Um estudo de caso sobre autenticação biométrica em dispositivos móveis

Matheus Luan Krueger, Dalton Solano dos Reis, Aurélio Faustino Hoppe

Departamento de Sistemas e Computação
Universidade Regional de Blumenau (FURB) – Blumenau, SC – Brasil
{mkrueger, dalton, aureliof}@inf.furb.br

Abstract. *This paper presents a case study on biometric authentication on mobile devices (iOS), whose processing power and memory are fewer than conventional computers. In order to verify the performance and accuracy of the techniques that concern the biometric recognition it was developed a prototype that performs the identification and verification of individuals using iris images captured by the device's camera. Experimental results show that it is possible to perform the biometric authentication on mobile devices in an acceptable time, with rates of 3.2% for false negatives and 0% for false positives in 10,000 comparisons.*

Resumo. *Este trabalho apresenta um estudo de caso sobre autenticação biométrica em dispositivos móveis (iOS), cuja capacidade de processamento e memória são limitadas em relação a computadores convencionais. Com o objetivo de verificar o desempenho e a precisão das técnicas envolvidas no reconhecimento biométrico, foi desenvolvido um protótipo que realiza a verificação e a identificação de indivíduos através de imagens da íris capturadas pela câmera do próprio dispositivo. Os resultados obtidos apontam que é possível realizar, em um tempo aceitável, a autenticação biométrica em dispositivos móveis com taxas de 3,2% para falsos negativos e 0% para falsos positivos em 10.000 comparações.*

1. Introdução

A segurança dos dados e das aplicações atualmente figuram na lista de prioridades não só das empresas, mas também das próprias pessoas. Os dispositivos móveis estão gradativamente com maior capacidade de armazenamento e processamento e, ao mesmo tempo, contento muitas informações valiosas que se almeja manter em sigilo.

Uma das formas de alcançar esse sigilo é controlando o acesso de pessoas a essas informações e até mesmo locais, ou seja, realizando a autenticação dos indivíduos. A sociedade tem adotado três mecanismos tradicionais para resolver este problema de autenticação de pessoas, os quais são: (i) baseado em posse, o qual se refere aos objetos físicos que certo indivíduo possui, como chaves, passaporte ou cartão; (ii) baseado em conhecimento, que utiliza informações secretas do indivíduo, como senhas; e (iii) baseado em biometria, onde as características físicas ou comportamentais são os elementos que diferem os indivíduos, como por exemplo a íris [Bolle et al. 2004].

É nesse contexto que este artigo apresenta um protótipo para dispositivos móveis que realiza a autenticação de pessoas através de características biométricas únicas (no caso a íris), capturadas através da câmera do próprio dispositivo, para depois autorizar ou não o acesso a informação confidencial.

O restante deste artigo está organizado como segue. A seção 2 contém a fundamentação teórica envolvida no processo de reconhecimento da íris. Na seção 3 é apresentada uma visão geral dos trabalhos mais recentes na área de reconhecimento biométrico que utilizam técnicas de processamento de imagens para fazer a verificação e a identificação de indivíduos. Na seção 4 são descritas as etapas da arquitetura adotada. Na seção 5, os resultados obtidos são apresentados e discutidos. Finalmente, a seção 6 apresenta as conclusões e trabalhos futuros.

2. Fundamentação teórica

Nesta seção é apresentada a definição de biometria, seguida de uma breve caracterização das medidas biométricas. Aborda-se também o conceito de autenticação biométrica e o funcionamento de sistemas biométricos. Por fim, são relacionadas as etapas de processamento necessárias para realizar a autenticação biométrica pela íris.

2.1. Biometria

Realizando a composição dos termos gregos "*bio*", que significa vida, e "*metria*", que significa medida, forma-se a palavra biometria, que é um ramo da ciência que busca identificar ou verificar a identidade de uma pessoa baseado nas suas características físicas ou comportamentais [Jain, Flynn e Ross 2008]. As características físicas, como impressão digital, face e íris, medem a estrutura ou a forma de uma parte específica do corpo de uma pessoa, enquanto que as características comportamentais estão mais preocupadas em como uma pessoa faz devida ação, como por exemplo, falar [Gregory e Simon 2008].

Independente da característica a ser utilizada para realizar a autenticação biométrica, seja ela física ou comportamental, algumas propriedades devem ser elencadas para que uma medida biométrica seja considerada útil, que são [Bolle et al. 2004]:

a) universalidade: todo indivíduo deve possuir a medida em questão;

b) unicidade: ser suficientemente diferente entre os indivíduos;

c) inalterabilidade: se manter estável em função do tempo;

d) mensurabilidade: ser passível de captura e digitalização;

e) aceitabilidade: os indivíduos devem concordar em fornecer a medida biométrica.

Outras duas propriedades para avalizar uma medida biométrica são elencadas por [Jain, Flynn e Ross 2008] – desempenho e evasão, que são, respectivamente, o investimento necessário para se alcançar o processamento/precisão desejada e a dificuldade de indivíduos utilizarem artifícios para burlar o sistema. Na Tabela 1 é apresentado o resultado de um estudo comparativo entre as medidas biométricas mais comuns com relação às propriedades descritas anteriormente.

Tabela 1. Comparação entre as medidas biométricas mais comuns. Os níveis alto, médio e baixo são denotados por " * ", " ** " e " * ", respectivamente. (adaptado de [Jain, Ross e Prabhakar 2004]).**

COMPARAÇÃO ENTRE AS MEDIDAS BIOMÉTRICAS MAIS COMUNS								
Medida biométrica	**Universalidade**	**Unicidade**	**Inalterabilidade**	**Mensurabilidade**	**Aceitabilidade**	**Desempenho**	**Evasão**	**Somatório**
Assinatura	*	*	*	***	***	*	*	11
Dinâmica de andar	**	*	*	***	***	*	**	13
Face	***	*	**	***	***	*	*	14
Geometria da mão	**	**	**	***	**	**	**	15
Impressão digital	**	***	***	**	**	***	**	17
Íris	***	***	***	**	*	***	***	18
Retina	***	***	**	*	*	***	***	16
Voz	**	*	*	**	***	*	*	11

Como pode ser observado na Tabela 1 (coluna Somatório), a íris é a medida biométrica que apresenta os níveis mais altos de propriedades em comparação com as outras elencadas. A utilização dela como medida biométrica foi sugerida no final de 1800. Porém, apenas em meados dos anos 1990 que os avanços em visão computacional, a captura de imagens e o processamento dos computadores permitiram a sua implementação prática [Matey, Broudssard e Kennell 2010]. Desde então, a íris vem sendo considerada a característica mais promissora dentre as medidas biométricas, devido à sua randomicidade, estabilidade, exatidão, unicidade, entre outros fatores [Daugman 1993].

2.2. Sistemas de autenticação biométrica

A autenticação biométrica é um processo que permite determinar a identidade de um indivíduo tomando como base quem ele é ao invés de algo que ele lembra ou possui. Dependendo do contexto em que for utilizada a autenticação biométrica pode operar de duas formas diferentes: verificação e identificação [Jain, Flynn e Ross 2008].

Para a verificação de um indivíduo é necessário que este apresente alguma informação referente a si mesmo (por exemplo, número de identificação) e sua respectiva medida biométrica. Esta forma de autenticação realiza comparações do tipo um-para-um (1:1) e caracteriza-se como uma combinação dos mecanismos de autenticação. Já a identificação é a forma de autenticação biométrica visto como autenticação pura, pois se baseia apenas na medida biométrica apresentada. Esta, diferentemente da verificação, realiza comparações do tipo um-para-muitos (1:n) e é mais difícil de implementar devido às necessidades de busca [Bolle et al. 2004].

Segundo [Gregory e Simon 2008], independente da forma de operação da autenticação, os sistemas de reconhecimento biométrico são divididos em três grandes fases: registro, utilização e atualização. A fase de registro compreende o cadastramento de indivíduos na base de dados, na qual a amostra biométrica é processada e armazenada em conjunto com as informações do indivíduo. O processo de atualização da amostra

biométrica é necessário tendo em vista as mudanças que certas características possam sofrer ao longo do tempo, como por exemplo, a face. A utilização ocorre quando a população que está cadastrada no sistema começa a fazer o uso da autenticação biométrica para controlar o acesso a lugares ou informações, sendo que a cada momento, uma dada amostra é capturada, processada e comparada com outras e, ao final, o sistema autoriza ou não o acesso.

Para que uma amostra biométrica seja mensurada e posteriormente comparada com outra existe uma série de etapas de processamento necessárias a se realizar, que variam de acordo com a amostra biométrica em questão. Especificamente em sistemas de autenticação biométrica por íris, [Wildes 1997] descreve três grandes etapas: aquisição da amostra biométrica, localização da íris e a comparação dos padrões.

Uma dos grandes desafios na etapa de aquisição é o de se capturar amostras da íris suficientemente boas para realizar a autenticação biométrica. Para isso deve-se levar em consideração vários aspectos, como: (i) distância da captura; (ii) iluminação; (iii) ruídos na imagem e (iv) posição da íris na imagem [Wildes 1997]. O próximo passo após a captura da amostra é o de se isolar a região específica da íris, no qual deve-se localizar as extremidades da íris considerando os possíveis ruídos e oclusões.

A última etapa definida por [Wildes 1997] envolve a normalização da imagem da íris, pois o tamanho, a escala e a rotação da amostra tendem a variar. Em seguida ocorre o processo de extração e codificação das características, as quais serão utilizadas para comparar uma amostra biométrica com outra.

O resultado da comparação entre uma amostra e outra gera uma saída do tipo "sim/não" e, esta situação, se enquadra perfeitamente na estrutura clássica da teoria da decisão estatística. Existem quatro tipos de saídas para os sistemas biométricos: *False Accept* (FA), *Correct Accept* (CA), *False Reject* (FR) e *Correct Reject* (CR), sendo que a primeira e a terceira são consideradas erros. A partir dessas saídas podem-se avaliar dois tipos de taxas de erro. A primeira taxa é chamada de *False Accept Rate* (FAR) e representa a probabilidade de um impostor ser aceito pelo sistema. Já a segunda taxa, denominada de *False Reject Rate* (FRR), representa a probabilidade de um indivíduo apto ser considerado um impostor, e ser recusado pelo sistema [Daugman 2000].

3. Trabalhos correlatos

Durante o processo de pesquisa não foram encontrados trabalhos semelhantes a este, que tivessem um estudo de caso sobre autenticação biométrica em dispositivos móveis e utilizassem, exclusivamente, o espectro de luz visível para iluminação. Desta forma, focou-se nos trabalhos correlatos desenvolvidos na plataforma desktop. Dentre as obras disponíveis, foram selecionados três trabalhos que buscaram estudar e implementar de forma genérica as diferentes técnicas envolvidas no processo de reconhecimento de íris, os quais são descritos por [Masek 2003], [Carneiro 2010] e [Boyd et al. 2010].

O trabalho de [Masek 2003] busca desenvolver um sistema de reconhecimento de íris de código aberto em MATtrix LABoratory (MATLAB). Cada etapa envolvida no processamento da amostra biométrica foi implementada separadamente e validada a partir de dois bancos públicos de imagens do olho: CASIA e LEI, compostos, essencialmente, por imagens capturadas com a utilização da iluminação infravermelho.

Em [Carneiro 2010] é apresentada uma pesquisa bibliográfica sobre os principais trabalhos na área de reconhecimento pela íris e a implementação das técnicas tradicionais em cada etapa de processamento. É discutido um novo método para a localização da íris e para extração de características. Para validar e comparar a implementação em MATLAB, que se baseou nos estudos de [Masek 2003], foram utilizados dois bancos públicos de imagens do olho – UBIRIS e MMU. Por fim, [Boyd et al. 2010] realizam a implementação dos métodos mais discutidos na bibliografia na linguagem de programação C++ e validam o protótipo a partir do banco público CASIA.

4. Desenvolvimento

Esta seção descreve o desenvolvimento das etapas que concernem a autenticação biométricas de pessoas pela íris. A arquitetura adotada (Figura 1) se sustenta nos estudos de [Daugman 1993] e [Wildes 1997] e foi implementada na plataforma móvel iOS.

Além de separar as etapas de processamento de imagens da íris, que variam desde a captura da amostra biométrica até a comparação entre duas ou mais amostras para se gerar um resultado, a Figura 1 destaca as três grandes fases de sistemas biométricos descritas por [Bolle et al. 2004], que são: registro, utilização e atualização.

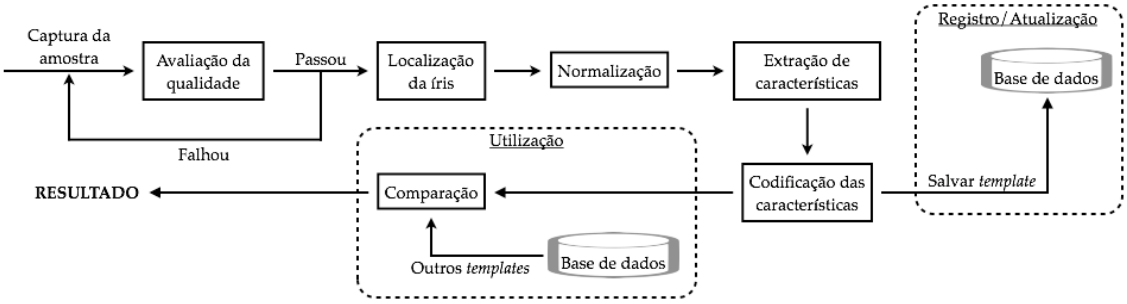


Figura 1. Arquitetura do sistema de reconhecimento biométrico adotada

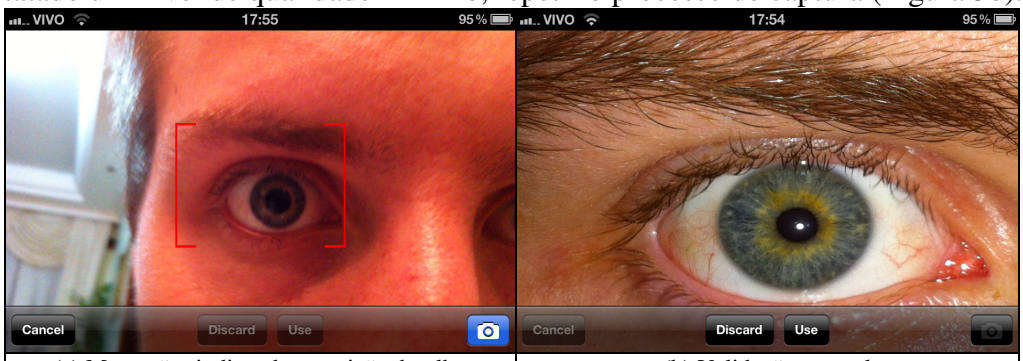
4.1. Aquisição da amostra biométrica

Considerando as ponderações feitas por [Wildes 1997] referentes à captura de imagens da íris e que a arquitetura adotada (ilustrada na Figura 1) prevê a aquisição de amostras biométricas de forma integrada, algumas configurações foram necessárias para permitir a captura de imagens pelo próprio dispositivo. Definiu-se que a aquisição das amostras seria realizada através da câmera traseira do dispositivo com a utilização do flash, considerando o foco da câmera no ponto central da imagem

Devido às variações de tamanho dos olhos em função da distância em que uma foto é tirada, fez-se necessário o desenvolvimento de uma estrutura de camadas para delimitar a região de interesse – íris, e instruir o usuário no processo de captura. Esta estrutura (Figura 2) é constituída por três camadas sobrepostas com funcionalidades distintas. Enquanto que a camada inferior é responsável por apresentar as imagens recebidas pela câmera em tempo real, a camada intermediária tem a função de desenhar um marcador que indica a posição do olho. Já a camada superior tem a função de desenhar os controles do usuário e tratar suas interações.

Figura 2. Camadas da tela de aquisição de amostras biométricas

Após a captura de uma amostra biométrica, a mesma passa por um processo de recorte da região de interesse, que consiste basicamente em descartar todo o conteúdo externo ao marcador indicado na Figura 3a. Em seguida, esta imagem é exposta ao usuário para que o mesmo realize uma avaliação da qualidade, podendo, caso não tenha constatado um nível de qualidade mínimo, repetir o processo de captura (Figura 3b).



(a) Marcações indicando a posição do olho (b) Validação manual

Figura 3. Processo de aquisição de amostras biométricas.

4.2. Localização da íris

Uma vez que a região de interesse fora recortada da imagem, inicia-se o processo de localização da íris. Este processo consiste em encontrar as extremidades da íris, oclusões e os possíveis ruídos, provenientes do fator humano ou do próprio processo de captura.

Devido ao fato da região de interesse ser colorida, é necessário realizar a conversão da imagem para tons de cinza [Hess 2011]. A partir da imagem em tons de cinza é aplicado o filtro da mediana para suavizar os ruídos e manter os detalhes dos contornos. Este filtro, descrito com detalhes em [Boyd et al. 2010], consiste basicamente em determinar o valor pixel a pixel de acordo com a média dos valores de seus vizinhos.

A localização da região da íris ocorre através da aproximação de círculos para representar as extremidades da íris. Este processo é feito aplicando-se a transformada de círculos de Hough [Nixon e Aguado 2008]. Para isso, utilizou-se a biblioteca OpenCV 2.3.3 pré-compilada para a arquitetura iOS e sua função específica `cvHoughCircles`, que aplica internamente o filtro de detecção de bordas de Canny e retorna os possíveis círculos de acordo com os parâmetros que foram passados. Este filtro é aplicado em dois momentos. No primeiro, os parâmetros são ajustados para encontrar o limite entre a íris e a esclerótica. No segundo momento alteram-se os parâmetros da função para que seja possível realizar a localização do círculo que representará o limite entre a íris e a pupila. Cabe mencionar que a detecção de ruídos e/ou oclusões não foi implementada.

4.3. Extração e codificação das características

No processo de extração de características, os detalhes mais significativos da estrutura da íris devem ser detectados da imagem normalizada. Para a normalização da íris foi implementado o método mais tradicional e amplamente utilizado, denominado *homogenous rubber sheet model*. Este método consiste em re-mapear a região da íris passando de coordenadas cartesianas para coordenadas polares adimensionais.

Em [Carneiro 2010] são elencadas diversas formas de se realizar a extração desses detalhes significativos. A utilização dos filtros de Gabor foi definida para realizar a extração das características, técnica apresentada e discutida em [Daugman 1993] e [Boyd et al. 2010]. A codificação dessas características mais significativas foi feita com base no algoritmo denominado IrisCode, proposto por [Daugman 1993] e implementado por [Boyd et al. 2010].

4.4. Comparação

A distância de Hamming foi utilizada como métrica para estabelecer o grau de similaridade entre duas amostras biométricas. O desenvolvimento dessa etapa se deu a partir dos trabalhos descritos por [Daugman 1993], [Masek 2003] e [Boyd et al. 2010].

5. Resultados e discussão

Para validar o protótipo foram realizados dois experimentos: o primeiro, com o intuito de validar o processo de reconhecimento pela íris; e o segundo, com o objetivo de verificar o desempenho do protótipo.

Inicialmente coletaram-se as amostras biométricas de 10 pessoas, em um ambiente com iluminação natural. A captura se deu a partir de um iPhone 4, que possui uma câmera de 5MP e resulta em imagens coloridas de 2.592 x 1.936 pixels. Foram capturadas 10 amostras biométricas de cada pessoa, sendo 5 amostras da íris do olho direito e 5 amostras do olho esquerdo, totalizando 100 amostras.

5.1. Precisão

A partir da coleta dos dados foram feitas comparações intra-classe e inter-classe entre as amostras. As distâncias provenientes dessas comparações foram agrupadas em grupos de 0,2 centésimos para facilitar a representação e a visualização das distribuições.

Nas comparações intra-classe, uma amostra biométrica é comparada com ela mesma. Tendo 5 amostras de cada íris, têm-se 5 comparações. Este processo foi repetido individualmente para cada um dos 20 grupos de amostras, totalizando em 500 comparações. Já nas comparações inter-classe cada amostra biométrica é comparada com todas as outras 95 amostras de íris diferentes. Dessa forma, as comparações dessa classe totalizaram em 9500 comparações.

Na Figura 4, pode-se observar que das 500 comparações realizadas, 78 foram consideradas iguais (variação 0). Porém, o resultado correto deveria ser 100, visto que têm-se 5 amostras em cada um dos 20 grupos e, que quando comparadas com elas mesmas deveriam ser consideradas iguais. Porém, não foi o que aconteceu. Para tentar descobrir o motivo desta diferença, optou-se por testar e analisar os resultados gerados em cada uma das etapas envolvidas no reconhecimento da íris. Ao final, identificou-se que a diferença era gerada na etapa de comparação. Entretanto, não descobriu-se o

motivo, pois nesta etapa tem-se apenas a implementação da distância de Hamming, conforme descrito na literatura [Boyd et al. 2010]. Todavia, nossas suspeitas recaem sobre uma possível limitação do tipo da variável utilizada, fato que ocasionaria arredondamento/truncamento do valor calculado para determinar o grau de similaridade. No entanto, são necessários mais estudos neste sentido.

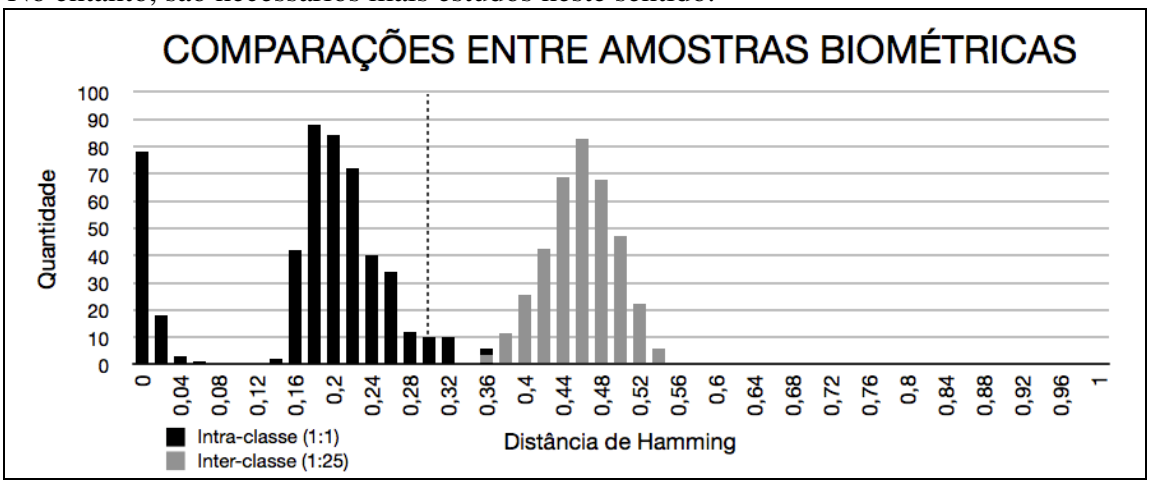


Figura 4. Distribuição das distâncias de Hamming obtidas a partir das comparações entre amostras biométricas (intra-classe e inter-classe).

A partir da Figura 4 percebe-se também que nas comparações intra-classe apenas 6 amostras possuem um discrepância maior (variação de 0,36). Esta variação é decorrente a problemas ocorridos na etapa de aquisição. Verificou-se que as amostras em questão estavam desfocadas e/ou com ruídos. Isto se deve ao fato de que o usuário que capturou as amostras as considerou de boa qualidade, mas não eram. A partir da Figura 4, é possível verificar que nenhuma das comparações inter-classe resultaram em uma distância de Hamming próxima a 0. Isso indica que o protótipo garante a distinção entre diferentes amostras.

Através das distribuições das distâncias de Hamming resultantes das comparações intra-classe e inter-classe consegue-se identificar qual é o melhor valor do limiar de decisão que minimiza as taxas de erro em relação à probabilidade de um invasor ser aceito pelo sistema (FAR) e a probabilidade de um indivíduo apto ser considerado um invasor (FRR) e, portanto, ser recusado pelo sistema. A Tabela 2 apresenta a relação entre a FAR e a FRR de acordo com a modificação do limiar entre classes, sendo que a decisão de se aumentar ou diminuir este limiar deve ser analisada caso a caso.

Tabela 2. Variação das taxas de erro (FAR / FRR).

VARIAÇÃO DAS TAXAS DE ERRO (FAR / FRR)							
Limiar HD	0,24	0,26	0,28	0,30	0,32	0,34	0,36
FAR (%)	0	0	0	0	0.06	0,1	0,94
FA	0	0	0	0	6	10	90
FRR (%)	14,4	7,6	5,2	3,2	1,2	1,2	0
FR	72	38	26	16	6	6	0

A partir da Tabela 2 observa-se que o valor do limiar de decisão deve situar-se próximo da distância de Hamming 0,3 para que o sistema de reconhecimento biométrico tenha um bom desempenho em termos de autenticação de utilizadores legítimos, e bastante seguro em termos de autenticação de utilizadores não legítimos.

Um aspecto importante a ser comentado a respeito do limiar entre classes é que conforme se aumenta ou diminui este valor altera-se diretamente a relação entre a FAR e a FRR. Por exemplo, aumentando o limiar entre as classes para 0,34, a quantidade de falsas rejeições (FR) cai de 16 para 6 enquanto que a quantidade de falsas aceitações (FA) aumenta de 0 para 10, resultando em uma FAR de 0,1% e uma FRR de 1,2%.

5.2. Desempenho

A avaliação de desempenho do protótipo foi realizada de forma individual para cada uma das 8 etapas envolvidas no reconhecimento da íris. Cada etapa foi executada 10 vezes, permitindo calcular as médias do tempo de execução individual, as quais estão expressas na Tabela 3. Os testes foram realizados em um iPhone 4 (Processador ARM Cortex-A8 1 GHz, 512MB eDRAM) e no simulador do iPhone em um MacBook Pro (Processador Intel Core i5 2.4GHz, 4GB DDR3).

Tabela 3. Desempenho individual das etapas envolvidas no processamento de uma amostra biométrica.

DESEMPENHO INDIVIDUAL DAS ETAPAS ENVOLVIDAS NO PROCESSAMENTO DE UMA AMOSTRA BIOMÉTRICA		
Etapa	**Tempo (segundos)**	
	iPhone 4	MacBook Pro
Captura da amostra biométrica / recorte da região de interesse	0,000133	0,002589
Localização da íris (conversão para escala de cinza)	0,078349	0,017497
Localização da íris (filtro da mediana)	25,78702	1,403432
Localização da íris (transformada de Hough)	2,819058	0,267903
Normalização	0,334168	0,022170
Extração de características	3,892799	0,271037
Codificação das características	0,001331	0,000245
Comparação (1:1)	0,029957	0,003611
Total	**32,94281**	**1,988485**

Na Tabela 3, pode-se observar que o tempo médio gasto para realizar o reconhecimento biométrico no iPhone 4 é de aproximadamente 33 segundos e, que a etapa localização da íris utilizando o filtro da mediana é a que gera o maior gargalo do protótipo, consumindo 78% do tempo total. Já no MacBook Pro o tempo gasto nesta etapa é de 1,40 segundos, representando 70%. Considerando apenas os percentuais da etapa de localização da íris (filtro da mediana), constata-se que o desempenho é equivalente tanto no dispositivo móvel como no simulador. Todavia, o alto custo computacional do filtro da mediana se deve ao fato de que não foram feitas otimizações no algoritmo proposto por [Boyd et al. 2010].

6. Conclusão e trabalhos futuros

Este artigo apresentou um estudo de caso sobre autenticação biométrica em dispositivos móveis sem a utilização de iluminação infravermelho, utilizando somente a própria câmera do dispositivo.

A arquitetura adotada (Figura 1) se sustenta nos estudos de [Daugman 1993] e [Wildes 1997], no entanto, foi adaptada para ser desenvolvida em uma plataforma móvel utilizando o SDK do iOS. Através dos resultados obtidos comprovou-se que é possível, em um tempo aceitável, realizar a autenticação biométrica com taxas de 3,2% para falsos negativos e 0% para falsos positivos. Estas taxas foram alcançadas após

análise e ajuste do valor do limiar entre classes para 0,3. Dessa forma garantiu-se um bom desempenho em termos de autenticação de utilizadores legítimos e ao mesmo tempo, bastante seguro em termos de autenticação de utilizadores não legítimos.

Em relação aos trabalhos correlatos, as taxas de erro e o valor do limiar entre classes ficaram próximos aos apresentados neste trabalho. Entretanto, o grande diferencial é que este trabalho implementou em um dispositivo móvel, de forma integrada, todas as etapas envolvidas em um sistema de autenticação biométrica.

Por fim, este estudo de caso resultou em diferentes extensões, entre elas: (i) utilizar uma base de imagens de íris maior; (ii) implementar a detecção de ruídos e oclusão; e (iii) estudar outras alternativas de implementar o filtro da mediana já que esta etapa é a que demanda mais processamento.

Referências

Bolle, R. M. et al. (2004), Guide to biometrics, Springer.

Boyd, M. et al. (2010), Iris recognition. Imperial College London, Inglaterra.

Carneiro, M. B. P. (2010), Reconhecimento de íris utilizando algoritmos genéticos e amostragem não uniforme. Tese, Universidade Federal de Uberlândia, Brasil.

Daugman, J. (1993), High confidence visual recognition of persons by a test of statistical independence. IEEE Transactions on Pattern Analysis and Machine Intelligence, p. 1148-1161.

Daugman, J. (2000), Biometric decision landscapes. Relatório técnico, University of Cambridge, United Kingdom.

Gregory, P. e Simon, M. A. (2008), Biometrics for dummies, Wiley.

Hess, C. (2011), API para transformação de imagem em cartum utilizando plataforma iOS. Monografia, Universidade Regional de Blumenau, Brasil.

Jain, A. K., Ross, A. A. e Prabhakar, S. (2004), An introduction to biometric recognition. IEEE Transactions on Circuits and Systems for Video Technology, p. 4-20.

Jain, A. K., Flynn, P. e Ross, A. A. (2008), Handbook of biometrics, Springer.

Matey, J. R., Broussard, R. and Kennell, L. (2010) “Iris image segmentation and sub-optimal images”, Image and Vision Computing, Massachusetts, p. 215-222.

Nixon, M. e Aguado, A. S. (2008), Feature extraction & image processing for computer vision, 2nd, Academic Press.

Masek, L. (2003) Recognition of human iris patterns for biometric identification. Relatório final, Western University, Austrália.

Wildes, R. P. (1997) “Iris recognition: an emergingi biometric technology”, Proceedings of the IEEE, p. 1348-1363.