BIOMETRIA PERIOCULAR EM *SMARTPHONE* USANDO QUANTIZAÇÃO DE FASE LOCAL

William Bin Falinski (Fundação Araucária), Alceu de Souza Britto Jr. (Orientador), e-mail: alceubritto@gmail.com.

Universidade Estadual de Ponta Grossa/Departamento de Informática.

Ciência da Computação, Metodologia e Técnicas da Computação.

Palavras-chave: Segurança, Biometria, Periocular, LPQ.

Resumo

O Projeto tem como objetivo analisar o descritor de texturas com **LPQ *(Local Phase Quantization)***, implementando um sistema de cadastro e reconhecimento da região periocular realizando a autenticação pessoal em um servidor remoto em conjunto com um aplicativo para *smartphones Android*. Utilizando a distância euclidiana a partir de histogramas retirados das regiões perioculares pós LPQ como fator de aceitação para validação dos dados de um sujeito, foi executado o experimento para avaliação de confiança do algoritmo, utilizando o banco de imagens UBIRIS.v2, onde constatou que o LPQ é um bom descritor de textura atingindo níveis aceitáveis para com um banco de imagens não ideal barrando falsas tentativas de validação de dados.

Introdução

O estudo da tecnologia aplicada na identificação de pessoas reduz a quantidade de fraudes trabalhando com as características únicas de cada ser, dentre as possibilidades de reconhecimento por padrões baseadas em informações do corpo humano estão a impressão digital, palma da mão e região periocular (olhos, pálpebras, cílios e parte das sobrancelhas).

O projeto aqui abordado tem como objetivo principal o desenvolvimento de um sistema de autenticação pessoal analisando as características retiradas da região periocular, características estas, extraídas de um descritor de textura LPQ, quantização de fase local, da área que abrange o olho e a sua região periférica.

Trabalhos pioneiros utilizando a região periocular foram abordados em [1], [2] e [3]. Em [3] a região periocular é utilizada pelos autores como uma forma de determinar o gênero e raça de um indivíduo com resultados acima de 90% de acerto.

O uso de aparelhos específicos para biometria em aplicações do dia-a-dia torna esse sistema de segurança inviável para tarefas de menor importância, uma vertente que a pesquisa e o desenvolvimento tecnológico se aprofundaram foi a utilização dos *smartphones* para fins de validação de dados, uma prova desse avanço é a utilização de leitores biométricos para desbloqueio dos aparelhos, reconhecimento facial e registro da região da face em câmeras.

O desenvolvimento de um aplicativo de validação de dados em *smartphone* torna viável o reconhecimento sem a necessidade de aparelhos específicos para a tarefa, um aplicativo que seja confiável pode ser utilizado em qualquer sistema de segurança e em qualquer local por sua portabilidade.

Materiais e Métodos

Este subprojeto encontra-se organizado nas seguintes etapas:

I. Levantamento do estado da arte sobre uso de região periocular como biometria.
II. Aquisição de imagens utilizando tecnologia WAMP (Web Application Messaging Protocol).
III. Detecção da região periocular em imagens adquiridas na Etapa 2.
IV. Estudo de métodos de extração de características de textura, em especial LPQ periocular.
V. Definição de módulo de cadastro de usuário com dados de biometria periocular.
VI. Definição de módulo de verificação de usuário via biometria periocular usando medidas de similaridade.

Analisando o estado da arte sobre a região periocular como forma de validação de dados (etapa I) na literatura [4], é possível compreender que o LPQ analisa a imagem no domínio da frequência e que a ferramenta utilizada para transformação é a transformada discreta de Fourier (DFT).

Para detecção da região periocular, adquiridas na etapa II, são utilizadas as ferramentas de código aberto em linguagem Python versão 2.7 (etapa III). Neste trabalho é utilizado o OpenCV (Open Source Computer Vision Library) versão 2.9.14 com o Haar-Cascade [5] método de detecção que pode ser treinado para identificar uma região ou objeto.

O LPQ extrai as características da região periocular adquirida pelo OpenCV calculando a DFT pixel à pixel analisando seus pixels vizinhos. Com todos os pixels da imagem analisados é gerada uma nova imagem, esta agora no domínio da frequência, onde a partir dela é calculado um histograma com 256 valores, esses valores são o vetor característico da imagem que será considerada a chave para a identificação e validação dos dados.

Ao dispositivo móvel foi empregada a tarefa de apenas fotografar o sujeito e captar informações úteis como nome e CPF, após a captura dos mesmos essas informações são enviadas para um servidor externo que tem a função de calcular o LPQ e a medida de similaridade, aqui abordada com a distância euclidiana, entre os vetores característicos retornando o resultado para o dispositivo.

Resultados e Discussão

Para cálculo de confiança do algoritmo LPQ utilizou-se do banco de imagens UBIRIS.v2 [6]. Cerca de 10 sujeitos foram analisados, contendo 9 imagens cada totalizando em 90 o número de imagens. Para definir o valor de limite de distância euclidiana para validação foi utilizado 25% da variação entre a menor distância euclidiana e a maior encontrada entre as imagens do mesmo sujeito, esse limite define a máxima variação que uma comparação deve ter para que ela possa ser considerada de um mesmo sujeito. A distribuição das distâncias euclidianas para C'n sujeitos analisados estão representadas na Tabela 1.

Foram considerados resultados positivos a tentativa de autenticação de um sujeito C'n com ele mesmo cujo resultado dera positivo, maior que 50% na distribuição, ou uma tentativa de um sujeito C'n se passar por outro cujo resultado dera negativo, menor que 50% na distribuição.

TABELA 1 – Distribuição de distâncias euclidianas para os sujeitos C1 à C21

	Certeza		Pode ser		Não tem certeza		Não é	
	100,00%		75,00%		50,00%		25,00%	
C1	<	249	249	308	308	366	366	>
C3	<	260	260	328	328	397	397	>
C7	<	258	258	306	306	355	355	>
C9	<	271	271	333	333	394	394	>
C11	<	231	231	310	310	388	388	>
C13	<	244	244	271	271	298	298	>
C15	<	258	258	296	296	335	335	>
C17	<	273	273	329	329	384	384	>
C19	<	246	246	300	300	353	353	>
C21	<	278	278	320	320	363	363	>

Falsos positivos foram considerados como um sujeito C'n se passando por outro cujo resultado dera positivo, maior que 50% na distribuição. Falsos negativos foram considerados como uma tentativa de autenticação de um sujeito C'n com ele mesmo cujo resultado dera negativo, menor que 50% na distribuição. Todos os resultados podem ser conferidos na TABELA 2.

TABELA 2 – Resultado do cálculo de confiança para o algoritmo LPQ.

Positivo - Confirmação com identidades Iguais	46.67%
Falso Negativo - Negação com identidades Iguais	53.33%
Positivo - Negação com identidades Diferentes	86.17%
Falso Positivo - Confirmação com identidades Diferentes	13.83%

Conclusões

O principal requisito que uma unidade de validação de dados deve seguir é a sua capacidade de barrar tentativas falsas de autenticação, neste trabalho foi possível obter um resultado de cerca de 86% sobre a capacidade do algoritmo de barrar falsas autenticações e uma falha de cerca de 14% onde o algoritmo falhou em barrar falsas autenticações, falsos positivos. Deve se levar em conta a taxa de acerto entre tentativas de autenticação válidas, ou seja de um mesmo sujeito, onde o LPQ apresentou um resultado de cerca de 47% de acerto e bloqueou cerca de 53% das tentativas de um mesmo sujeito validar seus próprios dados, falsos negativos.
Tais níveis de confiança mostram que o LPQ é um algoritmo de validação de dados satisfatório considerando a utilização do banco de imagens, UBIRIS.v2, contendo imagens com iluminação, distância e perspectivas diferentes.
A definição do limiar para a validação do usuário apresentou melhor eficiência da maneira neste trabalho apresentada, para outros valores a taxa de acertos, resultados positivos, e erros, falsos negativos e falsos positivos, não ficaram satisfazíveis à idéia principal do projeto de modo que a medida que a eficiência aumentava em relação a autenticação do sujeito com a identidade dele mesmo, aumentaria a taxa de falsos positivos. Da mesma maneira caso a taxa de negação

de um sujeito autenticando com outra identidade aumentasse, a taxa de falsos negativos também aumentaria. Tal característica de funcionamento pode ser denotada como a região de trabalho do algoritmo LPQ.

Agradecimentos

À Deus...
Ao Prof. Doutor Alceu de Souza Britto Jr. pela contribuição de seus conhecimentos e sugestões na orientação deste projeto.
Ao Prof. Doutor Ariangelo Hauer Dias pela paciência e auxílio oferecidos.
A Universidade Estadual de Ponta Grossa, pelos recursos cedidos.
A Fundação Araucária pela oportunidade e por financiar o desenvolvimento do projeto de pesquisa.
A todos que direta ou indiretamente contribuíram para a conclusão deste trabalho.

Referências

[1] WOODARD, D., PUNDLIK, S., LYLE, J., et al. “Periocular region appea- rance cues for biometric identification”. In: Computer Vision and Pattern Recognition Workshops (CVPRW), 2010 IEEE Computer Society Confe- rence on, pp. 162–169, 2010.
[2] PARK, U., ROSS, A., JAIN, A. “Periocular biometrics in the visible spectrum: A feasibility study”. In: BTAS ’09: Proceedings of the IEEE 3rd Interna- tional Conference on Biometrics: Theory, Applications, and Systems, pp. 1–6, Sept 2009.
[3] JUEFEI-XU, F., LUU, K., et al. “Investigating age invariant face recognition based on periocular biometrics”. In: Biometrics (IJCB), 2011 Internatio- nal Joint Conference on, pp. 1–7, 2011.
[4]FACE DETECTION USING HAAR CASCADES. Disponível em: <https://docs.opencv.org/3.4.1/d7/d8b/tutorial_py_face_detection.html>. Acesso em: 5 de set. de 2017.
[5]OPENCV/DATA/HAARCASCADES/HAARCASCADE_EYE.XML. Disponível em: <https://github.com/opencv/opencv/blob/master/data/haarcascades/haarcascade_eye.xml>. Acesso em: 20 de out. de 2017.
[6] Hugo Proença, Sílvio Filipe, Ricardo Santos, João Oliveira, Luís A. Alexandre. "The UBIRIS.v2: A Database of Visible Wavelength Iris Images Captured On-The-Move and At-A-Distance", IEEE Transactions on Pattern Analysis and Machine Intelligence, Agosto, 2010, volume 32, número 8, pag. 1529-1535, ISSN: 0162-8828, Digital Object Identifier http://doi.ieeecomputersociety.org/10.1109/TPAMI.2009.66.