DESENVOLVIMENTO DE UM PROTÓTIPO PARA CONTROLE DE ACESSO INTEGRANDO TECNOLOGIA *RFID* E RECONHECIMENTO FACIAL

José L. Bezerra [1], Danilo C. Cardoso[2], Açucena G. Parente[3], Layzan Leia S. Portela [4], Francisco Aldinei P. Aragão [5]
[1] Tecnólogo em Mecatrônica Industrial / IFCE Sobral-CE. [2] Tecnólogo em Mecatrônica Industrial / IFCE Sobral-CE. [3] Tecnóloga em Mecatrônica Industrial / IFCE Sobral-CE. [4] Tecnóloga em Mecatrônica Industrial / IFCE Sobral-CE.
[5] Prof. Me. Em Engenharia Elétrica / IFCE Sobral-CE
Email: j.linhares@outlook.com, dan.cardoso19@gmail.com, acucena.gois.p@gmail.com, layzan.p@gmail.com, aldinei@ifce.edu.br

Abstract— Radio frequency identification (RFID) technology has been widely adopted in access control systems. However, access to a certain environment and a guarantee of secure security of the RFID card and not of who, in fact, has authorization. Therefore, an access control system with RFID and facial recognition is proposed in this paper. Basically, the system identifies and recognizes a face of the user who makes use of the RFID card, denying access to an unmatched case. Three facial recognition algorithms were analyzed before implementation in prototype: Fisherfaces, Eigenfaces and 4SF. It was observed, mainly, the performance of the algorithms in a system of dynamic images for real-time recognition. The Fisherfaces algorithm presented the best results, with a high hit rate of more than 90%, being therefore implemented and shipped in a prototype in the laboratory.

Keywords— RFID Access Control, Facial Recognition, Fisherfaces, Eigenfaces, 4SF, Database.

Resumo—A tecnologia de identificação por rádio frequência (RFID) tem sido amplamente adotada em sistemas de controle de acesso. No entanto, o acesso à determinado ambiente é uma garantia de quem segura o cartão RFID e não de quem, de fato, possui autorização. Logo, um sistema de controle de acesso com RFID e reconhecimento facial é proposto neste trabalho. Basicamente, o sistema identifica e reconhece a face do usuário que faz uso do cartão RFID, negando o acesso caso ambos não combinem. Foram analisados três algoritmos de reconhecimento facial antes da implementação em protótipo: *Fisherfaces*, *Eigenfaces* e 4SF. Foi observado, principalmente, o desempenho dos algoritmos em um sistema de imagens dinâmicas para reconhecimento em tempo real. O algoritmo *Fisherfaces* apontou melhores resultados, com taxa acima de 90% na quantidade de acertos, logo, foi utilizado para implementação em protótipo de baixo custo no laboratório.

Palavras-chave— Controle de Acesso RFID, Reconhecimento facial, Fisherfaces, Eigenfaces, 4SF, Banco de dados.

1 Introdução

Com o advento de novas tecnologias, os sistemas de controle de acesso vêm adaptando-se às necessidades das novas gerações, de modo a garantir maior segurança dos usuários e/ou ambientes públicos e privados, como em edifícios governamentais, ambientes de segurança pública, empresas, universidades, escolas, residências, etc. Além disso, organizações governamentais em diversos países têm investido cada vez mais em sistemas de automação e segurança eletrônica, em virtude dos recentes ataques terroristas que afetam os mecanismos de segurança dos países mais desenvolvidos.

Atualmente, a maioria dos sistemas de controle de acesso utilizam identificação por rádio frequência (*Radio Frequency Identification* - *RFID*) ou através de biometria por impressão digital, entretanto, é crescente a demanda por outras tecnologias biométricas, como através da imagem da íris ou imagem da face (Battaglia, *et al.*, 2017; Ogechukwu, 2016).

Apesar da tecnologia *RFID* apresentar robustez para sistemas de controle de acesso, o *RFID* não fornece autenticação ao titular do cartão *RFID* (componente de identificação pessoal do usuário), uma vez que, qualquer indivíduo não autorizado, mas que detenha do cartão cadastrado, pode ter acesso consentido pelo sistema. Neste artigo, a identificação por rádio frequência é utilizada apenas como componente complementar e não como único sistema de identificação e acesso.

Quanto aos sistemas biométricos, compreendem dispositivos de captura de informação biométrica, que através de uma base de dados e técnicas de *software*, realizam a manipulação da informação (normalmente imagens pré-processadas), identificando usuários conforme suas características físicas ou comportamentais. Entretanto, as tecnologias biométricas convencionais são passíveis à falhas e/ou fraudes, muito em virtude da baixa qualidade das imagens coletadas para extração das características biométricas (Ogechukwu, 2016; Santhosh, S. 2014).

Apesar de promissora, a biometria enfrenta desafios que necessitam ser contrabalançados para não resultar em interpretações falsas e aplicações indevidas. Dentre os principais desafios constam: excesso de informação, paradoxo da população, privacidade, intrusividade, ruído, vulnerabilidade e classificação (Vertamatti, 2011). Desta forma, observa-se que a biometria precisa superar obstáculos para se tornar um padrão de segurança antifraude.

O principal problema da detecção de faces consiste em determinar se a imagem arbitrária representa uma face humana ou não, de modo a retornar as coordenadas da face reconhecida. Como solução, a recente literatura da área propõe técnicas de visão computacional e reconhecimento de padrões que frente aos avanços dos sistemas de computação, possibilitam respostas rápidas, considerando a relação de custo entre velocidade da informação e limitação temporal.

Para minimizar falhas de segurança, este trabalho propõe uma solução de baixo custo baseada na integração de um sistema *RFID* com um sistema de biometria facial. O protótipo foi projetado, desenvolvido e instalado em ambiente de laboratório. Para o protótipo, foram avaliadas metodologias e/ou técnicas de identificação e reconhecimento facial que melhor se adequassem a aplicação pretendida. O algoritmo de melhor desempenho foi embarcado na plataforma *Raspberry Pi* (processador *Broadcom BCM2837 quad core SoC, ARM Cortex-A53*).

Considerando o exposto, este artigo foi organizado da seguinte forma: (a) Apresentação dos principais componentes e características de um sistema de Identificação por Radiofrequência; (b) Revisão bibliográfica dos principais algoritmos de reconhecimento facial; (c) Descrição completa do sistema proposto; (d) Apresentação dos resultados; (e) Conclusão.

2 Sistema de Identificação por Radiofrequência (RFID)

A identificação por rádio frequência consiste em uma tecnologia que utiliza ondas de rádio para localizar e/ou identificar objetos. A identificação ocorre por consequência da comunicação entre um dispositivo leitor e *tags RFID*.

Para aplicação em sistema de controle de acesso, os principais componentes consistem (figura 1): leitor (ou interrogador), *tag RFID* (ou etiquetas) e *software* de aplicação com sistema de banco de dados (Finkenzeller, 2010).

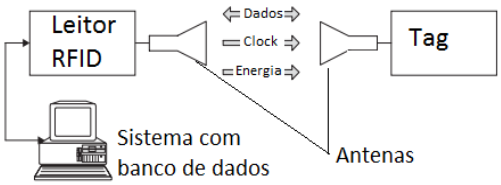


Figura 1 - Componentes do sistema RFID.

2.1 Tag RFID

Para cada aplicação pretendida, existe uma multiplicidade de *tags* com diferentes formas e tamanhos. No entanto, todas são compostas por três elementos principais: (i) substrato, que consiste na cobertura ou suporte da antena; (ii) antena; (iii) microchip dedicado, que integra funções de processamento, memória, e algumas vezes, sensores e dispositivos de segurança (Andía, *et al*., 2018, Khattab *et al.*, 2017).

As *tags* mais indicadas para aplicação proposta consistem nas *tags* de característica passiva, tendo em vista a necessidade de proximidade com o dispositivo leitor, além disso, apresentam baixo custo em relação as *tags* semi-passivas e ativas.

As *tags* passivas são alimentadas por ondas eletromagnéticas emitidas pela antena do dispositivo leitor/interrogador, logo, só conseguem enviar informações quando houver solicitação do mesmo. O processo é relativamente simples, a antena da *tag* captura ondas eletromagnéticas do interrogador e utiliza parte da energia induzida para alimentação da própria *tag*, bem como, para responder às solicitações do interrogador. (Dardari, *et al.*, 2016; Finkenzeller, 2010).

2.2 Leitor RFID (interrogador)

Com base no projeto e na tecnologia utilizada na fabricação do leitor, também denominado de interrogador, o dispositivo, tipicamente, é constituído por um módulo de radiofrequência, uma unidade de controle e uma unidade de acoplamento (antena do leitor). Além disso, muitos leitores são equipados com alguma interface adicional (*ethernet*, RS-232, etc) para comunicação com outro sistema, como computador ou unidade de controle de algum equipamento (Andía, *et al*., 2018).

As principais funções do interpretador são: a) ativar a *tag*; b) organizar a sequência de bits de comunicação com a *tag*; c) realizar a transferência de dados entre a *tag* e a aplicação de *software.* A figura 2 apresenta uma descrição básica do princípio de funcionamento do interrogador em relação ao *software* e as *tags RFID*.

Figura 2 - Fluxo de dados e comunicação mestre-escravo.

Observa-se que para estabelecer fluxo de dados é necessário existir uma relação mestre-escravo à partir do *software* (mestre) com solicitações de resposta para o interrogador (escravo), e consequentemente, do interrogador (mestre) com solicitações de resposta para a *tag RFID* (Finkenzeller, 2010).

3 Algoritmos de Reconhecimento Facial

Conforme literatura da área (Jin; Wang, 2017; Jaturawat, Phankokkruad, 2016; Ghorbel, 2016), existem diferentes metodologias e/ou técnicas para identificação e reconhecimento facial. Cada metodologia procura diferentes maneiras de extrair atributos da face e podem ser classificados em três grandes grupos:

- **Métodos geométrico:** utilizam informações dos olhos, nariz e boca para extrair informações em vetores para criação de um modelo da face.

- **Métodos holístico:** utilizam todos os *pixels* da imagem para extrair características do

rosto que possam gerar diferenças suficientes com outras imagens.

- **Método híbrido:** combinam técnicas distintas para gerar resultados mais significativos.

Neste artigo foram estudadas três técnicas de reconhecimento facial: *Eigenfaces*, *Fisherfaces* e *4SF* (*Spectrally Sampled Structural Subspace Features*). A finalidade do estudo consistiu em determinar a melhor técnica para aplicação proposta, realizando testes com imagens estáticas e imagens dinâmicas.

3.1 Eigenfaces fracionário

A técnica *Eigenfaces* é um método de extração de recursos utilizado para detecção e reconhecimento facial (Ghorbel, 2016). A técnica consiste num método de redução de dimensionalidade baseado em *PCA* (*Principal Component Analysis*), onde os coeficientes obtidos consistem numa representação reduzida dos dados originais sobre um novo espaço.

O algoritmo *Eigenfaces* consiste em quatro etapas: 1) Computação da matriz de covariância dos dados concatenados 2) Computação dos autovalores e vetores próprios da matriz de covariância. 3) Seleção dos autovetores com os valores máximos mais altos para formar o modelo da face. 4) Projeção dos dados originais em um novo modelo da face.

O *Eigenfaces* fracionário (Nasrollahi, 2012) é uma extensão do *Eigenfaces* baseado na teoria da matriz de covariância fracionada (European Commission, 2012), definida conforme equação 1.

$$L^r = \frac{1}{n}\sum_{j=1}^{m}\begin{bmatrix}(x_{1j})^r - (\psi_j)^r \\ \vdots \quad \ddots \quad \vdots \\ (x_{nj})^r - (\psi_j)^r\end{bmatrix}\begin{bmatrix}(x_{1j})^r - (\psi_j)^r \\ \vdots \quad \ddots \quad \vdots \\ (x_{nj})^r - (\psi_j)^r\end{bmatrix}^T \quad (1)$$

Onde n é o número de imagens m é número de características (número de pixels da face), x_i é a imagem da face e ψ é a média da imagem da face.

A computação dos autovetores é feita de acordo com a seguinte equação:

$$e_i = \frac{1}{(n\lambda_i)^{1/2}}[((X_1)^r - (\psi)^r),\ \ldots,\ ((X_n)^r - (\psi)^r)]e_i' \quad (2)$$

O treinamento é baseado numa transformação fracional do modelo da face para obter os coeficientes ω_i

$$\omega_i = E^T((X_i)^r - (\psi)^r) \quad (3)$$

Porém, uma dificuldade da técnica consiste quando submetida a variação de iluminação, pois como é baseada no *PCA*, a mesma não apresenta bons resultados para classificação sob tal condição (Ferreira, Carvalho, 2017).

3.2 Eigenfaces

A técnica pretende a maximização das dimensões entre duas ou mais classes de dados (Ferreira, Carvalho, 2017). A equação 4 demonstra como definir as características de um vetor *X* dentro de um conjunto de amostras de uma classe.

$$X = \{X1, X2, X3, \ldots, Xc\} \quad (4)$$

Onde as amostras são definidas como:

$$Xi = \{x1, x2, x3, \ldots, xn\} \quad (5)$$

As matrizes de dispersão *Sw* e S_B podem ser calculadas como segue:

$$S_{B=} \sum_{i=1}^{c} Ni\,(\mu i - \mu)\,(\mu i - \mu)^T \quad (6)$$

$$S_{W=} \sum_{i=1}^{c} \sum_{xj \in Xi} (xj - \mu i)\,(xi - \mu i)^T \quad (7)$$

O valor μ representa o valor médio, Ni o número de amostras da classe *i* e μi a média calculada da classe *i*, onde:

$$i \in \{1, 2, \ldots, c\} \quad (8)$$

$$\mu_i = \frac{1}{|Xi|}\sum_{xj \in Xi} x_j \quad (9)$$

Para melhorar a projeção de *W* o algoritmo de *Fisher* otimiza a separação de classe, através da equação 12:

$$W_{opt} = argmaxw\,\frac{|W^T S_B W|}{|W^T S_W W|} \quad (10)$$

3.3 4SF

O algoritmo 4SF consiste numa técnica que utiliza vários subespaços discriminativos para realizar o reconhecimento facial. O algoritmo trabalha juntamente a outros algoritmos em cascata, de detecção facial, detecção dos olhos e de correção da imagem, podendo ser modificado. O processo de reconhecimento do algoritmo *4SF* inicia com a detecção da face, seguido da detecção dos olhos para normalização de posição e escala da face (Klare, Burge, Klontz, Vorder Bruegge, Jain, 2012). O algoritmo faz a representação do conjunto de imagens através de histogramas de padrões binários locais. Depois é usado o PCA para cada imagem onde é feita uma

decomposição com variância de 98% (Klare, Burge, Klontz, Vorder Bruegge, Jain, 2012). As amostras são ponderadas aleatoriamente, em seguida o algoritmo *LDA* é aplicado para o aprendizado, utilizando cada amostra aleatória como modelo. Por último, os descritores compostos são convertidos em um vetor de distância euclidiana para melhorar a precisão do reconhecimento facial. A distinção entre duas faces é calculada através da soma das distâncias euclidianas de cada subespaço.

4 Sistema Proposto

4.1 Protótipo do sistema RFID

Para o protótipo, foi desenvolvido um *software* de cadastro e verificação de usuários que juntamente à um Sistema de Gerenciamento de Banco de Dados Relacional (SGBDR) armazena informações de data e hora de acesso. Como interface de comunicação entre o *software* e *hardware* adotou-se a comunicação *bluetooth*, porém, é importante mencionar a limitação.

A figura 3 apresenta o modelo do sistema sem a integração com o dispositivo de reconhecimento facial. O item a) corresponde ao *software* com banco de dados; item b) refere-se ao *hardware* desenvolvido para identificação por radiofrequência; item c) a trava elétrica utilizada.

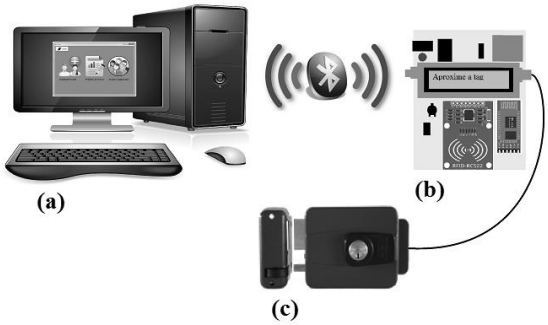


Figura 3. Modelo do sistema de identificação por radiofrequência.

A tabela 1 apresenta os principais componentes do *hardware* desenvolvido.

Tabela 1. *Hardware* desenvolvido.

Item	Principais Componentes	Características em operação (testado em laboratório)
1	Microcontrolador PIC18F4550	Freq.: 48 MHz, barramento de *8 bits; Consumo:* 100 mA; alimentação: 5.0 V.
2	Bluetooth HC-05	Freq.: 2,4 GHz; Consumo (conectado): 8 mA; Consumo (pareado): 35 mA Alimentação: 3.3 V.
3	Leitor chip Mfrc522	Freq.: 13,56 MHz; Consumo: 15 mA; Alimentação: 3.3 V.

4.2 Protótipo do sistema de biometria

Como mencionado anteriormente este trabalho propõe um sistema de controle de acesso combinando tecnologia *RFID* e reconhecimento facial de modo a garantir dois níveis de segurança.

A figura 4 apresenta o protótipo desenvolvido em laboratório. O item 1 corresponde a plataforma *Raspberry Pi* utilizada para embarcar os algoritmos de identificação e reconhecimento facial em tempo real, enquanto o item 2 consiste no sistema de radiofrequência desenvolvido.

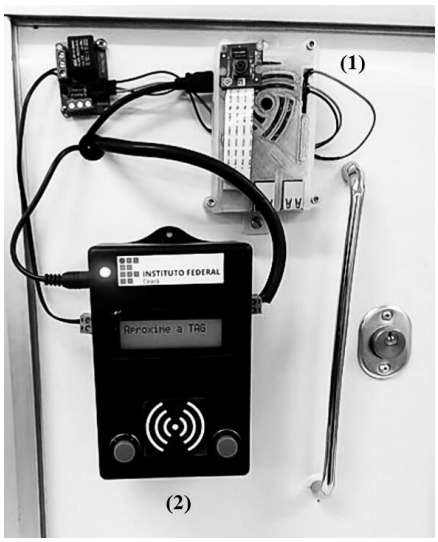


Figura 4. Protótipo do sistema de controle de acesso.

O diagrama simplificado e em blocos da plataforma *Raspberry Pi* é apresentado na figura 5.

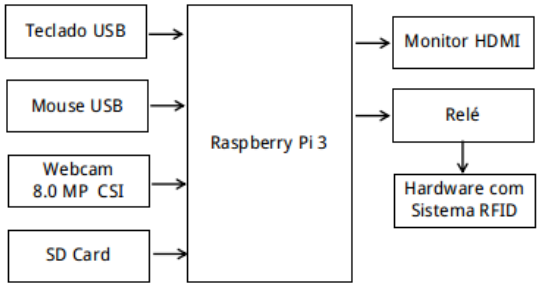
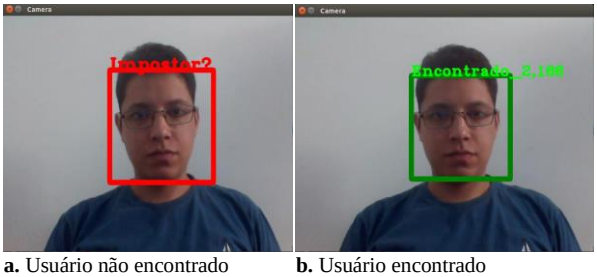


Figura 5. Protótipo do sistema de controle de acesso.

As saídas obtidas, a partir dos algoritmos estudados, são observadas na figura 6, através de um monitor *HDMI*.



a. Usuário não encontrado **b.** Usuário encontrado

Figura 6. Saídas obtidas do sistema

4.3 Operação do sistema de biometria

A identificação e reconhecimento da face opera, basicamente em quatro etapas (figura 7):

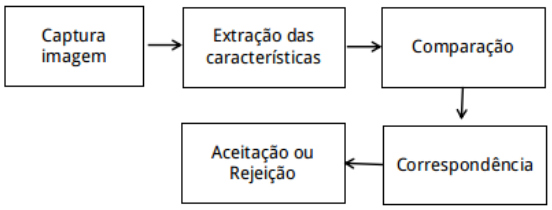


Figura 7. Fluxograma de operação do sistema de biometria

- **Etapa 1 (Captura):** Uma amostra física e/ou comportamental é capturada através de uma câmera, durante o cadastro e também no processo de identificação ou verificação
- **Etapa 2 (Extração):** Os dados originais são extraídos do exemplo e um modelo é criado.
- **Etapa 3 (Comparação):** O modelo é então comparado com uma amostra existente no banco de dados.
- **Etapa 4 (Correspondência):** O sistema decide se os recursos extraídos das novas amostras correspondem ou não, e, portando, aceita ou rejeitando a nova amostra.

4.4 Operação geral do sistema proposto

O fluxograma completo do sistema de controle de acesso é apresentado na Figura 8. Basicamente, o sistema solicita aproximação da *tag* cadastrada, após encontrar a *tag*, o mesmo compara as informações visuais coletadas em tempo real com as informações armazenas em um banco de dados no *Raspberry PI*. Todo processo de biometria (identificação e reconhecimento da face) ocorre por um período de aproximadamente três segundos, logo após a verificação do cartão *RFID*.

Enquanto o sistema de biometria compara as amostras coletadas em tempo real com as imagens armazenadas em banco de dados, o sistema de identificação por radiofrequência verifica a identificação única do cartão cadastrado na memória *EEPROM* do microcontrolador e/ou banco de dados. O acesso é autorizado quando, tanto o sistema *RFID*, quanto o sistema de biometria facial identificam o usuário cadastrado. Após autorização, uma aplicação de *software* armazena em banco de dados, as informações de data e hora do acesso.

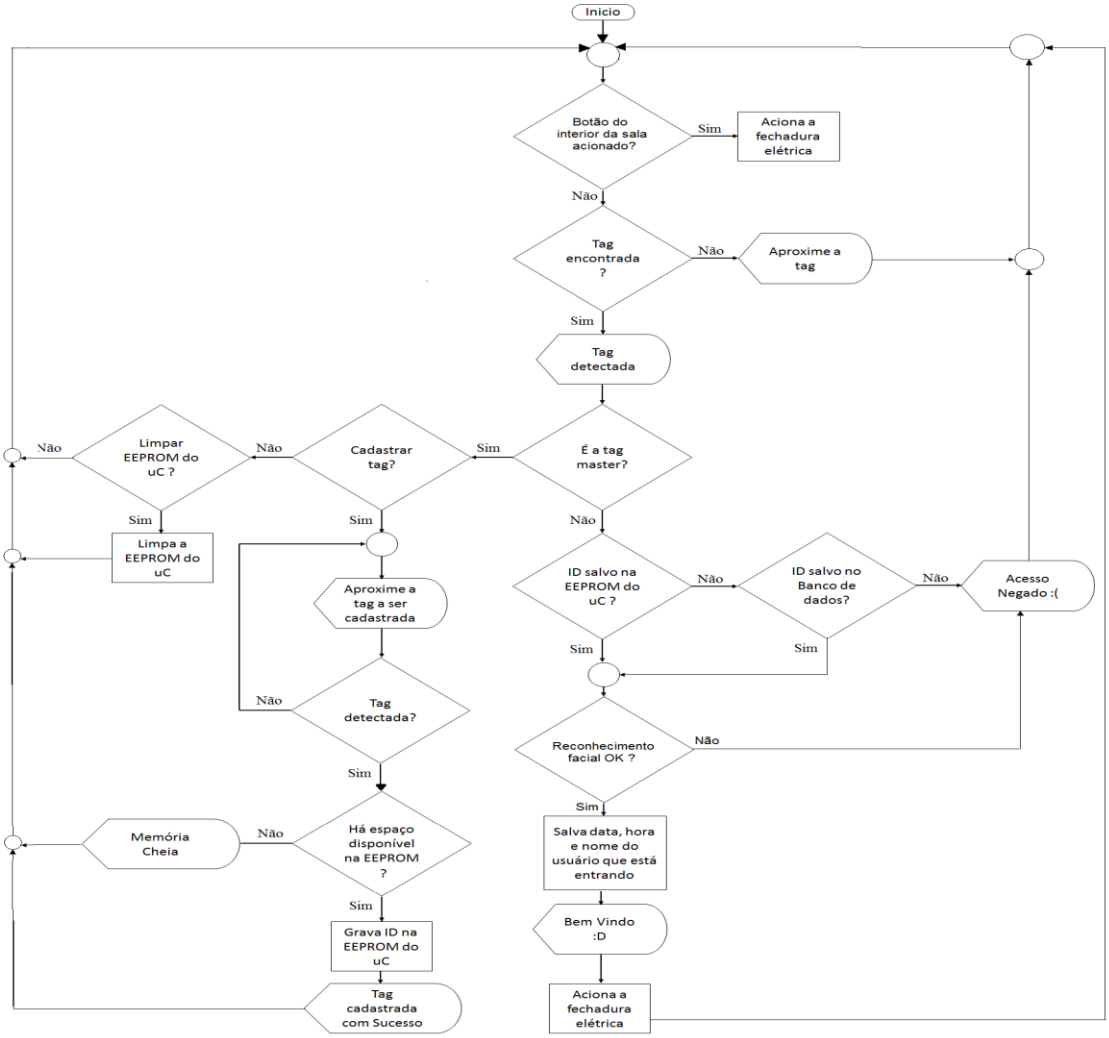


Figura 8. Fluxograma do Sistema proposto

5 Resultados

Para validar os algoritmos foram utilizados dois bancos de imagens, o primeiro, do *Center for Signal and Image Processing at Georgia Institute of Technology*, com 750 imagens de 50 indivíduos, sob diversas condições de iluminação e posição, muito comum para teste de algoritmos de reconhecimento facial. O segundo banco de dados foi elaborado com imagens de usuários do laboratório de eletrônica, contendo 52 imagens de 4 pessoas distintas. Dessa forma, foram organizados dois modelos de testes, para comparação de imagens e avaliação de resultados.

O modelo ‘A’ está descrito na tabela 2 e o modelo ‘B’ na tabela 3.

Tabela 2. Modelo ‘A’ de configuração de testes.

Conjunto de dados	N° de imagens por pessoa	Lógica de seleção das imagens
Banco de imagens para consulta	5	Imagens aleatórias do conjunto de treinamento
Imagens Alvo	2	Imagens exclusivas
Treinamento	13	Imagens do conjunto original

Tabela 3. Modelo ‘B’ de configuração de testes.

Conjunto de dados	N° de imagens por pessoa	Lógica de seleção das imagens
Banco de imagens para consulta	2	Imagens aleatórias do conjunto de treinamento
Imagens Alvo	1	Imagens exclusivas
Treinamento	13	Imagens do conjunto original

Os resultados obtidos para o modelo ‘A’ são apresentados nas figuras 9 e 10 respectivamente.

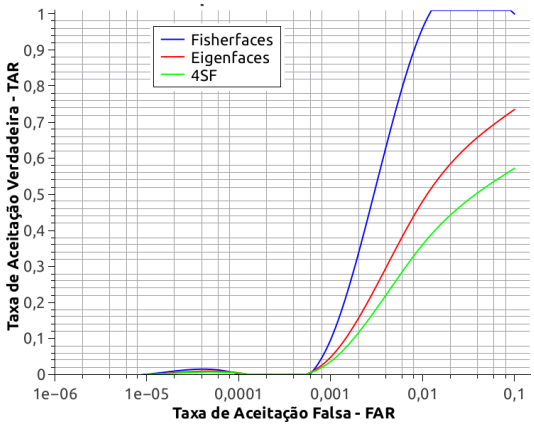


Figura 9. Taxas de aceitação dos algoritmos *Fisherfaces*, *Eigenfaces* e *4SF* para o modelo 'A'

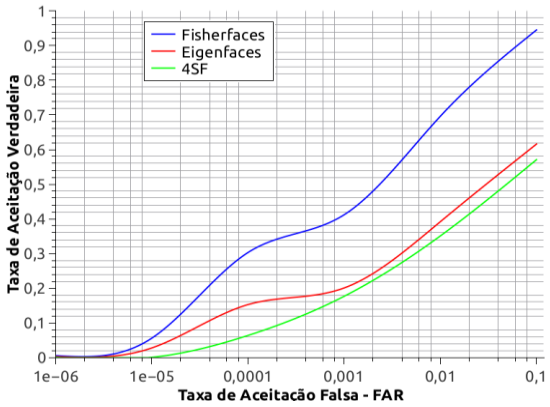


Figura 10. Taxas de aceitação dos algoritmos *Fisherfaces*, *Eigenfaces* e *4SF* para o modelo 'A'

Também são apresentados os resultados para o modelo 'B'.

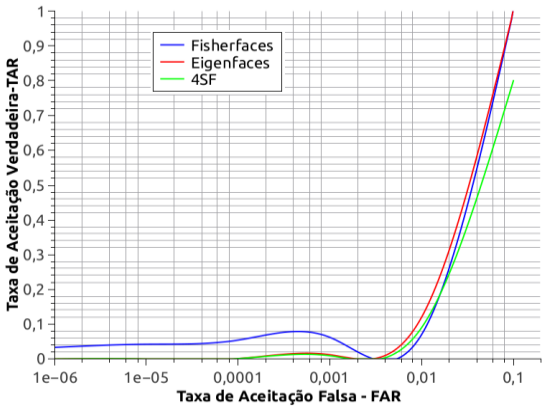


Figura 11. Taxas de aceitação dos algoritmos *Fisherfaces*, *Eigenfaces* e *4SF* para o modelo 'B'

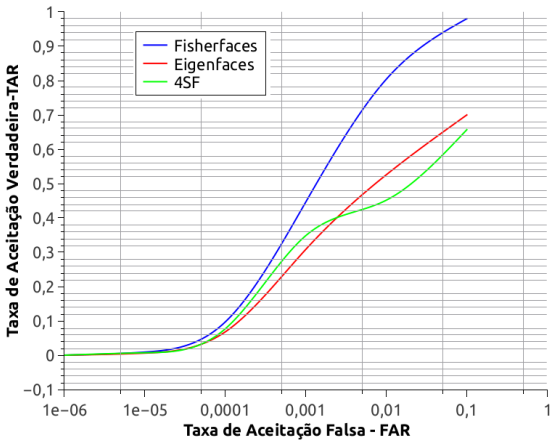


Figura 12. Taxas de aceitação dos algoritmos *Fisherfaces*, *Eigenfaces* e *4SF* para o modelo 'B'

6 Conclusão

Liste suas conclusões nesta seção, em vez de simplesmente relatar o que foi feito.

Agradecimentos

Mencione aqui seus agradecimentos às agências de fomento e aos colaboradores do trabalho.

Referências Bibliográficas

Andía, G., Duroc, Y., Tedjini, S. (2017) Non-linearities in Passive RFID Systems - Third Harmonic Concept and Applications, Great Britain and the United States by ISTE Ltd.

Battaglia, F., Iannizzotto, G., Bello, L. (2017) A Person Authentication System Based on RFID Tags and a Cascade of Face Recognition Algorithms. IEEE Transactions on Circuits and Systems for Video Technology, Vol. 7, No. 8, August.

Nasrollahi, K. and Moeslund, T. B. (2011). Extracting a good quality frontal face image from a low-resolution video sequence," IEEE Trans. Circuits Syst. Video Technol., vol. 21, no. 10, pp. 1353–1362, Oct.

European Commission (2012): Art. 29 Working Party, Working Document on Biometrics 00720/12/EN WP 193, 2012.

Dardari, D., Decarli, N. , A. Guerra and F. Guidi (2016), The future of ultra-wideband localization in RFID. IEEE International Conference on RFID (RFID), Orlando, FL, 2016, pp. 1-7.

Finkenzeller, K. (2010), RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification., 3rd ed. Wiley.

Ghorbel, A., Tajouri, I., Aydi, W., Masmoudi, N. A (2016). Comparative study of GOM, uLBP, VLC and fractional Eigenfaces for face recognition. IEEE IPAS'16 International Image Prossessing Applications and System Conference.

Jin, S., Wang, H. (2017) Automatic Modulation Recognition of Digital Signals Based on Fisherface. IEEE International Conference on Software Quality, Reliability and Security.

Jaturawat, P., Phankokkruad, M. (2016). An Evaluation of Face Recognition Algorithms and Accuracy based on Video in Unconstrained Factors. 2016 6th IEEE International Conference on Control System, Computing and Engineering, pp. 25–27 November.

Khattab, A., Jeddi, Z., Amini, E., Bayoumi. M. (2017) RFID Security - A Lightweight Paradigm - Analog Circuits and Signal Processing, Springer International Publishing.

Ogechukwu, N. L. (2016). Effective Statistical-Based and Dynamic Fingerprint Preprocessing Technique. IET Biometrics, The Institution of Engineering and Technology, Vol. 6, pp. 9-18.

Santhosh, S. (2014). Design and Development of a Security Module with Inbuilt Neural Network Methodologies and Advanced Technique on Fingerprint Recognition. IEEE/ICCPCT International Conferece on Circuit, Power and Computing Technologies.

Vertamatti, R. (2011). Assimetria Humana no Reconhecimento Multibiométrico. Tese, Escola Politécnica da Universidade de São Paulo. Engenhara em Sistemas Eletrônicos.