Detecção de Ataque de Apresentação em Imagens de Íris utilizando Descritores de Zernike

Geórgio Sá Colares[1], Igor Mahall M. De Sousa[1], Luciana R. Costa, Lucas G. M. de Castro[1], Myke D. M. Valadão[1], José Elislande B. S. Linhares[1,3], Rebeca S. Campos[1], Ana Júlia P. Corrêa[1], Gabriel M. Araújo[2], Frederico S. Pinagé[1], Celso B. Carvalho[1], Waldir S. S. Júnior[1]
[1]Universidade Federal do Amazonas e Centro de P&D em Elet. e Tec. Inf. (UFAM/CETELI), AM-Brasil
[2]Centro Federal de Educação Tecnológica Celso Suckow da Fonseca (Cefet/RJ), RJ-Brasil
[3]Instituto Federal de Educação, Ciência e Tecnologia do Amazonas (IFAM), AM-Brasil
Emails: {georgio.colares, igormahall, lucianarolim08, rebecacampos6104}@gmail.com, gabriel.araujo@cefet-rj.br, breno.linhares@ifam.edu.br, {lucas.muniz, mykedouglas, julia.correa, fredericopinage, waldirjr, ccarvalho_}@ufam.edu.br

***Resumo*— Neste artigo, propõe-se um *framework* simplificado de detecção de *spoofing* de imagens de íris sintéticas aplicadas na autenticação de segurança de sistemas. Os momentos de Zernike foram aplicados devido às suas propriedades, p.ex. a invariância à rotação. Investigamos o desempenho dos descritores de Zernike com três classificadores, variando seus respectivos parâmetros. Os experimentos resultaram que a magnitude dos momentos da representação em escala de cinza fornece bons resultados gerais de reconhecimento em uma variedade de classificadores. O desempenho da rede MLP, CNN e ResNet com momentos de Zernike obteve, respectivamente,** $79,0\%$**,** $90,0\%$ **e** $93,0\%$ **de acurácia.**

***Palavras-Chave*— Íris sintética, Falsificação, Momentos de Zernike, MLP, CNN, ResNet.**

***Abstract*— In this paper, we propose a simplified framework for spoofing detection of synthetic iris images applied in security authentication systems. Zernike moments were applied due to some of their properties, such as rotation invariance. We investigated the performance of Zernike descriptors on three classifiers, varying their respective parameters. The experiments resulted in the magnitude of the moments of the grayscale representation providing good overall recognition results on a variety of classifiers. The performance of the MLP, CNN, and ResNet network with Zernike moments obtained, respectively, the accuracy of** 79.0%**,** 90.0%**, and** 93.0%**.**

***Keywords*— Synthetic iris, Spoofing, Zernike moments, MLP, CNN, ResNet.**

I. Introdução

Sistemas biométricos têm desempenhado papel fundamental em aplicações de autenticação e controle de acesso [1]. Dentre as diversas modalidades biométricas, o reconhecimento de íris apresenta vantagens consideráveis, como alta estabilidade ao longo do tempo e robustez à ocorrência de correspondência de ambiguidades, ou seja, não deve gerar confusão de entradas de usuários distintos no sistema como se fossem iguais, devido à complexidade e singularidade dos padrões da íris [1], [2]. No entanto, tais sistemas não estão imunes a ataques de apresentação (*presentation attack detection* – PAD), os quais utilizam artifícios como imagens impressas, lentes texturizadas ou íris sintéticas, com o objetivo de enganar a autenticação [2], [3]. Neste contexto, há uma demanda crescente por mecanismos que identifiquem tentativas de spoofing e reforcem a segurança desses sistemas. Com isso, propõe-se um sistema de detecção de íris falsas utilizando descritores baseados em Momentos de Zernike, aplicados localmente a janelas da imagem. Essa abordagem permite capturar características geométricas relevantes com propriedades de invariância à rotação e robustez a ruídos [4], [5]. Para a tarefa de classificação, são avaliadas três arquiteturas de redes neurais artificiais: *multilayer perceptron* (MLP), *convolutional neural network* (CNN) e *residual neural network* (ResNet), técnicas que têm se mostrado eficazes em problemas de visão computacional e aprendizado de máquina [6], [7]. A metodologia é testada em bases públicas que contêm imagens reais (CASIA-Iris-Thousand e IIT Delhi Iris database) e imagens sintéticas de íris (CASIA-Iris-Syn e IITD Iris CSD), gerando um ambiente de avaliação realista. Os resultados indicam que a combinação de descritores de forma com classificadores neurais complexos pode ser eficaz na detecção de spoofing em imagens de íris, contribuindo para o desenvolvimento de sistemas biométricos mais seguros e robustos.

II. Trabalho Relacionados

No estudo conduzido por Khade *et al.* [8], apresenta-se uma abordagem de detecção de ataques *spoofing* em imagem de íris, utilizando os coeficientes extraídos das transformadas cossenos discretas [9], transformada Haar [10] e transformada híbrida [9]. Os autores utilizam seis bases de dados e nove tipos de classes de ataques *spoofing* para íris. Como modelos de treinamento de aprendizado de máquina, empregam-se os classificadores de máquina de vetor de suporte (SVM), *naive Bayes*, *random forest* (RF) e árvore de decisão (algoritmo J48) [11], assim como a combinação desses métodos, além do *multilayer perceptron* (MLP) para detectar a autenticidade da íris [11]. Em termos de resultados, há nove variantes de ataques *spoofing* e sete classificadores, todos aplicados a cada uma das transformadas. A transformada híbrida para imagem de íris com algoritmo RF obteve o melhor resultado de detecção com $99,95\%$ de precisão.

No trabalho proposto por M. Gupta e S. Gupta [12], utilizam os momentos de Zernike como descritores de forma e classificadores para determinar tumores cerebrais. Os descritores

são extraídos de imagens segmentadas do volume tumoral. A classificação é feita utilizando-se SVM, *naive Bayes*, e *bagged trees* [11], empregando validação cruzada com *k-fold* igual a 5. Um preditor decide o grau do glioma à partir das características classificadas. Como métrica, utilizam-se acurácia, sensibilidade e especificidade. Em termos de resultados, o método obteve precisão de 88% para SVM, 90% para *naive Bayes* e 88% para *bagged trees* na classificação de gliomas de baixo e alto grau.

Na pesquisa desenvolvida por Gautam, Raj e Mukhopadhyay [13], aborda-se um método denominado *deep supervised class encoding* (DSCE) para casos de detecção de três tipos de ataques de apresentação, chamados de PAD [14], para imagens de íris impressas, com lentes de contato e sintéticas. O DSCE é um *autoencoder* baseado em método de aprendizado supervisionado para classificação de recursos. O objetivo do DSCE é minimizar os erros de reconstrução e classificação simultaneamente durante a fase de treinamento. DSCE é empregado para projetar uma estrutura iris-PAD denominada *DeepI*, para perceber o acesso falso a uma íris. Resultados experimentais em diferentes bancos de dados mostram que o *DeepI* baseado em DSCE supera os atuais métodos de detecção de ataques *spoofing* com íris.

No trabalho publicado por Agarwal *et al.* [15], propõe-se um algoritmo para ataque *spoofing* unificado baseado em CNN, utilizando a fusão de uma variedade de imagens de íris e pontuações de classificação calculadas sobre essas informações. O sistema utiliza um conjunto de informações para aumentar a confiabilidade no classificador. No tratamento das variações, ocorre uma avaliação extensiva do algoritmo proposto em diferentes cenários (controlados e não controlados). Nesse trabalho, foram utilizados ataques *spoofing* de íris de lentes de contato 3D. Para a avaliação, utilizam-se os protocolos experimentais, que refletem configurações não controladas para ataque de apresentação de íris de lentes de contato 3D, onde as imagens pertencem tanto a condições controladas quanto adversas de imagem. Os experimentos apresentaram taxas de acerto de $94,7\%$ para teste com 50% de imagens não controladas e $98,2\%$ para testes com 100% das imagens controladas.

Na proposta de Kaur [16], apresenta-se um sistema robusto de detecção de falsificação de rosto, utilizando recursos com invariância local. As bases de dados utilizadas foram CASIA-FASD, Replay-Attack e Oulu-NPU. Recursos e artefatos foram extraídos por momentos de Zernike invariantes à rotação, transformadas harmônicas polares [17], momentos ortogonais discretos como Krawtchouk, Tchebichef e Dual Hahn [18]–[20]. As estruturas do sistema são todas as combinações de extratores em série com os classificadores. Invariância à rotação, escala e translação são recursos locais que viabilizam detectar pequenas variações em uma imagem genuína ou falsa. O método proposto apresenta desempenho superior em comparação às técnicas disponíveis no levantamento da literatura, onde a transformada polar combinada com momento de Zernike obteve, para as bases de dados CASIA-FASD, Replay-Attack e Oulu-NPU, a precisão de $99,98\%$; $99,98\%$ e $99,95\%$, respectivamente.

III. METODOLOGIA

A. Introdução

Nesta seção, apresenta-se a metodologia proposta para sistemas de *presentation attack detection* utilizando imagens de íris em um sistema de acesso biométrico. Para tal, foi desenvolvido um *framework* simplificado de um descritor baseado em momentos de Zernike para a extração de formas circulares e não lineares, combinado a três tipos de classificadores. O artigo de N. Kohli, D. Yadav, M. Vatsa, et. al., [21] foi utilizado como referência ao *framework*. Este artigo apresenta um sistema com o propósito de detectar a diferença entre imagens de íris reais e imagens de íris sintéticas. O *framework* descritor deste artigo parte da metodologia de extrair características locais de momentos de Zernike em virtude da divisão da imagem em janelas não sobrepostas para obter informações de formas circulares e não lineares. Estas características extraídas são termos de cada ordem de momento estatístico, p.ex. centroide, média, mediana, esperança, variância, covariância, assimetria, curtose, entre outros.

No sistema de referência, são extraídas características locais de informações de contornos e curvas, combinando o janelamento com momentos de Zernike de multi-ordem, e acrescenta-se a técnica LBPV para extrair informações de textura das imagens. Na técnica LBPV ou *local binary pattern variance*, calcula-se os valores em janelas da imagem com base em uma função binária a partir do pixel central da janela no sentido horário, e estrutura-se em um histograma. No sistema de referência, o LBPV é usado para extrair *features* ou características de contraste da imagem. Ambas as extrações são complementares em seu objetivo, e com a fusão, formam um vetor de características distintas. Este vetor compõe a entrada de uma rede neural *Multilayer perceptron* simples, a qual deve classificar se a imagem é real ou *spoofing*.

B. Framework descritor de Zernike

Para padronização da base de dados de entrada, é aplicado o redimensionamento da imagem de íris. Foi aplicada normalização em escala e em translação para padronizar as propriedades globais da imagem de íris. A normalização em translação foi realizada calculando-se o centroide da função densidade de probabilidade da imagem usando a equação de momentos de imagem, conforme a equação 1 e 2. Com isso, as resultantes dos momentos da imagem têm propriedades globais invariantes à translação.

$$Centroide\,(X_c, Y_c) = \left(\frac{\mu_{1,0}}{\mu_{0,0}}, \frac{\mu_{0,1}}{\mu_{0,0}}\right) \tag{1}$$

Sendo o momento $\mu_{i,j}(x, y)$, calcula-se a seguir:

$$\mu_{i,j}(x, y) = \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} I(x, y) x^i y^i \tag{2}$$

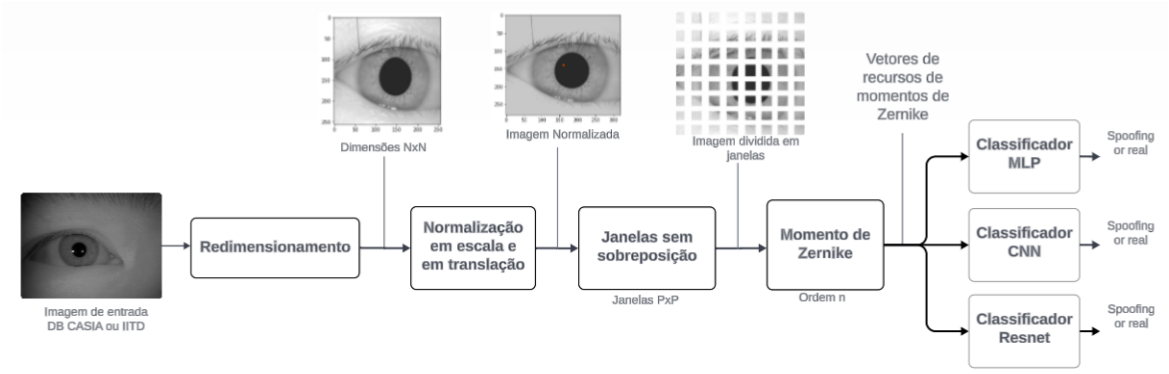

Fig. 1. Sistema de descritores de Zernike com classificadores para a detecção de ataque de apresentação utilizando *spoofing* de imagens de íris sintéticas.

onde $i, j = \{0, 1, 2, ..., N-1\}$, N é o número de *pixels* nas dimensões da imagem $N \times N$, e $\mu_{i,j}(x, y)$ é a $(i + j)$-ésima ordem do momento da função momento da imagem, e $I(x, y)$ é a função base da imagem referente à intensidade nas coordenadas x e y, ou seja, é a imagem a ser processada.

Na imagem normalizada, é aplicada a técnica de janelamento sem sobreposição, ou seja, a imagem é dividida em janelas quadradas sem bordas sobrepostas. Este conjunto de janelas é a entrada para o descritor de momento de Zernike. O cálculo de momento de Zernike é restrito à área de um disco unitário limitado às bordas da imagem, conforme a equação 3. O resultado é um vetor de magnitudes de momentos de Zernike. Os momentos de Zernike bidimensionais são, neste artigo, definidos pela variável ZM, n a ordem do momento, m o número de repetições das ordens, N e M são os números de *pixels* em cada eixo (x, y), $f(x, y)$ é um segmento de imagem delimitado pelo disco unitário, a variável ρ é o tamanho do vetor de origem para (x, y) no sentido anti-horário e θ é o ângulo entre o vetor ρ e o eixo x no sentido anti-horário. O $R_{n,m}$ é a parte real do polinômio de Zernike $Z_{n,m}$, sendo ZM expresso por:

$$ZM_{n,m} = \frac{(n+1)}{\pi} \sum_{x=1}^{N} \sum_{y=1}^{M} f(x, y) Z^*_{n,m}(\rho, \theta) \tag{3}$$

A ordem n tem valores inteiros positivos ou zero, enquanto m assume valores inteiros positivos e negativos definidos por $n - |m|$: par, e $|m| \leq n$. $ZM_{n,m}$ é limitado aos valores dentro de $x^2 + y^2 \leq 1$, sendo a resultante a magnitude de momentos complexos ortogonais à imagem, e são capturadas as informações locais sobre a janela. O polinômio de Zernike $Z_{n,m}$ é definido na equação 4.

$$Z_{n,m}(\rho, \theta) = R_{n,m} \exp(jm\theta) \tag{4}$$

Sendo a parte real do polinômio de Zernike, é definida como $R_{n,m}(p)$ na equação 5 :

$$R_{n,m}(p) = \sum_{s=0}^{(n-|m|)/2} (-1)^s \frac{(n-s)!}{s!\,(a-s)!\,(b-s))!} p^{(n-2s)} \tag{5}$$

$$\text{Sendo } a = \frac{(n+|m|)}{2} \text{ e } b = \frac{(n-|m|)}{2}. \tag{6}$$

Como classificadores, foram utilizadas as redes neurais *Multilayer Perceptron*, *Convolutional Neural Network* e *Residual Neural Network*. Em cada entrada da rede neural, o vetor é adequado a um formato que atenda às necessidades de processamento da rede neural em execução. A saída do classificador é o resultado da rede neural, determinando se a imagem de íris da entrada do sistema é sintética ou real. O sistema proposto é mostrado na Figura 1. Momento de Zernike agrega como vantagem a possibilidade de processar a imagem sem necessidade de transformá-las em formatos que distorcem a imagem de íris antes de aplicar o método de detecção. As características de formas circulares são bastante recorrentes em imagens de íris. Os momentos de Zernike processam a imagem radialmente, independente do tipo de coordenada adotada. As propriedades de invariância à escala, à translação e à rotação são também aplicáveis ao *framework* deste artigo, garantindo um nível de robustez ao sistema.

IV. Discussões e resultados

Nesta subseção, apresenta-se o procedimento experimental, de acordo com a metodologia descrita na Seção III-B, e no diagrama geral de blocos do *framework* proposto na Figura 1. No pré-processamento, definiram-se as imagens da base de dados para treinamento, validação e teste. As bases de dados CASIA-Iris-Thousand junto com CASIA-Iris-Syn, e a IIT Delhi Iris database junto com IITD Iris CSD, são utilizadas pelo pré-processamento, formando de cada uma destas duas bases de dados com 2000 e 6000 imagens selecionadas aleatoriamente. No bloco de redimensionamento, todas as imagens selecionadas na entrada serão convertidas para o formato de dimensões 256×256. Na normalização em escala, aplicou-se a normalização Min-Max em escala com valores no intervalo de 0 à 1. A normalização em translação é calculada com o centróide de momentos de imagens.

Na janela sem sobreposição, a imagem é dividida janelas utilizando tamanhos de 4×4, 8×8 ou 16×16 , exemplificadas na Figura 2. Para o bloco de momento de Zernike, a área de cálculo é delimitada ao disco com raio

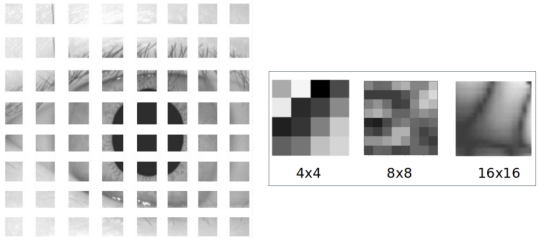

Fig. 2. Exemplo de janelamento da imagem sem sobreposição e diferentes tamanhos de janela da imagem.

unitário, conforme descrito na seção III-B. Cada execução do sistema proposto terá uma máxima ordem de polinômio de Zernike, que varia no conjunto de valores de $n = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$. O objetivo é explorar os níveis de extração de características que variam com a ordem do polinômio de Zernike. Os classificadores MLP, CNN e ResNet utilizaram k-*fold* igual à 4 e 10. A quantidade de neurônios na camada de entrada, oculta e de saída foi projetada de acordo com o arranjo das informações prévias da entrada, do tipo de rede e dos acordos com os valores e parâmetros obtidos no treinamento. As métricas utilizadas para avaliação foram acurácia, precisão, *recall* ou revocação, F1-*score*, e aplicou-se a matriz de confusão para entender os erros e acertos do *framework* proposto.

TABELA I

COMPARAÇÃO DE ACURÁCIAS PARA O DESCRITOR DE ZERNIKE DE **ORDEM 12** E **BASES DE DADOS CASIA** PARA CADA UM DOS CLASSIFICADORES

N^o **imagens**	**Janela**	**Rede**	**Acurácia**	**Precisão**	**Recall**	**F1-Score**
2000	**4x4**	**MLP**	0,77	0,53	0,81	0,64
	8x8		0,82	0,59	0,86	0,70
	16x16		0,72	0,50	0,88	0,63
6000	**4x4**		0,87	0,71	0,81	0,76
	8x8		0,91	0,77	0,89	0,82
	16x16		0,91	0,80	0,87	0,83
2000	**4x4**	**CNN**	0,87	0,67	0,92	0,78
	8x8		0,91	0,76	0,92	0,83
	16x16		0,89	0,72	0,92	0,81
6000	**4x4**		0,95	0,86	0,95	0,90
	8x8		0,93	0,82	0,93	0,87
	16x16		0,94	0,84	0,94	0,88
2000	**4x4**	**Resnet**	0,91	0,77	0,92	0,84
	8x8		0,92	0,78	0,92	0,85
	16x16		0,91	0,78	0,90	0,84
6000	**4x4**		0,91	0,81	0,82	0,81
	8x8		0,95	0,88	0,94	0,90
	16x16		0,93	0,84	0,89	0,87

As Tabelas I e II apresentam a comparação dos melhores resultados de acurácia do *framework* proposto em seus três classificadores, com suas bases de dados respectivamente. Na Figura 3, a comparação direta entre os resultados do sistema proposto usando classificador MLP, CNN e ResNet. O desempenho dos momentos de Zernike com MLP obteve performance inferior, especialmente em cenários de baixa ordem do polinômio, sendo o valor mais próximo para ordem de n igual à 12 com acurácia de 79% para precisão 55%. O momento de Zernike com classificadores CNN e ResNet obteve 90% e 93% de acurácia, para respectivamente 79%

TABELA II

COMPARAÇÃO DE ACURÁCIAS PARA O DESCRITOR DE ZERNIKE DE **ORDEM 12** E **BASES DE DADOS IITD** PARA CADA UM DOS CLASSIFICADORES

N^o **imagens**	**Janela**	**Classi-ficador**	**Acurácia**	**Precisão**	**Recall**	**F1-Score**
2000	**4x4**	**MLP**	0,51	0,32	0,84	0,46
	8x8		0,56	0,35	0,86	0,50
	16x16		0,62	0,40	0,99	0,58
6000	**4x4**		0,74	0,48	0,54	0,51
	8x8		0,68	0,38	0,48	0,43
	16x16		0,79	0,55	0,87	0,68
2000	**4x4**	**CNN**	0,63	0,38	0,75	0,51
	8x8		0,78	0,53	0,86	0,66
	16x16		0,59	0,36	0,78	0,49
6000	**4x4**		0,95	0,85	0,95	0,90
	8x8		0,78	0,56	0,64	0,60
	16x16		0,90	0,79	0,81	0,80
2000	**4x4**	**Resnet**	0,89	0,74	0,89	0,81
	8x8		0,82	0,61	0,76	0,68
	16x16		0,80	0,58	0,78	0,66
6000	**4x4**		0,86	0,68	0,80	0,74
	8x8		0,81	0,60	0,75	0,66
	16x16		0,93	0,84	0,89	0,86

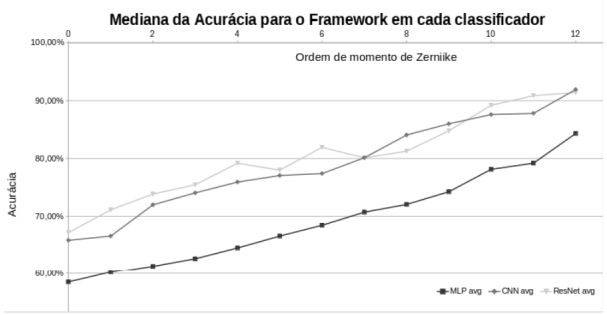

Fig. 3. Acurácias com o crescimento da ordem do *framework* de Descritores de Zernike em cada classificador.

e 84% de precisão. Observou-se que pra baixas ordens de Momento de Zernike (0 à 5), o resultado depende muito da imagem ter detalhes o suficiente para distinguir as formas e contornos, pois não extrai tantas características adequadamente da imagem. Para casos de ordem de momento de Zernike iguais à 6 à 9, o modelo tem resultados mais assertivos. Os melhores resultados foram para ordens maiores, de 9 à 12, onde consegue-se extrair mais características. Outra influência foi o tamanho da janela, que tem mais características de formas circulares distinguíveis e semelhanças de *pixels* na vizinhança.

Para uma comparação entre os métodos empregando o *framework* com MLP e o sistema de referência, foi utilizado o algoritmo do sistema proposto baseando-se no sistema de referência. Utilizou-se somente a base de dados IITD, a ordem de momento de Zernike n igual à 10, conforme descrito em [21], mas removendo a técnica do LBPV. Comparar o sistema proposto com o sistema de referência sem LBPV é mais justificável para realizar esta paridade. O resultado é apresentado na Tabela III, onde as diferenças entre o sistema de referência e os outros dois sistemas simulados propostos podem ser devido a os algoritmos terem otimizações distintas, além de usarem quantidades muito diferentes de termos dos momentos de Zernike. Outro motivo da diferença

pode ser possíveis distinções nas bases de dados. O sistema proposto tem diferente informação qualitativa sobre textura. Em contraponto, o sistema proposto extrai mais informações quantitativas estatísticas da imagem, com a utilização de muito mais termos de momentos de Zernike, consequentemente extrai mais características de formas da imagem.

TABELA III

COMPARAÇÃO ENTRE OS TRÊS SISTEMAS IMPLEMENTADOS UTILIZANDO MLP E BASE DE DADOS IITD DE 6000 IMAGENS, E COM ORDEM DO MOMENTO DE ZERNIKE IGUAL À 10.

Autor	Algoritmo de Classificação	Acurácia
Kohli, N., Yadav, D., Vatsa, M., et al.	**Sistema de Referência**	82,2%
Colares, G.S.	**Framework Proposto**	79,0%
	Sistema sem LBPV	80,0%

V. CONCLUSÕES

Neste artigo, investiga-se a influência da adição de blocos de pré-processamento a um sistema desenvolvido para executar a tarefa de detecção de imagens de íris em ataques de *spoofing* do tipo íris sintética. Entre as rotinas de pré-processamento realizadas, estão o redimensionamento da imagem, a normalização e seleção de parâmetros e variáveis que, quando combinados com classificadores (i.e., MLP, CNN e ResNet) de formas circulares ou não alinhadas, influenciam na melhoria de momentos de Zernike. Em relação às duas primeiras rotinas, verificou-se que não se mostraram primordiais no resultado final.

Para a última rotina, em ambas as bases de dados utilizadas, o sistema proposto de momentos de Zernike com ResNet é o *framework* com o melhor desempenho em termos de acurácia e precisão, obtendo, respectivamente, 93% e 84%, sugerindo que pode lidar melhor com as características de formas circulares. No entanto, com a base de dados IITD, verificou-se a presença de resultados com valores inferiores nos *frameworks*, tendo em vista o cenário desafiador para a detecção, por apresentar oclusão, mas com valores ainda próximos ao obtido no *framework* sem este tipo de imagem.

Portanto, conclui-se que a viabilização de uma abordagem com classificadores mais dedicados ao processamento de características de formas circulares não lineares se mostrou mais assertiva. Foi o caso em que utilizou-se CNN e ResNet na classificação, obtendo, respectivamente, valores de 90% e 93% de acurácia. No sentido de oferecer continuidade ao estudo de caso descrito nesta pesquisa, elencam-se, a seguir, algumas propostas para trabalhos futuros: i) explorar o uso de bases de dados com características específicas de imagens geométricas para validar a robustez do sistema em cenários complexos; ii) implementar a técnica de GAN ao classificador para avaliar a entrada de características das imagens de íris reais e de imagens geradas como ataque *spoofing* de íris sintética pela rede generativa; e iii) implementar, via APIs com uma gama de redes neurais artificiais otimizadas, um estudo de valores ótimos de classificadores para o sistema proposto.

AGRADECIMENTOS

Parte dos resultados desta pesquisa foram subsidiados por ENVISION Indústria de Produtos Eletrônicos LTDA nos termos da Lei Brasileira Federal No. 8.387/91 (SUFRAMA).

REFERÊNCIAS

[1] J. Daugman, "How iris recognition works," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 14, no. 1, pp. 21–30, Jan. 2004.

[2] "ISO/IEC 30107-1:2023, Information technology – Biometric presentation attack detection – Part 1: Framework," 2023, international Organization for Standardization.

[3] S. K. Khade, S. Gite, and S. D. Thepade, "Iris spoofing detection using hybrid transforms and classification techniques," in *IEEE Proc. Int. Conf. on Communication and Signal Processing (ICCSP)*, 2020.

[4] R. Mukundan and K. R. Ramakrishnan, *Moment Functions in Image Analysis*. Singapore: World Scientific, 1998.

[5] M. Kaur and S. Gupta, "Brain tumor detection using zernike moments and machine learning classifiers," *Int. Journal of Computer Applications*, vol. 175, no. 7, pp. 17–23, 2020.

[6] Y. LeCun, Y. Bengio, and G. Hinton, "Deep learning," *Nature*, vol. 521, no. 7553, pp. 436–444, 2015.

[7] K. He, X. Zhang, S. Ren, and J. Sun, "Deep residual learning for image recognition," in *IEEE Proc. Int. Conf. on Computer Vision and Pattern Recognition (CVPR)*, 2016, pp. 770–778.

[8] S. Khade and et. al., "Detection of iris presentation attacks using hybridization of discrete cosine transform and haar transform with machine learning classifiers and ensembles," *IEEE Access*, vol. 9, pp. 169 231–169 249, 2021.

[9] K. R. Rao and P. Yip, *Discrete cosine transform: algorithms, advantages, applications*. Academic press, 2014.

[10] J. Astola and L. Yaroslavsky, *Advances in signal transforms: theory and applications*. Hindawi Publishing Corporation, 2007, vol. 7.

[11] A. Charu C, *Neural networks and deep learning: a textbook*. Springer, 2018.

[12] M. Gupta and S. Gupta, "Classification of gliomas using efficient zernike moments based shape descriptors extracted from segmented mr images," in *IEEE Proc. Int. Conf. on Soft Computing and Signal Processing*. Springer, 2021, pp. 445–454.

[13] G. Gautam, A. Raj, and S. Mukhopadhyay, "Deep supervised class encoding for iris presentation attack detection," *Digital Signal Processing*, vol. 121, p. 103329, 2022.

[14] A. Husseis and et. al., "A survey in presentation attack and presentation attack detection," in *Proc. Int. Conf. on Security Technology (ICCST)*. IEEE, 2019, pp. 1–13.

[15] A. Agarwal, A. Noore, M. Vatsa, and R. Singh, "Generalized contact lens iris presentation attack detection," *IEEE Transactions on Biometrics, Behavior, and Identity Science*, vol. 4, no. 3, pp. 373–385, 2022.

[16] B. Kaur, "Face spoofing detection system using local invariant feature set," in *IEEE Proc. Int. Conf. Delhi Section Flagship (DELCON)*. IEEE, 2023, pp. 1–5.

[17] A. Averbuch and et. al., "Fast and accurate polar fourier transform," *Applied and computational harmonic analysis*, vol. 21, no. 2, pp. 145–167, 2006.

[18] R. Mukundan, S. H. Ong, and P. A. Lee, "Image analysis by tchebichef moments," *IEEE Transactions on image Processing*, vol. 10, no. 9, pp. 1357–1364, 2001.

[19] P.-T. Yap, R. Paramesran, and S.-H. Ong, "Image analysis by krawtchouk moments," *IEEE Transactions on image processing*, vol. 12, no. 11, pp. 1367–1377, 2003.

[20] H. Zhu, H. Shu, J. Zhou, L. Luo, and J.-L. Coatrieux, "Image analysis by discrete orthogonal dual hahn moments," *Pattern Recognition Letters*, vol. 28, no. 13, pp. 1688–1704, 2007.

[21] N. Kohli, D. Yadav, M. Vatsa, R. Singh, and A. Noore, "Detecting medley of iris spoofing attacks using desist," in *2016 IEEE 8th International Conference on Biometrics Theory, Applications and Systems (BTAS)*, 2016, pp. 1–6.