Autenticação Facial Contínua usando Imagens de Infravermelho

Matheus Magalhães Batista dos Santos, Maurício Pamplona Segundo
Departamento de Ciência da Computação
Universidade Federal da Bahia
Salvador, Brasil
matheusmbs@ufba.br, mauricio@dcc.ufba.br

***Resumo*—Diversos sistemas de autenticação tem sido desenvolvidos utilizando reconhecimento facial. Porém boa parte desses sistemas sofrem com variações de iluminação ambiente e não garantem que apenas o usuário permitido utilize o sistema. Para realizar esta tarefa apresentamos um sistema de autenticação facial contínua baseado em imagens de infravermelho para alcançar invariância à iluminação ambiente. Até onde sabemos, este é o primeiro sistema que utiliza imagens em infravermelho para a autenticação contínua. Avaliamos nosso sistema utilizando quatro vídeos de 1000 quadros cada e obtivemos uma taxa de reconhecimento de 93%.**

***Abstract*—Many authentication systems have been developed, including the ones that use face recognition. However, most of them are affected by changes in environmental illumination and cannot ensure than only the allowed user uses the system. To accomplish this challenge, we present a continuous infrared-based face authentication system to reach illumination invariance. At the best of our knowledge, this is the first system that uses infrared images for continuous authentication. We evaluated our system on four 1000 frames long videos and achieved a 93% true positive rate.**

***Keywords*-reconhecimento facial; infravermelho; padrões binários locais; autenticação contínua;**

I. Introdução

Com o passar dos anos, métodos tradicionais de autenticação como senhas ou cartões se tornaram arriscados em ambientes que demandam um controle de segurança mais . A biometria foi uma solução adotada em muitos sistemas para suprir essa demanda, e muitas pesquisas foram desenvolvidas nessa área recentemente [1]. Diversas características biométricas podem ser utilizadas, dentre elas: face, impressão digital, voz, íris, eletroencefalograma e eletrocardiograma [2]. Entretanto, a maioria desses sistemas de autenticação garantem acesso a usuários autorizados apenas uma vez e nenhuma verificação adicional é feita posteriormente. Com isso, não existe garantia que um acesso não autorizado pode ser feito após a verificação inicial. Para resolver esse problema, a autenticação contínua realiza a verificação constantemente, garantindo assim que o usuário autorizado seja o mesmo durante toda a utilização do sistema.

No contexto da autenticação contínua, a forma de digitar foi a característica pioneira [3], [4]. Apesar dos benefícios, é necessário muito tempo para se detectar um impostor, e comandos nocivos ao sistema podem ser digitados rapidamente antes que o sistema invalide o acesso. Sistemas baseados em impressão digital são inconvenientes, pois exigem que o usuário coopere constantemente para a obtenção das digitais [5]. Eletrocardiogramas exigem que o usuário utilize sensores e estão sujeitos a variações cardíacas causadas por fatores patológicos ou emocionais [2].

O reconhecimento facial é uma característica de custo relativamente baixo e resultados satisfatórios, e pode ser utilizada na autenticação contínua sem a colaboração do usuário. Existem três propriedades que podem ser utilizadas no reconhecimento facial: textura, infravermelho e geometria. A textura é uma propriedade obtida em fotos comuns, através da captura da luz visível da cena. Infravermelho é obtida através de luz invisível aos olhos humanos. A geometria captura a profundidade dos objetos e da cena em relação ao sensor.

Diversos fatores podem interferir na segurança de cada propriedade, dentre eles a presença de óculos, variações de pose, expressões faciais, iluminação e/ou temperatura facial. O sistema baseado em imagens de textura é o mais amplamente empregado, mas é também o que sofre mais influência da variação de iluminação externa, mesmo em ambientes fechados. Com isso, a variação causada pela iluminação em faces da mesma pessoa pode ser maior do que a variação entre imagens de pessoas diferentes com condições de iluminação semelhantes [6]. Para sistemas baseados em infravermelho no espectro termal, a temperatura da face pode alterar devido a condições emocionais ou prática de atividade física antes da verificação. Por fim, os baseados em geometria necessitam de sensores mais caros, possuem nível de ruído considerável e tem custo computacional maior.

Nesse artigo, nós propomos um sistema de reconhecimento facial baseado em imagens de infravermelho invariante a iluminação ambiente, rápido e seguro para fins de autenticação contínua. O uso de espectro próximo ao infravermelho (NIR, *Near-Infrared*) evita variações de iluminação permitindo uma classificação melhor. Câmeras em NIR são acessíveis atualmente, custando menos de 70 reais. Em especial, o Kinect One permite capturar imagens em infravermelho com baixo nível de ruído.

A. Trabalhos relacionados

O uso de infravermelho tem crescido muito no ramo do reconhecimento facial e diversos avanços foram obtidos na

área. Li *et al.* [7] apresentou um sistema de reconhecimento invariante a iluminação utilizando imagens NIR através do uso de padrões binários locais (LBP, *Local Binary Pattern*) e o algoritmo de aprendizagem AdaBoost para construir um classificador não linear para reconhecimento facial. Wei *et al.* [8] utilizou um algoritmo genético multi-objetivo na seleção de características mais discriminantes com LBP. Xie *et al.* [9] criou um algoritmo de seleção de padrões para superar a combinação dos métodos tradicionais de análise de componentes principais e análise linear discriminante. Maeng *et al.* [10] apresentou um sistema de reconhecimento facial em NIR à distância utilizando um telescópio. Emissões termais também foram exploradas com ondas longas de infravermelho [11]. Embora o reconhecimento facial em infravermelho tenha sido explorado nos últimos anos, ele não foi utilizado para a autenticação contínua.

B. Estrutura do artigo

Este artigo está organizado da seguinte maneira: A seção II descreve nosso trabalho para autenticação facial contínua com imagens em infravermelho. Na Seção III exibimos os resultados de testes obtidos com quatro vídeos de 1000 quadros cada um. Seção IV mostra nossas conclusões seguidas dos agradecimentos e das referências.

II. Autenticação utilizando imagens NIR

O sistema utiliza uma câmera NIR e realiza todas as etapas do reconhecimento facial utilizando implementações baseadas na biblioteca OpenCV[1], uma biblioteca de computação visual de licença aberta que possui todo um conjunto de funções, métodos, classes e algoritmos que lidam com computação visual. Além disso, utilizamos um filtro de equalização de histogramas, tanto no cadastro de faces quanto no reconhecimento, o que diminui a variação de iluminação causada pela proximidade da face em relação aos emissores de infravermelho. Para a detecção facial, treinamos um classificador em cascata baseado no trabalho de Viola e Jones [12]. Depois, as faces são normalizadas alinhando os olhos para que fiquem sempre na mesma posição e removendo informações de fundo da cena. Para evitar a perda de quadros quando os olhos não são detectados, utilizamos o Kalman Filter para estimar a posição dos olhos. Por fim, no reconhecimento facial foi usado o método de histogramas de padrões binários locais (LBPH, *Local Binary Pattern Histogram*) para obter as similaridades que são combinadas ao longo do tempo para calcular a probabilidade do sistema estar seguro. O sistema está seguro durante o período de login, então são capturados 5 quadros para serem utilizados como modelo do usuário. Após o login, cada quadro posterior tem sua similaridade calculada em relação ao modelo do usuário. Essa similaridade é utilizada para calcular a probabilidade do sistema ainda estar seguro. Se a probabilidade ficar abaixo de um limiar definido, o sistema é considerado inseguro e o usuário perde a autorização para utilizar o sistema. Para cada quadro, temos as seguintes etapas, como mostrado na Figura 1: (1) detecção da face; (2) normalização da face; (3) cálculo da similaridade LBPH; e (4) fusão de similaridade. Mais detalhes sobre cada etapa são dados nas subseções a seguir.

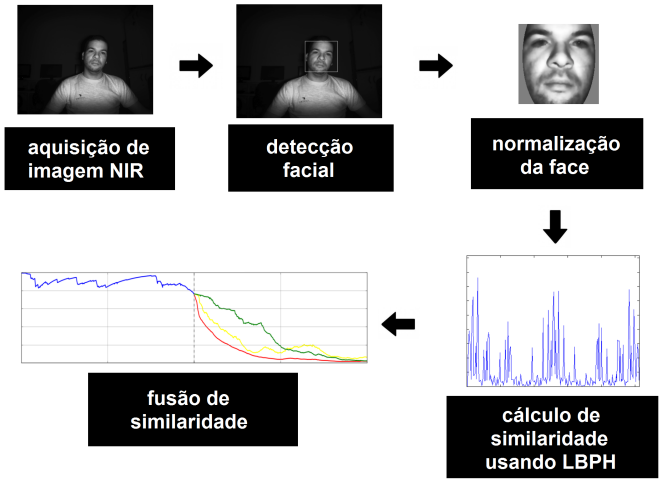


Figura 1. Diagrama de estágios do sistema.

A. Aquisição de imagens

O Microsoft Kinect One[2] é um dispositivo com sensor de profundidade, câmera colorida e um emissor de infravermelho. As imagens em infravermelho possuem resolução de 512x424. Seus emissores são capazes de gerar uma boa iluminação frontal com baixíssimo ruído, funcionando até mesmo em completa escuridão. Para a obtenção das imagens capturadas pelo Kinect nós utilizamos a biblioteca Libfreenect2[3].

B. Detecção facial

Nessa etapa foi utilizado um classificador em cascata de características de Haar [12], pois este permite detectar faces com grande velocidade e atingir altos índices de detecção. Existem muitos classificadores para imagens de textura, porém o mesmo não ocorre para imagens em infravermelho. Por este motivo, um classificador foi criado neste trabalho utilizando funções da biblioteca OpenCV. Ela possui tanto algoritmos de treinamento de classificadores quanto de detecção.

Primeiro utilizamos as bases Surveillance Cameras Face Database (SCFACE) [13] e a CASIA NIR Database (CASIA) [14] para treinar o classificador de faces em infravermelho. A SCFACE é uma base que contém 4160 imagens de 130 indivíduos, porém apenas 130 imagens estão em infravermelho. Já a CASIA possui 3940 faces de 197 pessoas em infravermelho. Para o conjunto de imagens negativas foram utilizadas as imagens destas bases com a região da face removida e também imagens aleatórias de paisagens e objetos capturados com câmeras de infravermelho, como ilustrado na Figura 2.

[1] http://opencv.org/

[2] https://www.microsoft.com/en-us/kinectforwindows/meetkinect/features.aspx

[3] https://github.com/OpenKinect/libfreenect2

(a) Imagem positiva (b) Imagem negativa (c) Face detectada

Figura 2. Exemplos de imagens para treino de um classificador e resultado da detecção.

Foram utilizadas no treinamento um total de 3986 imagens positivas e de 7645 imagens negativas. Realizamos o treino através das funções opencv_createsamples e opencv_traincascade com os seguintes parâmetros:

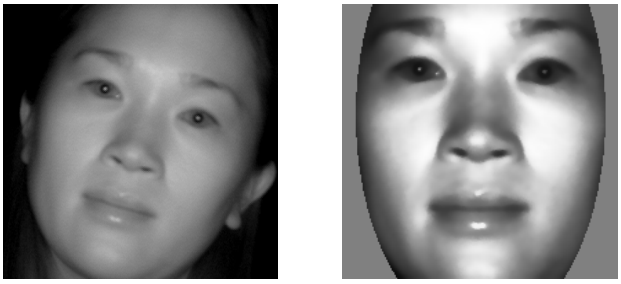
```
$ opencv_createsamples
    -bgcolor 0
    -bgthresh 0
    -maxxangle 1.1
    -maxyangle 1.1 maxzangle 0.5
    -maxidev 40
    -w 20
    -h 20

$ opencv_traincascade
    -data classifier
    -numStages 20
    -minHitRate 0.999
    -maxFalseAlarmRate 0.5
    -numPos 1000
    -numNeg 600
    -w 20
    -h 20
    -mode ALL
    -precalcValBufSize 1024
    -precalcIdxBufSize 1024
```

Para evitar que indivíduos que transitem atrás do usuário tenham suas faces detectadas e computadas, o sistema mantém a posição da última face corretamente detectada. A cada nova detecção ele compara a distância euclidiana entre esta nova face e a última detectada. Se essa distância for maior que um limiar estabelecido, a face é descartada. Do contrário ela será normalizada e computada.

C. Normalização da face

A primeira parte da etapa de normalização e pré-processamento da face é a detecção dos olhos. É possível assumir que os olhos estão em posição relativamente simétricas, além de possuírem uma posição e tamanho padrões em relação a face independentemente da expressão facial, e com isso evitar um custo computacional elevado para etapa de detecção. Para a detecção, utilizamos três classificadores em cascata da biblioteca OpenCV, um específico para o olho esquerdo, um para o olho direito e um genérico para ambos. Para cada subregião da face onde se encontram os olhos, primeiro é utilizado o classificador específico daquela região. Caso não seja possível detectar o olho, o classificador mais genérico é utilizado. Quando não é possível detectar os dois olhos, suas respectivas posições são estimadas utilizando um Kalman Filter. A cada normalização a posição dos olhos é estimada e corrigida pelo Kalman Filter. Para evitar o aumento no erro da normalização, esse recurso só é utilizado por um número fixo e pequeno de quadros onde não foi possível detectar um dos olhos.

Detectados os dois olhos, o ângulo entre eles é calculado para realizar uma rotação da face de maneira que eles fiquem alinhados horizontalmente. Depois a face é redimensionada para que a distância entre os olhos seja sempre a mesma, seguida de uma translação para que toda face tenha os olhos na mesma altura desejada. Uma máscara elíptica é aplicada para remover o máximo de informações irrelevantes que estão em volta da face. Por fim um filtro de equalização de histogramas e um filtro bilateral são aplicados para reduzir a variação de iluminação decorrente da distância dos emissores de infravermelho e possíveis ruídos, como mostrado na Figura 3.



(a) Face antes da normalização (b) Face normalizada

Figura 3. Resultado da etapa de normalização.

D. Cálculo da similaridade utilizando LBPH

Existem três métodos principais de reconhecimento facial implementados na biblioteca OpenCV: Eigenfaces, Fisherfaces e LBPH. Realizamos uma experiência utilizando os três métodos. Foram utilizadas, para cada método, 810 imagens de 90 pessoas diferentes para o treino, 810 imagens para o teste com pessoas cadastradas e 864 imagens de 48 pessoas não cadastradas. Como mostrada na curva de característica de operação do receptor (ROC, *Receiver Operating Characteristic*) da Figura 4, o método LBPH se mostrou superior em acurácia em relação aos outros dois métodos e por isso utilizamos o mesmo neste trabalho.

O LBP consiste em codificar uma estrutura local de uma imagem comparando cada pixel com seus vizinhos. Caso o valor de intensidade do pixel central for maior ou igual que a intensidade do vizinho, atribuímos o valor 1 a esse vizinho, ou 0 do contrário. No final do processo, cada pixel terá um valor numérico que é a concatenação dos valores atribuídos aos seus

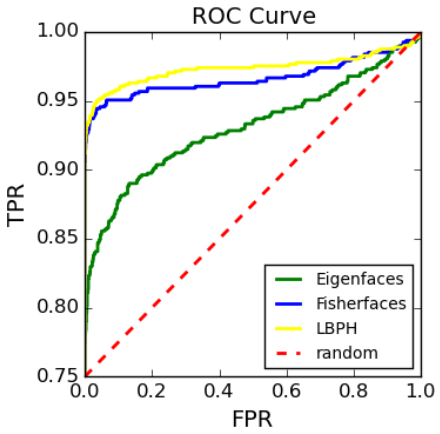


Figura 4. Curva ROC dos valores de similaridade para os métodos de reconhecimento testados.

vizinhos. A Figura 5 ilustra o LBP com uma vizinhança de 3x3.

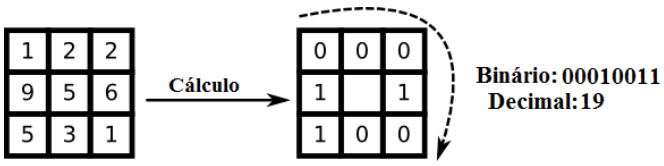


Figura 5. Operador básico LBP 3x3.

O LPB pode ser melhorado utilizando vizinhanças de diferentes tamanhos. A ideia é utilizar vizinhos em um círculo com um raio variável, como ilustrado na Figura 6. Quando as coordenadas de um ponto do círculo não correspondem a uma coordenada da imagem, é utilizada uma interpolação linear. A face é dividida em diversos blocos e para cada bloco é calculado o LBP de cada pixel e construído um histograma. Esses histogramas locais são concatenados em um único histograma global que representa a imagem da face. Para o reconhecimento é utilizado o classificador de vizinho mais próximo [15]. Após o período de login, um reconhecedor facial utilizando LPBH com raio 1 e 8 vizinhos é treinado com o modelo do usuário. Subsequentemente, para cada face detectada e normalizada com sucesso é feita uma comparação com o modelo, gerando um valor de similaridade.

E. Fusão de similaridade

Para cada quadro ao longo de um histórico de observações Z_t é calculada a probabilidade do sistema estar seguro, chamada de P_{seguro}, no momento t desse histórico. Cada observação $z_i \in Z_t$ corresponde a uma similaridade LBPH calculada entre a imagem atual e o modelo do usuário no instante i. Esta fusão de similaridades contínua é baseada no modelo proposto por Sim *et al.* [5], modificado por Pamplona *et al.* [16] e com uma pequena simplificação. Para garantir que

(a) Vizinha circular (8,1)

(b) Vizinha circular (8,2)

Figura 6. LBP com raio variável

o usuário atual continua sendo o usuário permitido, antigas observações são esquecidas sem a necessidade de manter um histórico de observações, apenas as probabilidades da última observação e da atual são mantidas.

A probabilidade do sistema estar seguro é calculado a todo momento, com ou sem observações, de acordo com as Equações 1, 2, 3 e 4. O sistema deve assumir que está seguro no momento do login, então P(seguro $\mid Z_0$) = 1 e P($\neg$seguro $\mid Z_0$) = 0, onde k é a taxa de decaimento que define quão rápido o sistema esquece antigas observações (*i.e.* P_{seguro} cai pela metade a cada k segundos sem observações), Δt é o tempo decorrido desde a última observação z_t, X = {seguro, $\neg$seguro} e u é o tempo da última observação antes de t, z_u.

$$P_{seguro} = \frac{2^{\frac{-\Delta t}{k}} \times P(seguro \mid Z_t)}{\sum_{x \in X} P(x \mid Z_t)} \quad (1)$$

$$P(seguro \mid Z_t) = P(z_t \mid x) + 2^{\frac{(u-t)}{k}} \times P(x \mid Z_u) \quad (2)$$

$$P(z_i \mid seguro) = 1 - \frac{1}{2}\left[1 + erf\left(\frac{similaridade - \mu_{seguro}}{\sigma_{seguro} \times \sqrt{2}}\right)\right] \quad (3)$$

$$P(z_i \mid \neg seguro) = \frac{1}{2}\left[1 + erf\left(\frac{similaridade - \mu_{\neg seguro}}{\sigma_{\neg seguro} \times \sqrt{2}}\right)\right] \quad (4)$$

Os parâmetros (μ_{seguro}, $\mu_{\neg seguro}$, σ_{seguro}, $\sigma_{\neg seguro}$) são respectivamente (30.0509, 95.6884, 24.8666, 30.7036), e foram obtidos através de experimentos com 100 imagens faciais de 5 indivíduos, onde cada uma foi selecionada para servir como modelo e todas as outras eram comparadas com esta. Para imagens da mesma pessoa do modelo, as similaridades pertencem ao grupo seguro. Para imagens de pessoas diferentes, não-seguro. Desde modo, μ e σ são as respectivas média e desvio padrão das similaridades para os estados seguro e não-seguro. A Figura 7 mostra o sistema em execução e sua respectiva probabilidade de estar seguro.

III. Resultados

Para os experimentos foram gravados 4 vídeos através do Kinect. Cada um desses vídeos possui 1000 quadros em que um usuário realiza o login e utiliza o computador normalmente, sem nenhum tipo de restrição imposta aos usuários sobre como eles deveriam utilizar o computador e sobre seu

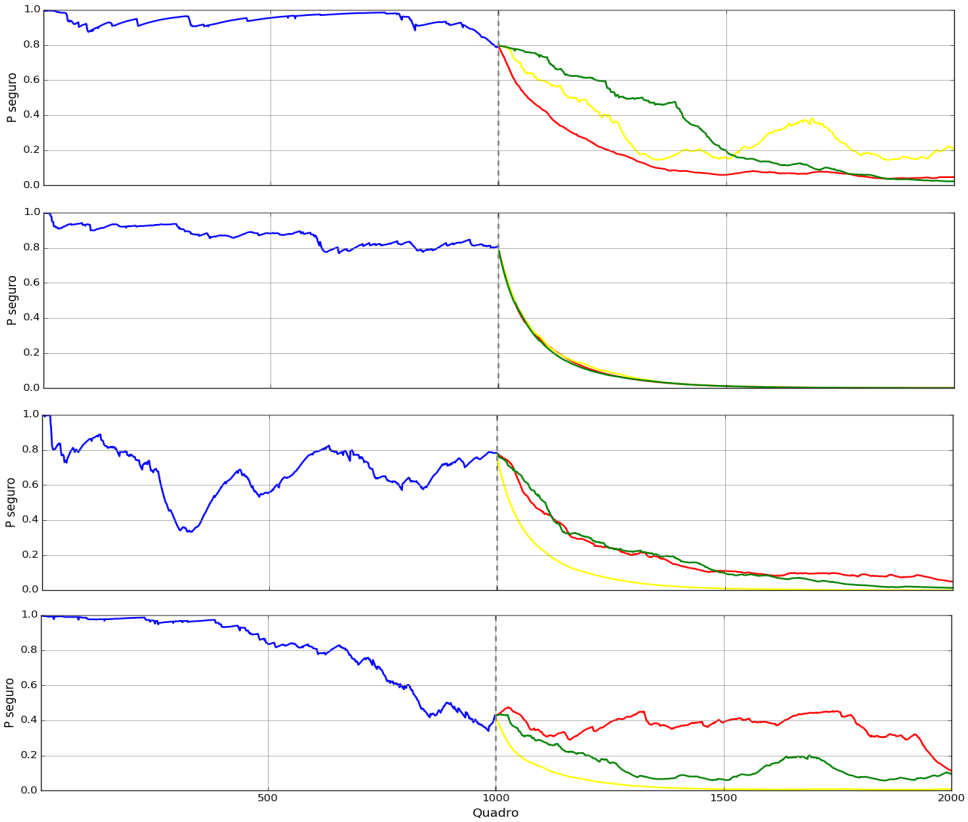
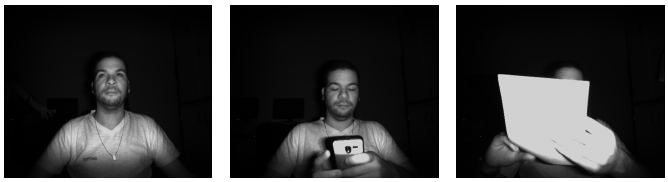


Figura 8. Cada gráfico é o resultado de um teste com um usuário. As linhas azuis representam os usuários autorizados nos primeiros 1000 quadros. As outras linhas representam os ataques de intrusos a partir do quadro 1000.

Figura 7. Execução do sistema. No topo é exibida a face normalizada e no canto inferior esquerdo à probabilidade do sistema estar seguro. Em cima da face é exibida sua similaridade.

comportamento, como ilustrado na Figura 9. Nenhum processamento paralelo ou em GPU foi utilizado nos experimentos.

Apenas no momento de login o usuário precisava olhar para a tela e permanecer imóvel. Esses vídeos foram utilizados como entrada para o sistema de autenticação contínua apenas



(a) (b) (c)

Figura 9. Exemplos de quadros em vídeo de teste mostrando: (a) utilização normal, (b) foco em outros objetos da cena e (c) oclusão.

com pessoas autorizadas. Para cada vídeo, foi concatenado ao seu final o início de cada outro vídeo restante para simular uma situação de ataque e verificar se o sistema detecta intrusos. No total foram 12 ataques realizados e os resultados são exibidos na Figura 8. Apesar de algumas sessões apresentarem uma queda no valor de P_{seguro} após o período de login, ele apresentou bom desempenho em simulações de ataque.

Como pode ser observado, na grande maioria dos quadros a probabilidade do sistema estar seguro com um usuário autorizado é maior do que a de um não autorizado. A curva ROC dos valores de P_{seguro} na Figura 10 mostra que o sistema consegue atualmente mais de 93% de acerto com uma taxa de alarme falso próxima de 7%. Isso significa que um usuário autorizado é reconhecido corretamente por cerca de 93% do tempo em que utiliza o sistema.

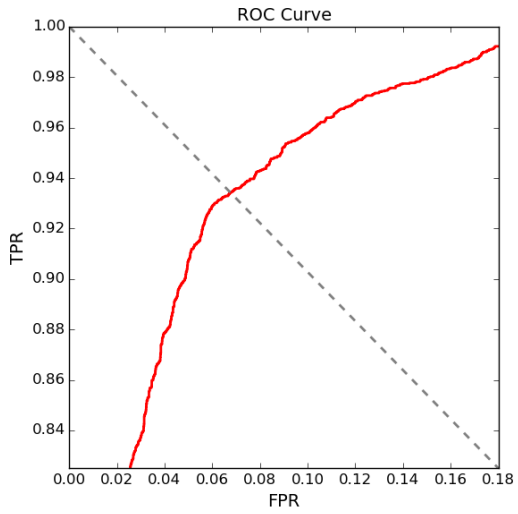


Figura 10. Curva ROC dos valores de P_{seguro}. No eixo x temos a taxa de positivos falsos (FPR, *False Positive Rate*) e no eixo y temos a taxa de positivos verdadeiros (TPR, *True Positive Rate*).

Analisando os resultados, vemos que o momento de captura de quadros no login é crucial no desempenho do sistema. O terceiro vídeo tem uma queda no valor de P_{seguro} que se deve à diferença de pose entre o login e o resto do vídeo, que pode conter fala com pessoas da cena, oclusões e interação com outros objetos da cena além do computador.

IV. Conclusão

Até onde sabemos, este é o primeiro sistema de autenticação contínua que utiliza faces em infravermelho para garantir que apenas o usuário permitido está utilizando o sistema. Apesar de usarmos o sensor Kinect One, o sistema pode ser utilizado com qualquer câmera que possua emissores de infravermelho. O sistema não precisa de cooperação do usuário, pois captura as imagens, detecta as faces, normaliza-as, e então calcula a similaridade e a probabilidade do sistema estar seguro, tudo de forma automática. Como as imagens em NIR são invariantes a iluminação ambiente, o sistema opera em qualquer condição de iluminação. Foram analisados 4000 quadros de usuários autorizados e 12000 quadros de tentativas de invasão, alcançando 93% de TPR e 7% de FPR.

Como trabalho futuro, pretendemos melhorar a normalização para evitar quedas na segurança do sistema com o usuário autorizado e implementar técnicas de treino dinâmico de modelo do usuário, onde, após o período de login, alguns quadros que atingirem uma alta probabilidade do sistema estar seguro serão inseridos no modelo do usuário para melhorar o desempenho à medida em que o sistema está operando.

Agradecimentos

Os autores gostariam de agradecer ao CNPq e à UFBA pelo suporte financeiro. Partes da pesquisa deste artigo usam a base de dados SCface de imagens faciais. Por isso, créditos são dados a Universidade de Zagreb, Faculdade de Engenharia Elétrica e Computação por prover a base de dados de imagens faciais.

Referências

[1] S. G. Kong, J. Heo, B. R. Abidi, J. Paik, and M. A. Abidir, "Recent advances in visual and infrared face recognition—a review," *Computer Vision and Image Understanding 97 (2005) 103–135*, vol. 97, p. 103–135, April 2004, issue 1.

[2] F. Agrafioti and D. Hatzinakos, "Ecg biometric analysis in cardiac irregularity conditions," *Signal, Image and Video Processing*, p. 3(4):329–343, 2009.

[3] D. Gunetti and C. Picardi, "Keystroke analysis of free text," *ACM Trans. Info. and System Security*, p. 8(3):312–347, 2005.

[4] J. Leggett, G.Williams, M. Usnick, and M. Longnecker, "Dynamic identity verification via keystroke characteristics," *Int'l Jrnl. of Man-Machine Studies*, p. 35(6):859–870, 1991.

[5] T. Sim, S. Zhang, R. Janakiraman, and S. Kumar, "Continuous verification using multimodal biometrics," *IEEE PAMI*, p. 9(4):687–700, 2007.

[6] Y. Adini, Y. Moses, and S. Ullman, "Face recognition: The problem of compensating for changes in illumination direction," *IEEE Trans. Pattern Analysis and Machine Intelligence*, vol. 19, no. 7, pp. 721–732, July 1997.

[7] S. Z. Li, R. Chu, S. Liao, and L. Zhang, "Illumination invariant face recognition using near-infrared images," *IEEE TRANSACTIONS ON PATTERN ANALYSIS AND MACHINE INTELLIGENCE*, vol. 29, no. 4, pp. 627 – 639, April 2007.

[8] T. Wei and X. Zhihua, "Infrared face recognition based on local binary pattern and multi-objective genetic algorithm," *Proceeding of the IEEE International Conference on Information and Automation Shenzhen*, pp. 359 – 362, June 2011.

[9] Z. H. Xie, J. Zeng, G. D. Liu, and Z. J. Fang, "A novel infrared face recognition based on local binary pattern," *Proceedings of the 2011 International Conference on Wavelet Analysis and Pattern Recognition*, pp. 55 – 59, July 2011.

[10] H. Maenga, H. C. Choia, U. Park, S. W. Leea, and A. K. Jaina, "Nfrad: Near-infrared face recognition at a distance," *Biometrics (IJCB), 2011 International Joint Conference on Biometrics Compendium, IEEE*, pp. 1 – 7, October 2011.

[11] D. A. Socolinskyt, L. B. Wolfft, J. D. Neuheiselt, and C. K. Eveland, "Illumination invariant face recognition using thermal infrared imagery," *Computer Vision and Pattern Recognition, 2001. CVPR 2001*, vol. 1, pp. I–527 – I–534, 2001.

[12] P. Viola and M. Jones, "Rapid object detection using a boosted cascade of simple features," *Conference on Computer Vision and Pattern Recognition (CVPR)*, pp. 511–518, 2001.

[13] M. Grgic, K. Delac, S. Grgic, and B. Klimpak, "Scface - surveillance cameras face database," *Multimedia Tools and Applications Journal*, vol. 51, no. 3, pp. 863–879, February 2011.

[14] S. Li, R. Chu, S. Liao, and L. Zhang, "Illumination invariant face recognition using near-infrared images," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 29, no. 4, April 2007.

[15] T. Ahonen, A. Hadid, , and M. Pietikainen, "Face recognition with local binary patterns," *Computer Vision - ECCV 2004*, vol. 3021, pp. 469–481, 2004.

[16] M. S. Pamplona, S. Sarkar, D. Goldgof, L. Silva, and O. Bellon, "Continuous 3d face authentication using rgb-d cameras," *Computer Vision and Pattern Recognition Workshops (CVPRW)*, pp. 64 – 69, June 2013.