motionR). Estas medidas computadas servem de entrada para rede Neural do tipo MLP (Multi-Layer Perceptron) a fim de detectar ataques.

$$R = \frac{\sum_{i=1}^N |FFT_i|}{|FFT_0|} \quad (2.2)$$

Configurada com uma camada intermediária com 5 neurônios e considerando janelas de tempo com 20 quadros, esta contramedida foi avaliada utilizando o subconjunto de ataques de fotografia da base de dados Replay Attack (IVANA REF) e apresentou  $HTER = 9\%$ . A Figura X apresenta a curva DET (Detection Error Trade-off) da contramedida. Uma análise da performance nos conjuntos de desenvolvimento e teste nesta base de dados para diferentes limiares de operação sugere que a contramedida possui uma boa capacidade de generalização.

### 2.2.3 Discrepância relativa à qualidade da imagem

Contramedidas baseada na discripância relativa à qualidade da imagem apoia-se na hipótese que o processo de amostragem de quantização de uma mídia de ataque (Fotografias, vídeos e etc.) geram padrões de imagem degradados em relação a captura de pessoas reais.

Pela razão de possuir propriedades reflexivas distintas mídias de ataque apresenta padrões distintos de faces reais. Apoiada nesta hipótese (?)<sup>2</sup> explora características de textura utilizando LBP em analizando quadros individuais. A figura X exibe o diagrama de blocos da contramedida proposta.

Neste trabalho, as faces são segmentadas e geométricamente normalizadas para  $64 \times 64$  pixels. Em seguida os parâmetros LBP configurado seguindo a configuração  $LBP_{8,1}^{u2}$  são extraídos e histogramados. Estes histogramas são a entrada do classificador que detecta ataques.

A tabela X apresenta a performance do algoritmo em termos de HTER em três bases de dados de referência; a base de dados Replay Attack, a base de dados CASIA FASD e a base de dados NUAA utilizando SVM e LDA como classificadores.

Tabela X.

Pode-se observar uma performance satisfatória nas três bases de dados entre  $\sim 15\%$  e  $\sim 20\%$ . Contudo uma análise da performance nos conjuntos de desenvolvimento e teste na base de dados NUAA sugere uma baixa capacidade de generalização da contramedida.

Ainda analizando texturas (MINHAS REF) propôs uma contramedida utilizando a dinâmica de uma textura ao longo do tempo utilizando o descriptor  $LBP - TOP$ . Complementar ao descriptor  $LBP$ , o descriptor  $LBP - TOP$  além de observar as componentes espaciais (direção X e Y), ele observa padrões de textura orientados no tempo como pode-se observar na Figura X.

Neste trabalho, as faces são segmentadas e geométricamente normalizadas para  $64 \times 64$  pixels. Em seguida os parâmetros  $LBP - TOP$  seguindo a configuração  $LBP - TOP_{8,8,8,1,1,1}^{u2}$  são extraídos e histogramados. Estes histogramas são a entrada de um classificador do tipo SVM

---

<sup>2</sup><http://pypi.python.org/pypi/antispoofing.lbp>

que detecta ataques. Avaliado utilizando a base de dados Replay Attack, esta contramedida apresentou um  $HTER = 7.60\%$  superando o trabalho apresentado em (IVANA) em  $\sim 50\%$

Apoiados na hipótese que imagens/vídeos utilizadas para ataques concentram mais informação em uma banda específica de frequência, (?) apresenta uma contramedida separando bandas específicas de frequência utilizando filtros de diferença de gaussianas (DoG).

Como pode ser observado no diagrama de blocos da Figura 1, quatro sequências de filtros DoG são aplicados na imagem. Cada filtro possuí uma máscara de  $3 \times 3$  e as configurações das variâncias de cada filtro são:

- $\sigma_1 = 0,5$  e  $\sigma_2 = 1;$
- $\sigma_1 = 1$  e  $\sigma_2 = 1,5;$
- $\sigma_1 = 1,5$  e  $\sigma_2 = 2;$
- $\sigma_1 = 1$  e  $\sigma_2 = 2.$

Após a filtragem as imagens são reescaladas para  $128 \times 128$  e estes dados são a entrada de um classificador SVM. A performance foi avaliada utilizando a base de dados CASIA é um EER de 17% foi alcançado.

Apoiado na hipótese de que as dimensões de uma face utilizando uma mídia para ataque em média será menor do que uma face real e as variações de movimento facial em um ataque são menores do que em uma face real, (REF FOURIER) propôs uma contramedia analizando o espectro Fourier. A expectativa com esta análise é que as imagens utilizadas para ataque contém menos componentes de alta frequência do que imagens de acessos reais. Avaliado utilizando uma base de dados construída pelos próprios autores e não disponibilizada publicamente, obteve-se uma acurácia de 100%

Para detectar padrões de ruído em ataques de spoofing, Pinto et al. desenvolveu uma contramedida analizando vídeos combinando diversos elementos. A Figura X apresenta o diagrama de blocos da contra medida apresentada.

Figura X

Primeiramente os quadros capturados são filtrados utilizando um filtro Gaussiano e uma filtro na Mediana respectivamente. Estas imagens filtradas são subtraídas na imagem original obtendo o ruído residual da imagem. Este ruído residual é analizado no domínio da frequência através da transformada de Fourier 2D. Todos os quadros de um vídeo capturado são combinados utilizando a técnica chamada Rítmico Visual (REF 25 DO PAPER DO HELIO) gerando uma imagem única caracterizando toda aquisição. Com esta etapa de pré-processamento concluída uma descrição utilizando Matriz de Co-ocorrência (GLCM) com 4 orientações são computadas. Uma matriz de co-ocorrência descreve a frequência de ocorrência de níveis de cinza entre pares de pixels. Através dessa matriz 12 medidas são extraídas e são elas: ESCREVER. Estas medidas são a entrada do classificador que detectará os ataques. Os classificadores avaliados foram o PLS e o SVM.

Com uma base de dados combinando o subconjunto de ataques utilizando fotografias da base de dados Replay Attack e uma base de dados criado pelos autores uma performance  $\sim 100\%$  em termos de AUC foi obtida.

## 2.3 Considerações Finais

Cada uma avalia de um jeito e não da pra saber qual é o melhor.



Capítulo **3**

## Metodología



Capítulo **4**

## Conclusões e Perspectivas

**Perspectivas**

**Publicações**

**Submissões**



## Bibliografia

- Jain, A., Bolle, R. & Pankanti, S. (1999). *Biometrics: personal identification in networked society*, kluwer academic publishers.
- Li, S. & Jain, A. (2011). *Handbook of face recognition*, Springer-Verlag New York Inc.
- Maltoni, D., Maio, D., Jain, A. & Prabhakar, S. (2009). *Handbook of fingerprint recognition*, springer.