# Detecção de Fraudes em Leitores de Impressões Digitais sem Contato Utilizando Descritores de Texturas e Redes Neurais Artificiais

Mateus M. E. da Silva, Alexandre Zaghetto e Cauê Zaghetto

***Resumo*— Este artigo apresenta um método capaz de detectar tentativas de fraudes em dispositivos de aquisição de impressões digitais multivista sem toque. Para tanto, um classificador baseado em redes neurais artificiais e descritores de textura ILBP (Padrão Binário Local Aperfeiçoado) e GLCM (Matriz de Co-ocorrência de Níveis de Cinza) foi desenvolvido. O intuito é classificar as imagens de impressões digitais adquiridas como sendo de dedos reais, dedos oclusos ou dedos não reais. Para treinar o classificador proposto, uma base de dados foi criada. A base de dados conta com um conjunto de 840 imagens, sendo 300 imagens de dedos reais, 60 imagens de dedos oclusos e 480 imagens de objetos que não são dedos. O classificador foi testado em 4 diferentes cenários, sendo que cada um utiliza um subconjunto de imagens do banco de dados. O primeiro cenário utiliza apenas as categorias "não dedo" e "dedo real", apresentando uma taxa de acerto de 98,11%. O segundo cenário utiliza as categorias "dedo ocluso" e "dedo real", apresentando uma taxa de acerto de 100%. O terceiro cenário utiliza "não dedo" e "dedo ocluso", apresentando uma taxa de acerto de 98,91%. Por fim, o quarto cenário utiliza todo o banco de dados, apresentando uma taxa de acerto de 93,71%.**

***Palavras-Chave*— Biometria, Antifraude, Impressão digital multivista sem toque.**

***Abstract*— This paper presents a method capable of detecting spoofing attempts against fingerprint touchless multiview devices. For such a task, a classifier based on artificial neural networks and the texture descriptors ILBP (Improved Local Binary Pattern) and GLCM (Gray-Level Co-occurrence Matrix) was developed. It aims to classify the acquired fingerprint images as real fingers, obfuscated fingers or not real fingers. To train the proposed classifier, a database was created. The database comprises a set of 840 images, among them 300 images were acquired from real fingers, 60 images from obfuscated fingers and 480 images from objects that are not fingers. The classifier was tested in 4 different scenarios, each of which using a subset of the database. The first scenario uses only the categories "not real finger" and "real finger", reaching a hit rate of 98.11%. The second scenario uses the categories "obfuscated finger" and "real finger", reaching a hit rate of 100%. The third scenario uses "not real finger" and "obfuscated finger", reaching a hit rate of 98.91%. Finally, the fourth scenario uses all the database, reaching a hit rate of 93.71%.**

***Keywords*— Biometrics, Anti-Spoofing, Multiview touchless fingerprint.**

## I. Introdução

A necessidade crescente de monitorar e restringir o acesso a informações ou a ambientes tem impulsionado grandes esforços na direção do desenvolvimento dos mais variados mecanismos de segurança. Um deles é o reconhecimento biométrico.

Dentre os diversos tipos de biometria [1], destacam-se as impressões digitais. Sistemas biométricos baseados em impressões digitais são, atualmente, os mais utilizados. Se comparadas com outros traços biométricos, as impressões digitais são consideradas as mais populares e largamente utilizadas ao redor do mundo [2].

A evolução de sistemas biométricos pode se dar por meio de melhorias dos algoritmos de extração de características discriminantes, métodos de aquisição de traços biométricos ou melhorias nos dispositivos e tecnologias de captura. No que tange a sistemas biométricos baseados em impressões digitais, podemos citar dispositivos de captura tradicionais que funcionam à base de toque e dispositivos de captura mais modernos baseados em múltiplas aquisições de imagens, que dispensam o posicionamento do dedo sobre uma superfície de contato. Um problema relacionado aos sistemas biométricos em geral é o fato de não realizarem uma correspondência perfeita e, por isso, serem passíveis de falhas e vulnerabilidades. Tais limitações abrem brechas para ataques de agentes mal intencionados que tentam se passar por um usuário válido, o que recebe o nome de *fraude*.

Com o objetivo de oferecer uma alternativa para combater interações maliciosas, este trabalho apresenta um método capaz de distinguir se um usuário está apresentando um dedo real, um dedo ocluso ou um objeto qualquer a um dispositivo de captura de impressões digitais multivista sem contato. A seguir, será apresentado o conceito de biometria.

## II. Biometria

Define-se biometria como sendo a identificação automatizada de um indivíduo a partir de suas características comportamentais e/ou fisiológicas que sejam únicas e cuja imitação por um terceiro seja não trivial [3], [4].

### A. Traços Biométricos

Características comportamentais são aquelas relacionadas ao modo de agir de uma pessoa. Características fisiológicas, por sua vez, são aquelas relacionadas à estrutura física do indivíduo. Exemplos de traços biométricos comportamentais são assinatura, marcas de pressão ao escrever, voz, modo de digitar e modo de andar. Exemplos de traços biométricos fisiológicos são impressões digitais, mãos, face, íris, retina e DNA. Uma determinada característica fisiológica ou comportamental pode

Departamento de Ciência da Computação, Universidade de Brasília, Brasília-DF, Brasil, E-mails: {msilva, azaghetto, zaghettoc}@bitgroup.co.

ser utilizada como biometria se atende aos seguintes requisitos [1]:

1) **Universalidade**: todos os usuários do sistema devem possuir tal característica;
2) **Unicidade**: deve ser diferente para cada indivíduo;
3) **Permanência**: não deve variar com condições externas ou ao longo do tempo;
4) **Coletabilidade**: é necessário que seja possível sua medição;
5) **Aceitabilidade**: é necessário que os usuários estejam dispostos a fornecê-la;
6) **Evasibilidade**: diz respeito à facilidade de se burlar o sistema biométrico.

*Impressão digital* é o nome dado à marca formada pelo conjunto de cristas e sulcos presentes na superfície de cada dedo (falange). Essa marca é única para cada indivíduo e é imutável, ou seja, mesmo com o passar do tempo esse traço permanece o mesmo. Trata-se de um traço biométrico que possui altas unicidade, permanência e performance; médias universalidade, coletabilidade, aceitabilidade e evasibilidade [1]. Por isso, a impressão digital é um dos traços que resulta em sistemas biométricos bastante eficientes, sendo, por isso, amplamente utilizados [4].

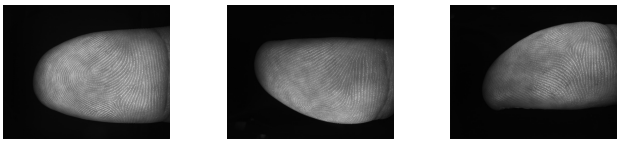
### *B. Métodos de aquisição de impressões digitais*

*1) Aquisição com contato:* O processo de aquisição de impressões digitais com contato consiste em pressionar o dedo sobre a superfície do sensor e, dessa forma, a leitura da impressão digital é realizada. É o tipo de aquisição mais comum nos sistemas atuais [5]. Os dados extraídos neste processo representam a versão 2D da impressão digital. Este processo, entretanto, implica algumas desvantagens, que são inerentes ao seu modo próprio de captura. Devido a elasticidade da pele humana, ao realizar o contato entre o dedo e o sensor, a impressão digital sofre deformações. Dessa forma, as medições obtidas pelo sensor podem não ser suficientemente fieis à impressão digital original e sua replicabilidade pode ser comprometida. Outras fontes de deformações existentes são: doenças de pele, umidade do ar, suor, etc.

*2) Aquisição sem contato:* O processo de aquisição de impressões digitais sem contato consiste em posicionar o dedo em frente a um sensor que não exige contato. Este sensor costuma fazer uso de uma ou mais câmeras de tal forma que as medições da impressão digital sejam obtidas a partir de imagens fotográficas do dedo.

Devido a ausência de contato físico com a superfície do sensor, este método não deforma a impressão digital e é menos suscetível a fatores como sujeira, umidade e demais condições da pele e ambiente. Além disso, não está sujeito a impressões digitais latentes.

A Figura 1 mostra um exemplo de uma impressão digital obtida a partir de um dispositivo sem contato multivista dotado de três câmeras: uma câmera principal, destinada a capturar a parte do dedo que contém o núcleo e o delta, e além desta, outras duas câmeras laterais, espaçadas de $45^{\text{o}}$ no sentido anti-horário e $45^{\text{o}}$ no sentido horário em relação à câmera principal [6]. Para efeito de casamento entre impressões digitais, as três imagens podem ser costuradas para gerar uma única rolada equivalente.



(a) (b) (c)

Fig. 1. Conjunto de imagens capturadas por um sensor de impressões digitais sem contato multivista com três câmeras: (a), (b) e (c) exemplificam a captura realizada pela câmera principal e pelas câmeras espaçadas de $45^{\text{o}}$ no sentido anti-horário e horário, respectivamente.

## III. Ataques a Sistemas Biométricos

O ato de se tentar burlar um sistema biométrico é chamado de *ataque* [7], e pode ser realizado das mais diversas maneiras e em diferentes pontos do sistema. Ataques são classificados em dois tipos: (a) **ataque indireto** - este tipo de ataque consiste em uma ação interna ao sistema. O foco do ataque está em nível de software. Alteração em bancos de dados, alteração de *features* capturadas, desvios no fluxo de execução do sistema, etc. são exemplos de ataques indiretos. Como medidas preventivas, é comum o uso de *firewalls*, anti-vírus e encriptação; e (b) **ataque direto** - neste tipo de ataque, o atacante interage com o sistema biométrico diretamente através do sensor de aquisição. É uma interação puramente física, não havendo qualquer tipo de alteração no sistema em si. Este tipo de ataque é mais comum em ambientes não supervisionados.

Um ataque direto, ainda, pode ser classificado em 3 subcategorias: quando um atacante altera seus traços biométricos para que o sistema não seja capaz de reconhecê-lo, diz-se que houve *oclusão*; quando um atacante se apresenta como um usuário válido e simplesmente fornece seus traços biométricos inalterados, diz-se que houve um *ataque de esforço zero*; quando um atacante forja um traço biométrico, diz-se que houve um *ataque de apresentação* ou fraude.

Sendo assim, ataques diretos, incluindo fraudes, representam um grande risco, pois não exigem que um intruso tenha conhecimentos de programação e suas técnicas são de acesso relativamente fácil.

## IV. Descritores de Textura

Descritores de texturas são algoritmos que extraem características de uma imagem e que podem ser utilizadas para fornecer informações que a diferenciam de outras imagens. A seguir, serão apresentados três descritores de texturas: Padrão Binário Local, Padrão Binário Local Aperfeiçoado e Matriz de Co-ocorrência de Níveis de Cinza.

### *A. Padrão Binário Local e Padrão Binário Local Aperfeiçoado*

O Padrão Binário Local (ou *LBP*, do original em inglês) [8] é um algoritmo computacionalmente simples e invariante na escala de cinza, ou seja, que apresenta resultados suficientemente próximos para uma mesma imagem independente de quantos níveis de cinza forem utilizados.

O LBP consiste em analisar a vizinhança de cada *pixel* de uma região da imagem e gerar um código que a descreve.

Para definir o conjunto de *pixels* considerados como sendo a vizinhança, há diversas técnicas. Aqui, é sempre adotada a vizinhança de 8.

Considere $g_p$ como sendo o conjunto de *pixels* que formam a vizinhança de um *pixel* central $g_c$. Para calcular o descritor de textura local de um *pixel* $g_c$, segue-se a Equação (1).

$$LBP(g_c) = \sum_{p=0}^{7} s(g_p - g_c)2^p \quad , \tag{1}$$

sendo que,

$$s(x) = \begin{cases} 1, & \text{se} \quad x \geq 0 \\ 0, & \text{se} \quad x < 0 \end{cases} \tag{2}$$

Além disso, é necessário garantir a invariância à rotação. A abordagem aqui adotada é bem simples. O vetor de números binários possui seus elementos deslocados de forma circular e, para cada deslocamento, calcula-se o código LBP. O menor código obtido é adotado como o código final daquele *pixel*, conforme a Equação (3).

$$LBP(g_c) = min \left\{ \sum_{p=0}^{7} s(g_{(p+i \bmod 8)} - g_c)2^p | \quad i = 0, 1, \ldots, 7 \right\} \tag{3}$$

Dentre as diversas variações do LBP [9], merece atenção o Padrão Binário Local Aperfeiçoado (ou *ILBP*, do original em inglês). O ILBP possui as mesmas características do LBP, porém aquele é capaz de detectar certos padrões que este não consegue [10].

O ILBP utiliza em seus cálculos a média de toda a vizinhança (incluindo o *pixel* central) no lugar de $g_c$. Ou seja, a Equação (2) substitui a Equação (4),

$$ILBP(g_c) = \sum_{p=0}^{8} s(g_p - Avg(g_c))2^p \quad , \tag{4}$$

onde,

$$Avg(g_c) = \frac{g_0 + g_1 + \ldots + g_7 + g_c}{9}. \tag{5}$$

E, ainda, a Equação (3) é substituída pela Equação (6),

$$ILBP(g_c) = min \left\{ \sum_{p=0}^{8} s(g_{(p+i \bmod 9)} - Avg(g_c))2^p | \quad i = 0, 1, \ldots, 8 \right\}. \tag{6}$$

### B. Matriz de Co-ocorrência de Níveis de Cinza

Outro descritor de texturas é a Matriz de Co-ocorrência de Níveis de Cinza (ou *GLCM*, do original em inglês) [11].

Este método consiste em criar uma matriz $M_{L \times L}$ que tem seu elemento $M(i, j)$ incrementado todas as vezes em que dois *pixels* adjacentes, considerando uma determinada direção, apresentam os valores $i$ e $j$, contidos no intervalo entre 0 e $L - 1$.

| | 1 | 2 | 3 | 4 |
|---|---|---|---|---|
| 1 | 1 | 2 | 4 | 3 |
| 2 | 2 | 1 | 4 | 3 |
| 3 | 2 | 2 | 3 | 1 |
| 4 | 4 | 2 | 1 | 2 |

(a)

| | 1 | 2 | 3 | 4 |
|---|---|---|---|---|
| 1 | 0 | 2 | 0 | 1 |
| 2 | 2 | 1 | 1 | 1 |
| 3 | 1 | 0 | 0 | 0 |
| 4 | 0 | 1 | 2 | 0 |

(b)

Fig. 2. Matrizes envolvidas no GLCM: (a) imagem de entrada em níveis de cinza que variam de 1 à 4 e (b), a GLCM resultante de (a). A direção em análise considera o *pixel* à direita. Por exemplo, a posição $[1, 2]$ da matriz GLCM indica que, na imagem original, há 2 ocorrências de um *pixel* de valor 2 à direita de um *pixel* de valor 1.

Após a montagem da matriz, há 4 métricas que são comumente extraídas. São elas, o contraste, a correlação, a energia e a homogeneidade, definidas nas Equações de 7 à 10, respectivamente.

$$\textit{Contraste} = \sum_{i,j} |i - j|^2 GLCM(i, j) \tag{7}$$

$$\textit{Correlação} = \sum_{i,j} \frac{(i - \mu i)(j - \mu j)GLCM(i, j)}{\sigma_i \sigma_j} \tag{8}$$

$$\textit{Energia} = \sum_{i,j} GLCM(i, j)^2 \tag{9}$$

$$\textit{Homogeneidade} = \sum_{i,j} \frac{GLCM(i, j)}{1 + |i - j|} \tag{10}$$

## V. Método Proposto

O método proposto tem por objetivo avaliar as imagens capturadas por um leitor biométrico multivista e decidir se as aquisições são provenientes de um dedo real, de um dedo ocluso ou de um objeto que não é dedo. A seguir, o método será apresentado passo a passo.

### A. Aquisição

Cada amostra é composta por três imagens capturadas pelas três câmeras do dispositivo biométrico. É importante ressaltar que o algoritmo trata cada uma dessas imagens individualmente.

### B. Pré-processamento

Esta etapa consiste no processamento da imagem de entrada de forma a prepará-la para as etapas seguintes. O resultado desta fase é uma imagem com a área do dedo segmentada e realçada. O pré-processamento é detalhado nos passos descritos a seguir.

1) **Filtro circular de média**: esse filtro suaviza a imagem, removendo parte do ruído.
2) **Binarização**: a imagem é binarizada a partir de um limiar aplicado globalmente.
3) **Operação Morfológica**: essa etapa é realizada sobre a imagem binária e tem por objetivo remover ruídos que a filtragem de média não foi capaz de tratar, bem como outros ruídos que possam ter surgido após a binarização.

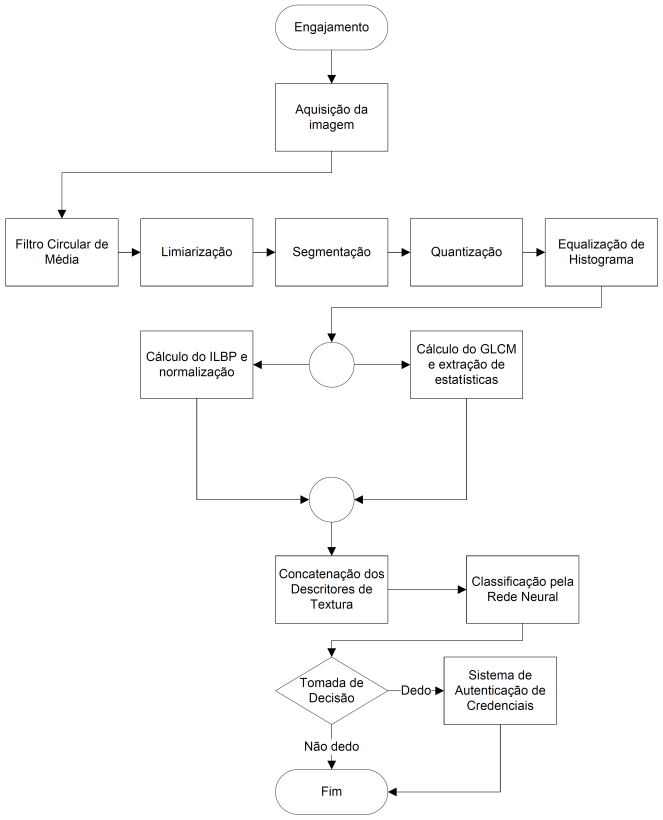
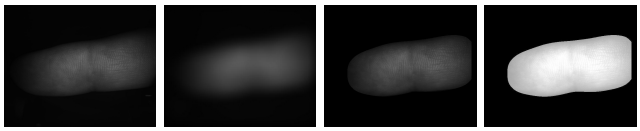



Fig. 3. Fluxograma do algoritmo anti-fraude proposto.



(a) (b) (c) (d)

Fig. 4. Exemplo de (a) imagem de entrada; (b) resultado da aplicação do filtro de suavização; (c) segmentação da região de interesse e (d) aplicação da equalização de histograma à região de interesse.

4) **Segmentação**: a imagem binária é utilizada como máscara e uma região de interesse definida.
5) **Equalização de Histograma**: aplica-se uma equalização de histograma à região de interesse.

A Figura 4 mostra um exemplo de imagem de entrada (a), bem como a imagem gerada após a suavização (b), a região de interesse selecionada pela máscara binária resultante da binarização e do processamento morfológico (c) e a imagem de saída, após a equalização de histograma ter sido aplicada à região de interesse (d).

### C. Extração de Características

O método aqui proposto utiliza uma combinação dos descritores ILBP e GLCM. O cálculo do ILBP é realizado apenas sobre os *pixels* pertencentes à área de interesse. Para o algoritmo do GLCM, é necessário definir quais descritores irão compor o vetor de características $v_c$ definido pela Equação (11). Aqui são utilizados o contraste, a correlação, a energia e a homogeneidade.

$$v_c = [a_1 \dots \ a_{512} \quad b_1 \quad b_2 \quad b_3 \quad b_4] \quad , \tag{11}$$

onde $a_1$ a $a_{512}$ representam os códigos ILBP e os elementos $b_1$, $b_2$, $b_3$ e $b_4$ representam, respectivamente, o contraste, a correlação, a energia e a homogeneidade, caculados a partir da matriz GLCM.

### D. Classificação

A partir dos vetores de características, as amostras adquiridas pelo dispositivo de captura serão classificadas por redes neurais alimentadas em uma de duas classes, de acordo com os cenários descritos a seguir:

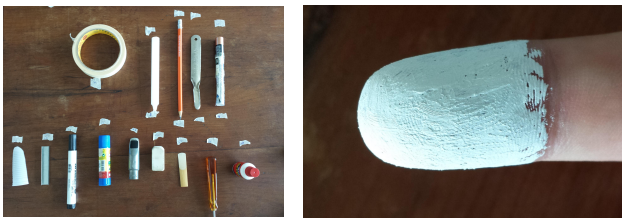
1) Classificação entre "não dedo" e "dedo real", deixando a classe "dedo ocluso" de fora;
2) Classificação entre "dedo ocluso" e "dedo real";
3) Classificação entre "não dedo" e "dedo ocluso";
4) Classificação entre "não dedo" e "dedo real", porém utilizando todo o banco de imagens. Neste caso, a classe "dedo ocluso" é incorporada à classe "não dedo". É o cenário mais próximo ao de uso real.

As redes neurais propostas são tipo *feed-forward* e possuem três camadas: a camada de entrada, a camada escondida e a camada de saída. A primeira camada é composta pelo vetor de características e a camada de saída é composta por um único neurônio. A quantidade de neurônios da camada escondida variou de cenário para cenário, sendo esta quantidade determinada experimentalmente. A quantidade de neurônios que resultou na menor taxa de erros foi adotada. A função de ativação dos neurônios nas camadas escondida e de saída é a tangente hiperbólica. O treinamento é supervisionado e utiliza *Levenberg-Marquardt*.

## VI. Resultados Experimentais

Os experimentos foram realizados a partir de um conjunto composto por $14$ objetos (de alguns objetos, foram utilizadas ambas as extremidades), além de impressões digitais reais e impressões digitais oclusas. Cada objeto foi adquirido 10 vezes e as imagens obtidas foram incorporadas ao banco de imagens. Além disso, foram adquiridas 10 amostras de dois dedos com impressões digitais parcialmente oclusas por tinta branca e fita crepe. A Figura 5 mostra os materiais utilizados. Por fim, foram adquiridas 100 amostras de dedos válidas. É importante ressaltar que cada amostra é definida aqui como um conjunto de três imagens, cada imagem proveniente de uma das três câmeras do dispositivos de aquisição. Em resumo, o banco de imagens utilizado no experimento é composto por 840 imagens: 300 imagens de dedos reais; 60 imagens de dedos oclusos; 480 imagens de não dedos.

Para a avaliação do método proposto, foram utilizados os $4$ cenários já detalhados na Seção V-D. Quanto ao treinamento, o banco de imagens foi dividido de forma homogênea em três conjuntos. O conjunto de treinamento propriamente dito foi utilizado para ajustar as sinapses das redes; o de validação foi utilizado no controle do sobreajuste; e o de teste, para avaliar o desempenho das redes. A seguir serão avaliados os resultados obtidos separadamente para cada um dos cenários.



(a) (b)

Fig. 5. Materiais utilizados para gerar o conjunto de teste: (a) fita adesiva (enrolada em dedo real para causar oclusão), vela (suas duas extremidades foram capturadas), um lápis de escrever (duas extremidades capturadas), um removedor de clip (ambas as extremidades capturadas), uma pilha, um cartão de papel enrolado, um pedaço de copo plástico, um conjunto de clips, uma caneta de quadro branco, uma cola de bastão, uma boquilha de metal de saxofone soprano, uma borracha, uma palheta de bambu de saxofone soprano numeração 2 $1/2$, a parte de baixo de uma chave de fenda e uma embalagem de corretor. (b) é um dedo ocluso com o uso de tinta branca.

Foram utilizadas a taxa de acerto, a *False Acceptance Rate* (FAR) e a *False Reject Rate* (FRR). De maneira sucinta, é possível afirmar que as métricas FAR e FRR dizem respeito aos erros cometidos pelo sistema biométrico enquanto a taxa de acerto indica sucesso na classificação.

Primeiro cenário ("não dedo" e "dedo real"): este cenário foi avaliado com o uso de 160 imagens da classe "não dedo" e 100 imagens da classe "dedo real". Foi empregada uma rede neural com 17 neurônios na camada escondida. A taxa de acerto observada foi de $98,11\%$. Além disso, foram obtidos os valores de FAR (*False Acceptance Rate*) = $0,75\%$ e FRR (*False Reject Rate*) = $1,13\%$.

Segundo cenário ("dedo ocluso" e "dedo real"): este cenário foi avaliado com o uso de 20 imagens da classe "dedo ocluso" e 100 imagens da classe "dedo real". Foi empregada uma rede neural com 20 neurônios na camada escondida. A taxa de acerto observada foi de $100\%$. Foram obtidos os valores de FAR = $0$ e FRR = $0$. Dessa forma, nenhum dedo real foi rejeitado e nenhum dedo ocluso foi aceito.

Terceiro cenário ("não dedo" e "dedo ocluso"): o terceiro cenário foi avaliado com o uso de 160 imagens da classe "não dedo" e 20 imagens da classe "dedo ocluso". Foi empregada uma rede neural com 11 neurônios na camada escondida. A taxa de acerto observada foi de $98,91\%$. Foram obtidos os valores de FAR = $0$ e FRR = $1,09\%$.

Quarto cenário (banco de imagens completo): por fim, o quarto e último cenário utiliza 160 imagens da classe "não dedo", 20 imagens da classe "dedo ocluso" e 100 imagens da classe "dedo real", sendo que esta representa uma combinação dos cenários anteriores. É importante ressaltar que, aqui, o método classifica internamente os dados entre as 3 classes ("não dedo", "dedo ocluso" e "dedo real"), porém a sua tomada de decisão é binária. Caso o dado seja classificado como "dedo ocluso", o comportamento do sistema será o mesmo do caso em que a classificação fosse "não dedo". Dessa forma, este cenário se aproxima ao uso real do sistema.

Nesse caso, foi observada uma taxa de acerto de $93,71\%$. Foi empregada uma rede neural com 12 neurônios na camada escondida. Nesta situação, a taxa de acerto considera 3 categorias. Assim, mesmo que a tomada de decisão seja a mesma para "não dedo" e "dedo ocluso", a classificação errônea em uma dessas duas classes também implica em queda na taxa de acerto. Foram obtidos os valores de FAR = $0,70\%$ e FRR = $1,75\%$. Nesse caso, "não dedo" e "dedo ocluso" são considerados como pertencendo à mesma classe.

TABELA I

RESULTADOS OBTIDOS COM A APLICAÇÃO DO CONJUNTO DE TESTE SOBRE AS REDES NEURAIS JÁ TREINADAS EM CADA CENÁRIO.

| Cenário | FAR | FRR | % de Acerto |
|---|---|---|---|
| "não dedo" e "dedo real" | 0,75% | 1,13% | 98,11% |
| "dedo ocluso" e "dedo real" | 0 % | 0% | 100% |
| "não dedo" e "dedo ocluso" | 0 % | 1,09% | 98,91% |
| "não dedo", "dedo ocluso" e "dedo real" | 0,75% | 1,13% | 98,11% |

A Tabela I resume os resultados obtidos.

## VII. CONCLUSÃO

Este trabalho propôs um método capaz de detectar fraudes no contexto de leitores biométricos multivista de impressões digitais sem contato que utiliza dois descritores de textura: Padrão Binário Local Aperfeiçoado (ILBP) e Matriz de Co-ocorrência de Níveis de Cinza (GLCM). O algoritmo encontra maior aplicabilidade em ambientes não supervisionados e seu enfoque é a distinção entre a apresentação de credenciais que não são dedos, que são dedos oclusos e dedos reais. Ao analisar o cenário mais próximo ao seu uso real, apenas 2,45% das avaliações foram errôneas (FAR = 0,70% e FRR = 1,75%). Além disso, obteve resultados ainda melhores em sub-cenários, apresentando sempre taxas de acerto acima de 98%.

Ainda é necessária, entretanto, a realização de experimentos com bases de imagens maiores e mais abrangentes, além de estudos voltados ao seu comportamento contra ataques de apresentação.

## REFERÊNCIAS


[1] Anil K. Jain, Arun Ross, e Salil Prabhakar. *An introduction to biometric recognition*. IEEE Transactions on Circuits and Systems for Video Technology, 14(1), Janeiro 2004.

[2] Arun Ross, e Anil K. Jain. *Human recognition using biometrics: an overview*. Annales Des Télécommunications. Vol. 62. No. 1-2. Springer-Verlag, 2007.

[3] Benjamin Miller. *Vital signs of identity*. IEEE Spectrum, 1994.

[4] Anil Jain, Brendan Klare, e Arun Ross. *Guidelines for best practices in biometrics research*. 8th IAPR International Conference on Biometrics, 2015.

[5] Ruggero Donida Labati, Angelo Genovese, Vincenzo Piuri, e Fabio Scotti. *Touchless fingerprint biometrics: a survey on 2d and 3d technologies*. Journal of Internet Technology, 15(3):325-332, Maio 2014. 1607-9264.

[6] Caue Zaghetto, et al. *Touchless multiview fingerprint quality assessment: rotational bad-positioning detection using Artificial Neural Networks*. Biometrics (ICB), 2015 International Conference on. IEEE, 2015.

[7] Nalini K. Ratha, Jonathan H. Connell, e Ruud M. Bolle. *Audio- and Video-Based Biometric Person Authentication*. Springer Berlin Heidelberg, 2001.

[8] Timo Ojala, Matti Pietikäinen, e Topi Mäenpää. *Multiresolution gray-scale and rotation invariant texture classification with local binary patterns*. Pattern Analysis and Machine Intelligence, IEEE Transactions on 24.7 (2002): 971-987.

[9] Sébastien Marcel, Yann Rodriguez, e Guillaume Heusch. *On the recent use of local binary patterns for face authentication*. International Journal of Image and Video Processing, Special Issue on Facial Image Processing, 2007.

[10] Hongliang Jin, Qingshan Liu, Hanqing Lu, e Xiaofeng Tong. *Face detection using improved lbp under bayesian framework*. Multi-Agent Security and Survivability, IEEE First Symposium on, 2004.

[11] Vishal S.Thakare, Nitin N. Patil, e Jayshri S. Sonawane. *Survey on image texture classification techniques*. International Journal of Advancements in Technology, 2013.