Fechadura Baseada em Reconhecimento Facial Via Dispositivos Móveis Android

Arthur Trindade Abreu de Gusmão, Agostinho Luiz da Silva Castro e Ronaldo de Freitas Zampolo

***Resumo*— Na busca por maior segurança no dia a dia, fechaduras são utilizadas como meio de se garantir a propriedade privada. Fechaduras convencionais apresentam falhas por não identificarem o usuário que utiliza o sistema. Este trabalho propõe uma solução para o problema na forma de uma fechadura ativada mediante reconhecimento facial, baseado em OpenCV e no uso de *eigenfaces*. O processamento é realizado em smartphone que se comunica com um circuito de ativação através de Bluetooth. Resultados preliminares relativos ao desempenho do sistema proposto demonstram seu potencial para uso prático.**

***Palavras-Chave*— Reconhecimento facial, OpenCV, eigenfaces, Arduino, Bluetooth, Android.**

***Abstract*— Seeking to improve the security in daily life, locks are used as a way to ensure private property. Common locks are flawed by not identifying the users who unlock them. This paper proposes a solution in the form of an electric lock activated by facial recognition based on eigenfaces and OpenCV. The processing is performed on a smartphone that communicates with an activation circuit through Bluetooth. Preliminary results regarding the performance of the proposed system show its feasibility.**

***Keywords*— Face recognition, OpenCV, eigenfaces, Arduino, Bluetooth, Android.**

I. Introdução

A definição mais genérica de segurança é de um estado de percepção de proteção, de se estar livre de riscos, situação em que não há nada a temer. De acordo com o Human Developement Report de 1994 [1], a palavra *segurança* indica, em âmbito internacional, a salvaguarda de fronteiras e políticas externas de países; para cidadãos comuns, o termo está fundamentalmente relacionado aos riscos do dia a dia: garantia de alimentação, estabilidade no emprego e proteção contra a criminalidade. Vinte anos depois da publicação do referido relatório, o problema da violência é percebido por grande parte da população como grande ameaça à segurança. No caso da América Latina, os altos índices de violência restringem significativamente o modo de vida das pessoas. A versão de 2014 do relatório supracitado [2] reforça esta ideia, dando como exemplo o medo de se deslocar à noite pelas cidades, o que prejudica, dentre vários outros aspectos, o comércio noturno. Baseado neste contexto, tem-se o conceito de controle de acesso. Bai e Zeng [3] definem controle de acesso como o ato de regular o acesso (a um objeto, recurso ou lugar) a partir de um sujeito mediante o uso de um instrumento. A ideia de segurança advinda a partir de controle de acesso tem sido amplamente aplicada no cotidiano e está presente em casas, veículos, contas bancárias e serviços virtuais. O objetivo é garantir a propriedade privada, integridade e privacidade.

Diversos trabalhos técnicos e científicos destacam a preocupação com a segurança. Por exemplo, o controle de recursos de computadores compartilhados em rede é citado por [3]. Nesse trabalho, é ressaltado o quanto o controle de acesso é importante na implementação de segurança em sistemas computacionais. Para o controle de acesso de locais físicos, as fechaduras são soluções convencionais. Normalmente anexadas a portas ou caixas, as fechaduras impedem mecanicamente o movimento de uma parte móvel. Como consequência, ao se realizar o trancamento por uma fechadura, limita-se o acesso ao portador de uma chave específica. A fechadura mais antiga conhecida, conforme [4], foi encontrada nas ruínas do palácio de Khorsabad, onde hoje se encontra o Iraque. Acredita-se que tenha mais de 4000 anos de existência. Esse tipo de fechadura consistia de um bastão de madeira perfurada, que mantinha a porta segura em suportes que impediam o movimento. A chave era uma larga peça de madeira com palitos em sua extremidade combinando com os furos da fechadura que, quando encaixados, permitiam que o bastão fosse movimentado. Existem muitos outros tipos de fechaduras, sendo a mais comum a de segredo mecânico. De forma similar à fechadura encontrada em Khorsabad, uma chave convencional, cujas saliências combinem com as da fechadura, permite o movimento de uma trava presente na porta. O uso de chave é altamente aceito pela sociedade e está presente na maioria das casas, não depende de energia elétrica, sendo simples e rápido de usar. Em contrapartida, todo o conceito é baseado na ideia de que o portador da chave está autorizado a entrar, sem tentar identificar quem é o portador da chave, criando problemas, por exemplo, caso a chave seja roubada ou perdida. Outro modelo de fechadura é a eletromagnética, em que um impulso elétrico ativa uma bobina magnética que libera a peça que bloqueia a movimentação da porta. Essa classe de fechadura permite que vários tipos de chave sejam utilizados, tais como: cartões magnéticos, senhas ou biometria. Dentre as técnicas de identificação biométricas, o reconhecimento facial é uma das menos invasivas, quando comparada a outras modalidades que envolvem contato, geram desconforto ou são potencialmente prejudiciais para o ser humano, como, por exemplo, a leitura de retina, cujo processo envolve direcionar um feixe de luz ao olho. O reconhecimento facial, devido às suas características de conforto e naturalidade, possui grande aceitação entre a população, conforme citado em [5].

Arthur T. A. Gusmão, Agostinho L. S. Castro e Ronaldo F. Zampolo, Faculdade de Engenharia da Computação e Telecomunicações, Universidade Federal do Pará, Belém-PA, Brasil, Emails: arthur.gusmao@itec.ufpa.br, agcastro@ufpa.br, zampolo@ufpa.br

Este trabalho tem como objetivo implementar um sistema de fechadura eletrônica ativada através do reconhecimento facial, sendo composto de hardware para acionamento da fechadura e aplicação para dispositivos móveis portadores de sistema operacional Android. O hardware controla o estado da fechadura eletrônica, cujo comando de ativação é enviado através de sinal de rádio segundo padrão Bluetooth. Por sua vez, a aplicação para smartphones Android tem como tarefa realizar a captura de imagens do rosto do usuário, executar o reconhecimento facial e se comunicar com o circuito da fechadura informando o resultado da identificação que resultará ou não na autorização ao portador do aparelho.

O restante deste texto está organizado como segue. A Seção II disserta sobre fechaduras inteligentes. A arquitetura e as características do sistema empregadas no trabalho são apresentadas na Seção III, bem como uma simplificada avaliação de desempenho do sistema implementado na Seção IV. A Seção V apresenta as Considerações Finais.

II. Fechaduras Inteligentes

Fechaduras inteligentes, diferentemente das convencionais, têm capacidade de tomada de decisão. Isto quer dizer, que a fechadura tem o poder de autorizar a entrada baseado em alguma lógica programada e realizar outras tarefas a partir do destravamento da porta. Isto é muito utilizado, por exemplo, em hotéis. Hóspedes recebem cartões magnéticos ou RFID (Radio-Frequency IDentification) que liberam o acesso para seus quartos. Os cartões são genéricos, e habilitados para funcionar em determinado quarto por certo período de tempo. Caso o hóspede perca seu cartão, este perderá a funcionalidade quando o período de hospedagem acabar, ou pode ser desabilitado do sistema quando o balconista do hotel for notificado.

Existem diversas propostas de fechaduras elétricas, algumas com e outras sem inteligência. Em [6], [7], travas eletromagnéticas são propostas utilizando um PIC 16F87XA para controlar seus circuitos de ativação. Ambos os trabalhos são bem similares entre si, diferenciando-se na forma de ativação de seus circuitos, tendo o primeiro se baseado em um dispositivo que utiliza rádio para comunicação, enquanto o segundo utiliza tecnologia RFID na forma de cartões. Ambos requerem que o usuário seja portador de um objeto para fazer a abertura da porta. Em contrapartida, Chang et al. [8] propõem um sistema de porta inteligente que é capaz de controlar a posição de uma câmera a fim de realizar uma boa captura de imagem do usuário e fazer uma identificação visual para a liberação ou não da porta. Este sistema é de alto desempenho, com uma placa de FPGA (Field Programmable Gate Array) programada para fazer cálculos de reconhecimento facial e detecção de posição do usuário baseada no som. Toda a solução depende de um hardware montado especificamente para a tarefa, aumentando o custo de implementação. Em sua conclusão, o próprio artigo sugere o uso de smartphones como possibiidade para redução de custo do sistema.

Urien [9] propõe um sistema que usa Near Field Communication (NFC) em smartphones para fazer a ativação de portas. A abordagem envolve um leitor de NFC, que faz uma requisição a um servidor contendo chaves criptográficas, sendo

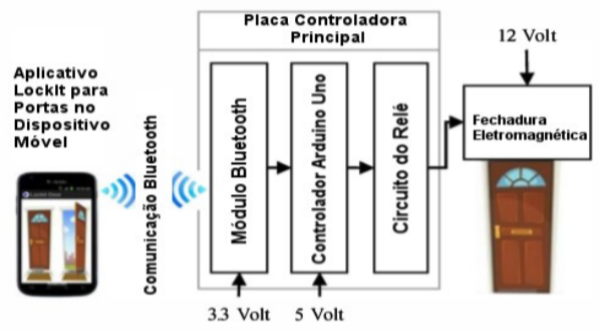

Fig. 1. Arquitetura de controle de fechadura para dispositivos móveis usando Bluetooth (Adaptado de [10]).

essa entidade a realizadora da requisição para um computador que, então, ativa da porta por uma interface USB. Apesar da maior segurança ao delegar o trabalho de validação do celular para um servidor externo, o sistema requer conexão com a internet e que um computador esteja sempre ligado, e conectado fisicamente com o circuito de ativação da porta, o que pode ser inconveniente.

Um exemplo de estrutura bem próxima da adotada no presente trabalho pode ser visto no artigo de Shamsuddin et al. [10]. Nesta publicação, os autores criaram uma aplicação móvel para dispositivos Android que controla uma fechadura elétrica, visando ajudar cadeirantes a se locomoverem em ambientes fechados. No referido artigo, também é defendido o uso de tecnologia Bluetooth, pela sua segurança e ampla disponibilidade em aparelhos celulares comercializados. O aplicativo proposto, porém, não tenta prover segurança, e sim facilidade de acesso, não havendo identificação de usuário ao abrir a porta. A arquitetura proposta para o sistema é mostrada na Figura 1. Nesta, é diagramada a comunicação entre um dispositivo celular e um módulo Bluetooth. Os dados recebidos no circuito são enviados ao microcontrolador que tem a tomada de decisão sobre a ativação do relé, que comanda uma fechadura elétrica.

III. Arquitetura e Características do Sistema Proposto

Esta seção apresenta o desenvolvimento e a implementação da fechadura eletrônica, bem como as principais características da aplicação móvel de reconhecimento facial e da camada da persistência de dados. A arquitetura do sistema proposto possui 4 camadas: circuito de ativação, *firmware*, comunicação e aplicação, conforme indicado na Figura 2 e que serão explicadas com mais detalhes a seguir.

A. Circuito de ativação

O esquemático do circuito montado junto à fechadura eletromagnética é exibido na Figura 3. Este pode ser interpretado como dois circuitos distintos: o circuito de comunicação Bluetooth, na parte superior do esquemático e o circuito de acionamento da fechadura, na parte inferior.

O sistema tem seu controle baseado na plataforma de prototipagem de hardware Arduino. Os componentes utilizados para a montagem do circuito foram:

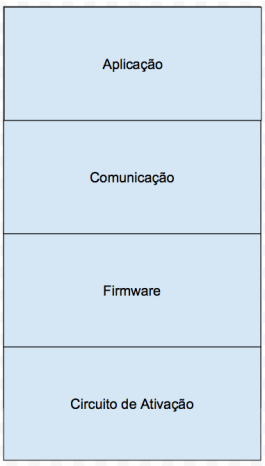

Fig. 2. Módulos da fechadura em modelo de camadas. De baixo para cima, do hardware até a aplicação que o usuário utiliza.

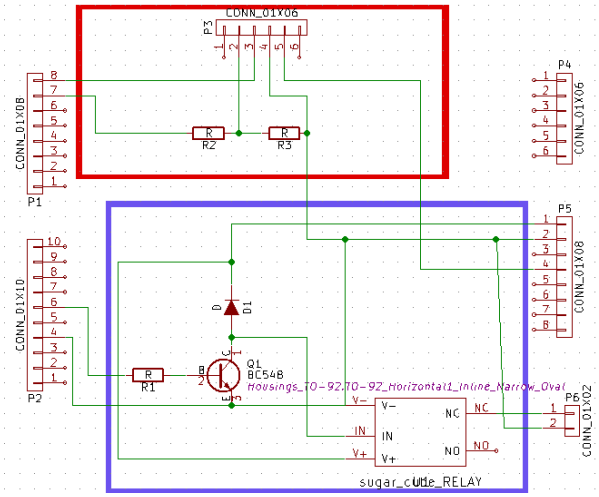

Fig. 3. Esquemático do projeto de *hardware*. A região destacada em vermelho corresponde ao circuito de comunicação, enquanto a região destacada em azul mostra o circuito de acionamento.

- Relé de bobina de 5 V e comum de até 127 V.
- Resistências de 1 kΩ e 220 Ω
- Diodo 1N4007
- Módulo Bluetooth HC-05
- Transistor BC 458

A parte de comunicação funciona com transferência serial de dados que, para o Arduino, pode ser utilizada de duas formas, por hardware ou por software. O modo de comunicação implementado em hardware funciona apenas com as portas digitais 1 e 2 da placa. Na implementação em software, com o emprego da biblioteca SoftwareSerial [11], não existe essa limitação, permitindo inclusive a conexão com mais de um aparelho ao mesmo tempo, sendo esse processo, contudo, mais custoso para o microcontrolador. Não necessitando de múltiplas portas para comunicação, este trabalho utiliza o modo de comunicação por hardware.

O módulo de comunicação Bluetooth necessita apenas de um divisor de tensão indicado por R2, e um resistor *pull down* na resistência R3, para o pino de TX, indicado pelo número 2, conforme mostrado na Figura 3. Os outros pinos do módulo de comunicação: RX, Vcc e Terra (pinos 3,4 e 5), podem ser ligados diretamente ao processador. Os dois pinos restantes, pinos 1 e 6, não precisam ser conectados para este projeto.

Como a tensão do microcontrolador é de 5 V, é necessário o uso de um relé JQC 3F(T73), indicado na Figura 3 por *sugar_CUBE_relay*, para ativar a trava, cujo sinal de controle deve ter tensão de 12V.

B. Firmware

O *firmware* foi implementado para a plataforma Arduino. A tarefa principal do programa, que é executado em um laço infinito, é identificar um sinal em um socket aberto que se comunica com o módulo do rádio Bluetooth.

Primeiramente, o programa aguarda que seja iniciada uma conexão a partir de uma fonte externa, ou seja, o programa executa em modo servidor.

Uma vez que uma nova conexão é iniciada, o programa embarcado aguarda pelo sinal de ativação. Com seu recebimento, um sinal digital em nível alto é enviado para a porta 12, conectada ao resistor R1 na Figura 3, onde o transistor está conectado. Um atraso de 500 ms é aplicado, tempo suficiente para fazer a ativação da fechadura. Após isto, o sinal é novamente levado ao nível lógico baixo.

C. Comunicação

As partes deste sistema têm sua comunicação baseada no modelo de rede pessoal sem fio (WPAN) Bluetooth. Este é uma especificação de rede sem fio de curto alcance, até 100 metros de distância. A especificação foi idealizada como tecnologia substituta de cabos de comunicação em aplicações. O módulo HC-05 e o sistema operacional Android fazem o gerenciamento da pilha de comunicação Bluetooth.

O módulo utilizado neste projeto corresponde a um dispositivo de classe 2 [12], tendo seu alcance limitado a 10 metros. O alcance limitado é muito interessante para o projeto, pois força o usuário estar próximo ao circuito de ativação.

D. Aplicação

A aplicação tem como principal objetivo ser a interface de interação com a fechadura. Para tanto, ela deve ser capaz de fazer todo o processo de reconhecimento facial. O trabalho de Castilho [5], que é utilizado como referência neste projeto, faz uma revisão das principais abordagens usadas para reconhecimento facial.

Antes da identificação facial propriamente dita, uma fase de pré-processamento é realizada, conforme descrito por Castilho [5], compreendendo 4 etapas: (a) conversão das imagens capturadas para representação em níveis de cinza; (b) localização e extração da região da face (se houver); (c) redimensionamento da região extraída; e (d) equalização de histograma da região extraída. O pré-processamento é importante, pois reduz o custo computacional nas etapas posteriores e melhora a qualidade da identificação.

Para localizar faces, a aplicação usa a implementação do algoritmo Viola-Jones [13] (CvHaarCascateClassifier) que faz

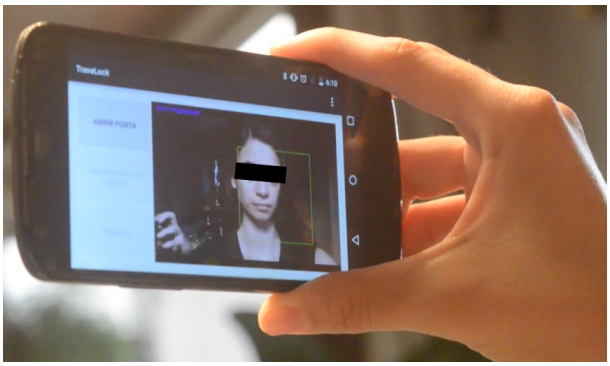

Fig. 4. Aplicação identificando rosto no fluxo de vídeo (olhos ocultados).

parte da biblioteca de código aberto OpenCV (do inglês - *Open Source Computer Vision*).

A aplicação mantém um fluxo de vídeo aberto, transportando quadros capturados para o localizador de faces a cada 500 ms. A Figura 4 mostra um exemplo do momento da detecção de um rosto no fluxo. O atraso de 500 ms é adotado de forma a economizar recurso computacional, pois câmeras de celulares costumam capturar em média 24 quadros por segundo, que se fossem todos processados levaria a aplicação utilizar grande parte do poder de processamento do smartphone, aumentando sobremaneira o consumo de bateria do equipamento.

Uma vez localizada uma face, as operações de pré-processamento são iniciadas. Primeiramente, a imagem é convertida para escala de cinza mediante o método Imgproc.cvtColor() e o modo COLOR_RGB2GRAY (OpenCV). Em seguida, a região do rosto é extraída e redimensionada para 320×240 pixels. Este tamanho foi escolhido empiricamente por apresentar um bom compromisso entre qualidade de identificação e custo computacional. O pré-processamento é concluído pela operação de equalização de histograma da imagem da face (OpenCV, método Imgproc.equalizeHist()) e eventual armazenamento dessa imagem de forma persistente, por exemplo, em um cartão de memória do smartphone, utilizando o formato Cairo PNG e a mesma resolução utilizada após o redimensionamento.

Na fase de treinamento do sistema de reconhecimento, a ser detalhada em seguida, as etapas de pré-processamento são repetidas até que se tenha um número mínimo imagens armazenadas na memória do celular. É a partir de tais imagens que serão determinados os parâmetros do sistema de reconhecimento de faces. A abordagem de reconhecimento adotada é a de *Eigenfaces*, proposta por Turk e Pentland [14]. Neste método, as imagens das faces a serem identificadas são representadas por suas projeções em um subespaço de autovetores da matriz de covariância do conjunto de treinamento.

O sistema de identificação de faces possui dois modos de funcionamento: treinamento ou cadastro de usuário; e identificação ou autenticação de usuário.

No treinamento, um certo número de imagens da face dos usuários a serem cadastrados são combinadas para formar uma única matriz $\mathbf{\Gamma}$ de tamanho $l \times c$, onde l representa o número de pixels de cada uma das imagens de face, e c corresponde ao número total de imagens. Note que para formar a matriz $\mathbf{\Gamma}$, cada imagem de usuário é reorganizada como vetor coluna. Em seguida, é calculada a imagem média, $\mathbf{\Psi}$:

$$\mathbf{\Psi} = \frac{1}{c}\sum_{i=1}^{c}\mathbf{\Gamma}_i \tag{1}$$

onde $\mathbf{\Gamma}_i$ denota a i-ésima coluna de $\mathbf{\Gamma}$.

Subtrai-se, então, a imagem média de cada uma das imagens de face dos usuários

$$\mathbf{\Phi}_i = \mathbf{\Gamma}_i - \mathbf{\Psi}, \quad i = 1, 2, \cdots, c \tag{2}$$

onde $\mathbf{\Phi}_i$ representa a i-ésima coluna da matriz $\mathbf{\Phi}$.

A fim de reduzir a complexidade computacional associada ao cálculo dos autovetores da matriz de covariância $\mathbf{\Phi}\mathbf{\Phi}^t$ (matriz de dimensão $l \times l$), Turk e Pentland [14] descrevem um método alternativo que se baseia no cálculo dos autovetores de $\mathbf{\Phi}^t\mathbf{\Phi}$ (matriz de dimensão $c \times c$):

$$\mathbf{U}_j = \mathbf{\Phi}\mathbf{V}_j, \quad j = 1, 2, \cdots, c \tag{3}$$

onde $\mathbf{U}_j$ e $\mathbf{V}_j$ são autovetores das matrizes $\mathbf{\Phi}\mathbf{\Phi}^t$ e $\mathbf{\Phi}^t\mathbf{\Phi}$, respectivamente.

As imagens de treinamento $\mathbf{\Phi}_i$ podem ser representadas por suas projeções no subespaço formado pelo conjunto de autovetores $\mathbf{U}_j$, de acordo com

$$\mathbf{W}_{ij} = \mathbf{U}_j^t\mathbf{\Phi}_i \tag{4}$$

O sistema deve armazenar os autovetores $\mathbf{U}_j$, bem como a matriz de características $\mathbf{W}_{ij}$ para posterior reconhecimento de usuários.

No modo de reconhecimento, a identificação de usuários é feita mediante cálculo da distância Euclidiana entre o vetor de características de uma nova imagem de entrada e os vetores de características das imagens de treinamento:

$$\mathbf{d}_i = \left[\sum_{j=1}^{c}(\mathbf{W}_j - \mathbf{W}_{ij})^2\right]^{\frac{1}{2}} \tag{5}$$

onde $\mathbf{W}_j$ denota a projeção da imagem do usuário a ser autenticada no autovetor $\mathbf{U}_j$; e d_i representa a distância Euclidiana entre os vetores de características da imagem do usuário a ser autenticado e da i-ésima imagem cadastrada.

Imagens cujo d_i estejam abaixo de um determinado valor de limiar são consideradas de um usuário cadastrado. Este valor pode variar de acordo com os objetivos da aplicação e testes devem ser feitos para encontrar o valor ideal.

E. Implementações

A aplicação desenvolvida tem como alvo aparelhos smartphones com sistema operacional Android que sejam suportados pela biblioteca OpenCV. Também é necessário que os dispositivos possuam uma câmera fotográfica e suporte para Bluetooth. Através de tal suporte, é possível parear e controlar o circuito da fechadura, o que permite o controle de acesso.

Na placa contendo o circuito de ativação existe um borne de dois conectores para ser feita a ligação dos polos da fechadura eletromagnética e uma barra de pinos fêmea de 6 posições para o Bluetooth. O esquema de pinagem com o microcontrolador tem como objetivo ser Arduino compatível.

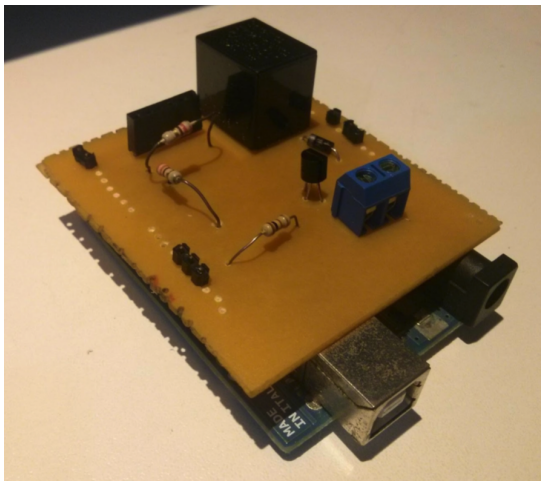

Fig. 5. Placa de ativação acoplada ao Arduino.

TABELA I
RESULTADOS DE TESTES.

	Aceitos (%)	Rejeitados (%)
Rosto Cadastrado	60	40
Rosto Não Cadastrado	7,5	92,5

IV. PROCEDIMENTO DE AVALIAÇÃO E RESULTADOS

A. *Circuito de acionamento, firmware e comunicação*

Foram feitos testes informais com as camadas de acionamento, firmware e comunicação. Para testar a camada de acionamento, um programa simples que alternava o sinal da fechadura entre alto e baixo a cada um segundo foi criado. A fechadura respondeu com sucesso a estes sinais.

Para as camadas de firmware e comunicação, os testes foram realizadas com uma aplicação de ativação simples para celular. Nesta, o apertar de um botão na interface gráfica realizava uma conexão com o circuito de ativação e enviava uma mensagem requerendo a abertura da fechadura. Os resultados foram satisfatórios, não havendo quaisquer problemas a tratar.

B. *Reconhecimento facial*

Estudos realizados por Castlho [5] indicaram que é possível se obter 95% de sucesso durante o processo de reconhecimento com um número reduzido de 4 images de treino. Detalhes dessa análise podem ser consultados em [5].

De forma a comparar o desempenho da implementação neste trabalho com o de [5], 10 indivíduos foram convidados. Cada um deles realizou 20 testes, 10 como agentes autorizados e 10 como não autorizados. O objetivo era buscar o número de aceitações, rejeições, falsos positivos e falsos negativos.

Conforme pode ser visto na Tabela I, a porcentagem de acerto tem certa similariade com [5], quando comparados com os testes em modo online. Em seus testes de modo online, a autora indica dificuldades no sistema em lidar com ambientes e poses diferentes, encontrando falsos negativos e falsos positivos.

Os resultados de rejeição de rostos não cadastrados são satisfatórios, rejeitando 92.5% dos rostos não cadastrados. Em contrapartida, o percentual de rejeição de rostos cadastrados no sistema (40%) é um ponto que necessita ser trabalhado.

V. CONSIDERAÇÕES FINAIS

Neste trabalho é proposto um sistema de ativação de fechadura eletrônica, desde o circuito de ativação até a aplicação. O circuito de ativação é baseado na plataforma de prototipagem Arduino, tendo como função intermediar a comunicação do módulo Bluetooth e fazer a ativação do relé de forma a emitir um pulso.

As taxas de aceitação e rejeição ainda precisam ser polidas. Ainda é necessário investigar um método de reconhecimento facial de tempo real que possa ser utilizado dentro das limitações do ambiente de aplicações para dispositivos móveis. Dentre algoritmos atuais, é necessário fazer uma avaliação sobre o desempenho nesta aplicação. Também é necessário aperfeiçoar a estratégia de avaliação dos métodos de reconhecimento para um modelo menos subjetivo.

Do ponto de vista da segurança de rede, ainda é preciso investigar e implementar medidas padrão para evitar ataques como *spoofing*, *replay* e sequestro de sessão dentro de uma comunicação baseada em tecnologia Bluetooth.

O ambiente de dispositivos Android ainda é bem fragmentado, tendo diferenças entre as especificações determinadas e as implementações de cada fabricante. Sendo assim, é importante fazer um estudo sobre a consistência dos resultados do reconhecimento facial e execução da aplicação em geral em diversos modelos de aparelhos. Para buscar garantir uma experiência mais uniforme através de telefones, uma implementação baseada em nuvem, deixando o telefone apenas como terminal de captura de imagem e comunicação Bluetooth é uma ideia consistente.

REFERÊNCIAS

[1] UNDP. Human development report. United Nations Development Programme. 1994.
[2] UNDP. Human development report. United Nations Development Programme. 2014.
[3] Q. Bai and Y. Zheng. Study on the access control model in information. *Cross Strait Quad-Regional Radio Science and Wireless Technology Conference*, 2011.
[4] Encyclopaedia Britannica Academic. Lock, August 2012.
[5] J. M. Castilho. Estudo e implementação de técnicas de processamento de imagens aplicadas em reconhecimento de face. *Trabalho de Conclusão de Curso*, 2012.
[6] J. P. Pelipos. Smart key door with wireless security system using rf signal. *Final Year Project Report*, 2010.
[7] J. M. Shah. Door locking system using rfid technology. *Final Year Project Report*, 2009.
[8] T. Kim, H. Park, and Y. Chang. Integration of face recognition and sound localization for a smart door phone system. *IEEE International Conference on Consumer Electronics*, 2013.
[9] P. Urien. A secure cloud of electronic keys for nfc locks securely controlled by nfc smartphones. *Consumer Communications and Networking Conference*, 2014.
[10] N. H. Ismail, Z. Tukiran, N. N. Shamsuddin, and E. I. S. Saadon. Android- based home door locks application via bluetooth for disabled people. *IEEE International Conference on Control System, Computing and Engineering*, 2014.
[11] Arduino. Arduino - softwareserial.
[12] Ling Xin. Product data sheet.
[13] P. Viola and M. J. Jones. Robust real-time face detection. *International Journal of Computer Vision*, 2(57):137–154, 2004.
[14] M. Turk and A. Pentland. Eigenfaces for recognition. *Journal of Cognitive Neuroscience*, 1991.