Sistemas automáticos de impressões digitais integrando Java e Arduino

Esequias Aquino Duarte Neto[1], Ricardo de Sousa Job[2], Amanda Drielly Pires Venceslau[3], Samuel Alves da Silva[4], Valnyr Vasconcelos Lira[5]

[1] neto.jpa@hotmail.com; [2] ricardo.job@ifpb.edu.br; [3] driellyads@gmail.com; [4] samuel@ifpb.edu.br; [5] valnyr@ifpb.edu.br. Instituto Federal de Educação, Ciência e Tecnologia da Paraíba – IFPB. Rua José Antônio da Silva, 300 – Jardim Oásis – Cajazeiras (PB) – (83) 3532-4100

RESUMO

A biometria digital é a característica biométrica mais difundida e utilizada dentre as demais. Ela utiliza-se das variações das linhas existentes nas pontas dos dedos para determinar a identidade de um indivíduo. Aparentemente trata-se de uma tecnologia futurista, mas a biometria digital foi uma prática adotada pelas civilizações passadas, que as utilizavam para realizar transações comerciais e enviar documentos confidenciais. Com o grande volume de dados, novos métodos que visavam aprimorar o trabalho com impressões digitais foram propostos, mesmo assim todos possuíam dificuldades para armazenar e realizar buscas. Para resolver o problema foram criados os Sistemas Automáticos de Impressões Digitais, que por envolver múltiplas áreas de conhecimento, torna difícil a implementação para os desenvolvedores. Este trabalho apresenta as etapas necessárias que envolvem a implementação dessa tecnologia, afim de tornar o leitor capaz de compreender e desenvolver os processos e o funcionamento de um Sistema Automático de Identificação de Impressões Digitais utilizando a linguagem de programação Java e a plataforma de desenvolvimento Arduino.

Palavras-chave: Biometria. Impressões digitais. Sistema de identificação.

ABSTRACT

The digital biometric is the most wide spread biometrics characteristics and used among others. It utilizes the variations of existing lines on the fingertips to determine the identity of an individual. Apparently this is a futuristic technology, but digital biometrics was a practice adopted by past civilizations that used to conduct business transactions and send confidential documents. With the large volume of data, new methods aimed at enhancing the work with fingerprints have been proposed, yet all of them had difficulties to store and conduct searches. To solve the problem were created the Automated Fingerprint Systems, which involve multiple areas of knowledge, it becomes difficult to implement by developers. This work presents the necessary steps involved in this technology in order to make the reader able to understand and develop the processes and operation of an Automatic Identification System Fingerprint using the Java programming language and the Arduino development platform.

Keywords: *Biometrics. Fingerprint. Identification systems.*

1 Introdução

A biometria digital é a característica biométrica mais difundida e utilizada dentre as demais (PINHEIRO, 2008), sendo uma prática adotada desde as civilizações antigas para realizar transações comerciais e enviar documentos confidenciais. A biometria digital utiliza as variações de linhas existentes nas pontas dos dedos para identificar um indivíduo. Com o tempo, surgiram métodos que visavam aprimorar o trabalho com impressões digitais. No entanto, esses métodos ainda possuem dificuldades, como armazenamento e busca dos dados. Para resolver esse tipo de problema, foram criados os AFIS (*Automatic Fingerprint Identification System*), que, aliados com o atual poder computacional, possibilitam agilidade de processamento e larga escala de armazenamento (PINHEIRO, 2008). Outro problema é a interdisciplinaridade no desenvolvimento dos AFIS, pois envolvem múltiplas áreas de conhecimento, desde a parte de hadware – leitores biométricos e comunicação com o dispositivo – à de software – extração e análise das características da impressão digitalizada.

Diante do exposto, esta pesquisa discute os conceitos técnicos necessários sobre essa tecnologia, além de apresentar um estudo de caso com duas operações, cadastro e identificação, através das impressões digitais, utilizando a linguagem de programação Java e a plataforma de desenvolvimento Arduino.

2 Metodologia

O trabalho foi desenvolvido basicamente em duas etapas. Na primeira, foi realizado um levantamento bibliográfico para compreensão do tema abordado. Já na segunda etapa, foi desenvolvido um estudo de caso para consolidar a teoria apresentada. Para execução do estudo de caso, foram utilizados alguns componentes eletrônicos, dentre eles: um leitor de impressão digital e um Arduino Ethernet, com um kit de desenvolvimento que inclui um LCD, um conversor serial para USB, cabos, LEDs e um protoboard. Além disso, foi implementado um programa em Java que tem como objetivo controlar a execução das tarefas programadas no Arduino, que por sua vez se comunica com o leitor de impressão digital, emitindo avisos para o LCD acoplado e à aplicação Java via porta serial.

3 Sistemas de identificação biométrica

O termo "biometria" tem sua origem no latim e significa "medida da vida". Segundo Sucupira Junior (2004), biometria é a ciência que estuda a mensuração dos seres vivos, ou seja, refere-se às medições de características únicas e intransferíveis de um indivíduo, sejam elas comportamentais ou físicas. Essas características únicas são divididas em dois grupos. O primeiro, está relacionado a características comportamentais: voz, escrita e assinatura; e o segundo, está relacionado a características físicas: face, íris, odor, dedo, mão, retina, orelha.

No mundo computacional, biometria pode ser definida como um conjunto de métodos automatizados capazes de identificar, autenticar e/ou verificar a identidade de um indivíduo por meio de uma de suas características físicas (PINHEIRO, 2008).

3.1 Impressões digitais

As impressões digitais são encontradas na derme[1] e se formam na epiderme[2]. É na derme que encontra-se as papilas, dispostas em uma série de linhas (cristas papilares) separadas por sulcos. As impressões digitais são formadas próximo do sexto mês de gestação humana e durante o envelhecimento, apesar de ocorrer mudança de tamanho, o formato original permanece inalterado durante toda a vida de um indivíduo (ABE, 2005; SILVA, 2006). As pesquisas de Galton (1895) comprovaram cientificamente a unicidade e estabilidade das impressões digitais, tornando essa característica um excelente identificador biométrico. O estudo biométrico, utilizando os dedos como forma de medição, é chamado de datiloscopia ou dactiloscopia. Segundo Costa S. (2001), esse termo é de origem grega – daktylos = dedo e skopein = examinar –, significando a análise dos dedos (mãos ou pés).

Uma impressão digital é basicamente composta por três elementos: núcleo, deltas e linhas. As linhas são os elementos-chave na formação de uma digital; através delas são formados todos os outros elementos. Deltas são figuras formadas pela junção de linhas de vários sentidos, fazendo parecer um triângulo.

1 Derme: tecido conjuntivo sobre o qual se apoia a epiderme.

2 Epiderme: porção superficial da pele

Os deltas possibilitam a divisão das impressões em diversas classes e regiões (marginal, nuclear, basilar). Já os núcleos são formados pelas linhas encontradas no centro de uma impressão digital. O desenho encontra-se nas curvas mais internas com angulação maior ou igual a 180° e é denominado de loops. Esses três elementos são ilustrados na Figura 1.

Figura 1 – Elementos Básicos das Impressões Digitais (PINHEIRO,2008).

A identificação de uma impressão digital é possível através de características nelas encontradas, denominadas de minúcias ou aspectos de Galton, antropólogo britânico que provou cientificamente que as impressões digitais não mudam no decorrer do tempo e nenhuma é exatamente igual a outra. As minúcias ou pontos característicos são resultados de acidentes apresentados pelas linhas (ou cristas) papilares e representam a garantia de unicidade em impressões digitais (MARANHÃO, 1989).

As minúcias são divididas em duas categorias: elementos básicos e compostos. Os elementos básicos são formadas por apenas uma linha, enquanto os elementos compostos são formados por duas ou mais linhas, conforme visto nas Figuras 2 e 3, respectivamente.

Figura 2 – Elementos Básicos (Costa, 2001)

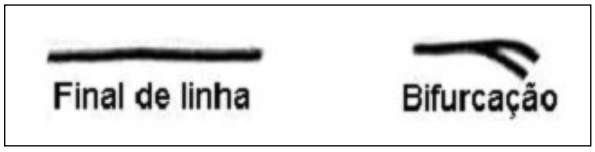


Figura 3 – Elementos Compostos (Costa, 2001).

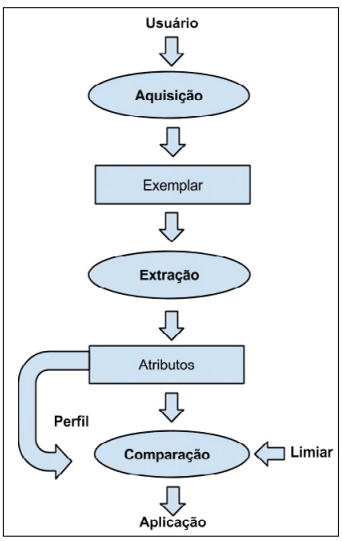
3.2 Sistemas biométricos

Os sistemas biométricos surgiram na década de 70 e devido à necessidade de agilizar o processamento de reconhecimento de um indivíduo, a partir dos dados biométricos armazenados, iniciou-se uma grande corrente de pesquisa nesse ramo. Em 1902, a Comissão de Serviço Civil de Nova York começou a utilizar AFIS, sendo logo adotada por todo país. Organizações, como FBI (2013), começaram a implantar sistemas biométricos para controlar o acesso a locais restritos, escolas passaram a usá-los em cantinas, baseados na geometria da mão, como forma de identificação. Houve também grande interesse do Governo pela tecnologia de reconhecimento e principalmente pelos AFIS, por seu baixo custo (SINFIC, 2013; FORUMBIOMETRIA, 2013; ARAUJO, 2000).

Segundo Pinheiro (2008), sistemas biométricos podem ser definidos como um conjunto de hadware e software para reconhecimento de padrões de propósito específico, que operam através da aquisição automática de uma das características de um indivíduo, extração de um modelo ou exemplar a partir dessa característica e comparação desse modelo com uma coleção de outros modelos, previamente armazenados em uma base de dados.

Um sistema biométrico deve seguir um modelo conceitual simples, apresentado na Figura 4, que leva em consideração os dados e processos básicos comuns a qualquer outro sistema biométrico.

Figura 4 – Modelo Conceitual Simples (PINHEIRO,2008).



O funcionamento ocorre da seguinte maneira: um usuário é previamente registrado e seu perfil biométrico fica armazenado; posteriormente, ao utilizar o sistema, o processo de aquisição coleta os dados biométricos através do leitor; características particulares dos dados são extraídas para comparação com o perfil armazenado; o processo de comparação decide a partir do limiar de comparação, que é um número que representa o grau de aceitação pré-estabelecido, se os dados apresentados são suficientemente similares ao perfil armazenado (PINHEIRO, 2008; COSTA, 2006).

3.3 AFIS - Sistema Automático de Identificação de Impressões Digitais

Os AFIS são sistemas baseados na detecção dos diferentes tipos de minúcias encontrados na impressão digital e que, segundo Pinheiro (2008), visam garantir a unicidade de identificação de um indivíduo e agilizar esse processo de identificação. Para isso, os AFIS seguem o modelo conceitual simples, de um sistema biométrico.

3.3.1 Aquisição da imagem

Neste processo, um leitor de impressão digital (*fingerprintreader*) é utilizado para adquirir uma imagem da impressão digital, chamada de exemplar. É possível encontrar vários modelos desses dispositivos no mercado, que geralmente utilizam uma comunicação via serial ou USB.

3.3.2 Pré-processamento da imagem

Para que seja possível extrair as minúcias, são aplicados filtros, a fim de obter uma imagem mais nítida, reduzindo a quantidade de ruídos e riscos. O algoritmo abordado foi proposto por Hong, Wan e Jain (1998), por ser um dos mais referenciados e conceituados na literatura. A fim de obter uma imagem binária otimizada, o algoritmo adotado propõe que a imagem passe pelos processos de normalização de cores, estimativa de orientação, estimativa de frequência, geração de máscara de filtragem e aplicação do filtro, de forma sequencial.

3.3.3 Extração de minúcias

Este processo identifica os vários tipos de minúcias. A partir dessa identificação, são extraídas todas as características necessárias para formação de um *template*, que será armazenado em uma base de dados para posteriores comparações. Segundo Costa L. (2006), neste processo devem ser realizadas três operações: refinamento da imagem otimizada, detecção do núcleo e mapeamento e armazenamento das minúcias.

A esqueletização da imagem ou refinamento é utilizada para extrair características de um objeto em uma imagem. Esse processo retira todos os dados redundantes e forma uma representação do objeto, preservando todas as informações originais, com um menor número de pixel, formando assim um esqueleto (skeleton). Dentre vários métodos, um que está sendo adotado é o algoritmo de Zhang e Suen (1984), pois é de fácil entendimento e simples implementação.

Para encontrar o núcleo, localiza-se o primeiro loop da impressão digital para que as coordenadas de todas as minúcias encontradas sejam fornecidas levando-o em consideração. Para realizar essa localização do núcleo é utilizado o cálculo do índice de Poincaré.

Através do esqueleto obtido pelo algoritmo de refinamento, varre-se a imagem a fim de encontrar as minúcias. A localização é feita buscando apenas os elementos básicos (bifurcações e finais de linhas) através de uma janela 3x3, averiguando a conectividade do pixel. As bifurcações têm a conectividade igual a 3 e os finais de linhas têm conectividade igual a 1. Após a descoberta da localização das minúcias, marca-se a posição (x, y), tendo como referência o núcleo encontrado e a orientação. O conjunto dessas informações é chamado de *template*, o qual será armazenado na base de dados para posteriores comparações.

3.3.4 Comparação

Neste processo é realizado o confronto entre dois *templates*, tomando como base o grau de similaridade, a partir do limiar configurado no sistema. Apesar de não ser regra, a taxa de limiar com um percentual de 80% é o aceitável para uso nos AFIS. O processo de comparação inicia-se com o alinhamento pelo núcleo das impressões a serem comparadas. Logo após, as minúcias são confrontadas, levando em consideração uma margem de erro na localização (x, y) das minúcias, causadas pela elasticidade da pele.

4 Resultados e discussão

O principal resultado deste trabalho é aplicar a teoria e a prática em um estudo de caso, não tendo o objetivo de comparar as possíveis soluções para cada etapa de construção dos AFIS. Sabendo das dificuldades encontradas – que envolvem múltiplas áreas de conhecimento, desde a parte de hadware (leitores biométricos e comunicação com o dispositivo) à de software (extração e análise das características da impressão digitalizada) – foi realizado um estudo de caso em que foi aplicado AFIS em uma fechadura eletrônica.

No estudo de caso foram efetuadas duas operações básicas: cadastro e identificação através das impressões digitais. Para execução do estudo de caso foram utilizados alguns componentes eletrônicos, dentre eles: um leitor de impressão digital, que realiza a análise, comparação e armazenamento da impressão digital e um Arduino Ethernet, que manipula os processos do leitor, juntamente com um kit de desenvolvimento que inclui um LCD, um conversor serial para USB, cabos, LEDs e uma protoboard. Além disso, foi implementado um programa em Java que tem como objetivo controlar a execução das tarefas programadas no Arduino, que por sua vez se comunica com o leitor de impressão digital, emitindo avisos para o LCD acoplado e à aplicação Java via porta serial.

O estudo de caso é capaz de cadastrar e identificar um indivíduo através de sua impressão digital, liberando ou negando acesso a um ambiente restrito com uma fechadura eletrônica. Será exposto um sistema na plataforma Arduino, responsável por manipular as etapas do modelo conceitual implementadas pelo leitor de impressão digital, e um outro na plataforma Java, que irão se comunicar via porta serial. O sistema da plataforma Arduino possui um sensor biométrico, um display, dois LEDs e um conversor serial/USB. Já na plataforma Java, foi desenvolvido um sistema desktop que possui uma base de dados Postgre SQL para armazenar as informações pessoais dos indivíduos (exceto a impressão digital) e que utiliza os frameworks EclipseLink para parte de persistência de dados e Java Swing para parte visual.

Por motivos financeiros, a fechadura eletrônica é simulada por dois LEDs, sendo o primeiro verde, indicando que o acesso foi liberado, e o outro vermelho, indicando que o acesso foi negado. Deixar de utilizar a fechadura eletrônica não interfere nos resultados da pesquisa. O estudo de caso aborda uma parte de hadware, vista na seção 4.1, e outra de software, vista na seção 4.2.

4.1 Hardware

Nesta seção serão descritos os componentes eletrônicos utilizados no estudo de caso. Inicialmente, temos a placa do microcontrolador, escolhida para o estudo de caso por suportar a comunicação serial, além de sua plataforma permitir um desenvolvimento ágil, portabilidade, e por ser pequena e de baixo consumo de energia, podendo ser alimentada pela porta USB. Em especial foi escolhida uma placa Arduino Ethernet (ARDUINO, 2013), a qual possibilita a troca da comunicação serial por uma comunicação em rede, abrindo muitas possibilidades de desenvolvimento, inclusive aplicações comerciais.

O sensor de impressão digital utilizado foi escolhido por realizar a parte pesada do processamento da imagem digital, disponibilizar o protocolo e uma API de comunicação via serial, simplificando o processo, e ter um baixo nível de falsa aceitação e rejeição. Em razão do processamento ser feito no próprio dispositivo e possuir uma memória interna capaz de armazenar 162 *template*s, suficiente para nossa pesquisa, o leitor tem grande poder de processamento, para realizar as tarefas de processamento da imagem, armazenamento e buscas, tornando-se superior se comparado aos sensores que não realizam esses processos internamente.

4.1.1 Arduino

O projeto Arduino foi criado na Itália, em 2005, com o objetivo de oferecer uma plataforma de prototipagem eletrônica de baixo custo e de fácil utilização para criação de projetos com objetos e ambientes interativos (ARDUINO, 2013). Possui código fonte aberto, possibilitando aos utilizadores adequá-lo às suas necessidades reais. Segundo Mellis (2009), um dos fundadores do Arduino, isso contribuiu com a popularização do hardware que vem sendo utilizado desde a construção de projetos de luminárias inteligentes até aviões que se auto pilotam.

A placa eletrônica do Arduino consiste em um microcontrolador Atmel[3] da família AVR que permite

3 Atmel Corporation é uma manufaturadora de semicondutores, fundada em 1984. http://www.atmel.com/.

milhares de gravações e regravações em sua memória de programa. Um aspecto importante é como a placa do Arduino permite conexões de módulos expansíveis, conhecidos como shields. Os shields são placas eletrônicas que têm por objetivo expandir as funcionalidades da placa Arduino. Geralmente elas são fixadas no topo do Arduino através de conexões alimentadas por pinos-conectores, agregando funções que variam desde controle sobre motores até sistema de rede wireless.

Alguns modelos baseados no Arduino e shields têm surgido ultimamente graças à função da plataforma open source do projeto, os quais são denominados modelos não oficiais. Eles são produzidos/desenvolvidos por empresas e até mesmo pela própria comunidade Arduino em toda parte do mundo. Esses modelos estão listados no site oficial do projeto (ARDUINO, 2013).

O modelo escolhido para o estudo de caso foi o Arduino Ethernet, que é uma placa microcontroladora baseada no Atmega328. Seus principais componentes são 14 entradas/saídas digitais, 6 entradas analógicas, uma conexão RJ45 e uma entrada para alimentação de 12V. O Arduino Ethernet difere-se das outras placas por possuir no lugar de um chip controlador USB-serial, uma interface Ethernet, que é a mesma interface encontrada no shield Ethernet. Por essa razão, os pinos de 10 a 13 são reservados para interface do módulo de Ethernet e só devem ser usados caso não se tenha a intenção de utilizar esse módulo. Outra peculiaridade é o fato de possuir um leitor de cartão microSD, que pode ser usado para armazenar dados para disponibilizar/servir em rede. O pino 4 é reservado para comunicação com o cartão SD (ARDUINO, 2013).

4.1.2 Sensor de impressão digital Adafruit

Adafruit é uma indústria fundada em 2005 que além de produzir uma grande diversidade de ferramentas, equipamentos e componentes eletrônicos projetados para utilizadores de qualquer idade, tem o objetivo de ser o melhor site de aprendizagem em eletrônica. Todos os seus produtos são selecionados e testados pessoalmente pela engenheira Limor, a qual foi a primeira engenheira mulher a aparecer na capa da revista Wired e escolhida como empreendedora do ano 2012 pela revista Entrepreneur (ADAFRUIT, 2013).

O sensor foi produzido com alta tecnologia e utiliza um leitor óptico para capturar a impressão digital em forma de imagem através de um diodo emissor de luz em sua lente. Há um chip DSP (Digital Signal Processor) de alta potência que faz a renderização e o processamento da imagem com cálculos de hash. Por essa razão, além do leitor de impressão digital deixar transparente para o desenvolvedor toda parte burocrática e cansativa do processamento de imagem digital, seguindo o modelo conceitual de um sistema biométrico, ele também é capaz de processar em menos de 1 segundo as imagens, trabalhando em uma janela de 14 mm x 18 mm.

O leitor trabalha com um limiar variável de 1 a 5, configurável, possui uma taxa de falsa aceitação de menos de 0,001% e uma taxa de falsa rejeição de menos de 1% quando o limiar está configurado em nível de segurança 3. Ao processar a imagem, o leitor gera um *template* de 512 bytes que pode ser armazenado em sua própria memória ou em qualquer outro dispositivo que tenha uma interface TTL serial para comunicação, como por exemplo um cartão de memória do Arduino.

4.1.3 Conversor USB/serial FT232RL e LCD 16x2

O conversor tem uma função importante no estudo de caso, pois converte a comunicação USB para serial, além de suprir energia para o Arduino Ethernet, porque no lugar do chip controlador USB-serial, possui uma interface Ethernet.

O LCD possui 16 colunas e 2 linhas, uma luz de fundo ou backligth na cor verde e escrita na cor preta. Esse LCD foi utilizado no estudo de caso para emitir avisos aos usuários.

4.2 *Software*

O estudo de caso foi desenvolvido utilizando um leitor biométrico, a plataforma Arduino e uma aplicação Java. Seguindo o modelo conceitual, sua execução inicia quando a aplicação Java, através da porta serial utilizando a API RXTX, envia ao Arduino um dos dois modos de operação. O primeiro é o modo cadastro, que realiza um pré-cadastro na aplicação Java com os dados do indivíduo. Nesse pré-cadastro, é gerado um identificador único, pelo framework JPA (Java Persistence API), que serve para ligar os dados do indivíduo cadastrado na aplicação Java à impressão digital que será armazenada no leitor biométrico. Em seguida, o identificador é transmitido ao Arduino, que realiza a captura da impressão digital através

do leitor com a apresentação da mesma impressão digital por duas vezes. Então, o leitor analisa a qualidade da imagem. Se ela estiver dentro da qualidade aceitável, é realizado o pré-processamento da imagem, extração das minúcias e formado o *template* da impressão digital. Com o *template*, o Arduino solicita ao leitor o armazenamento, finalizando esse modo de operação. O segundo modo é a identificação, em que o Arduino aguarda a leitura da impressão digital no leitor, para posterior comparação com as digitais armazenadas. Em ambos os modos, há notificações no LCD ligado ao Arduino e na aplicação Java com mensagem na tela.

O programa implementado em Java tem como objetivo controlar a execução das tarefas programadas no Arduino, que por sua vez se comunica com o leitor de impressão digital, emitindo avisos para o LCD acoplado e à aplicação Java, via porta serial. Com essa integração entre Java e Arduino algumas das limitações de ambas as linguagens são superadas. O Arduino controla a parte de hadware, tarefa difícil de ser realizada utilizando a linguagem Java. Por outro lado, com uma plataforma baseada em componentes, a linguagem Java possibilita o controle do Arduino por outras interfaces como web e dispositivos móveis.

4.2.1 Modo Cadastro

No modo de operação cadastro, a aplicação Java realiza um pré-cadastro com as informações do indivíduo, que, gerando um identificador único, o envia para o Arduino antes da ativação do leitor biométrico. Posteriormente, o Arduino fica no aguardo do indivíduo para que esse apresente por duas vezes a mesma impressão digital ao leitor. Caso a impressão seja capturada corretamente, o Arduino armazenará na base de dados do leitor a impressão digital do indivíduo, juntamente com o identificador fornecido, desativando o modo cadastro e notificando à aplicação Java que a impressão digital foi cadastrada com sucesso.

Para exemplificar o passo a passo da execução do modo de cadastro, será adicionado um novo usuário. Nas Figuras 5 e 6 são descritos os passos necessários para o cadastro:

Passo 1: Primeiramente, o usuário clica no ícone de adição; outra tela será aberta para inserção do nome do usuário.

Passo 2: Ao clicar em salvar, o sistema gera um identificador único o qual será persistido em uma base de dados Postgre SQL, juntamente com o nome preenchido e um campo booleano com o valor falso, indicando que o indivíduo ainda não possui digital cadastrada.

Passo 3: Logo após selecionado o modo cadastro, o usuário é direcionado para uma tela de busca em que o indivíduo anteriormente cadastrado na base de dados será listado. Todos os indivíduos que não possuem uma digital cadastrada são apresentados.

Passo 4: Após esses passos, selecionado o indivíduo, a aplicação Java envia dois comandos para o Arduino. O primeiro ativa o modo de cadastro e o segundo é o identificador, anteriormente gerado, do indivíduo selecionado. A captura é realizada comparando as mesmas impressões do indivíduo apresentadas duas vezes ao leitor.

Figura 5 – Etapas do funcionamento do estudo de caso no modo cadastro.

Passo 5: Caso sejam idênticas, é emitido o aviso no LCD e a digital é armazenada na memória do leitor na posição do identificador único, anteriormente gerado, pela aplicação Java que logo é notificada que a impressão foi capturada com sucesso.

Passo 6: Posteriormente, a aplicação Java recupera os dados a partir do identificador, altera o atributo booleano isdigital para true, e finaliza o cadastro emitindo um aviso indicando que o processo foi bem sucedido.

Figura 6 – Funcionamento do estudo de caso no modo cadastro.

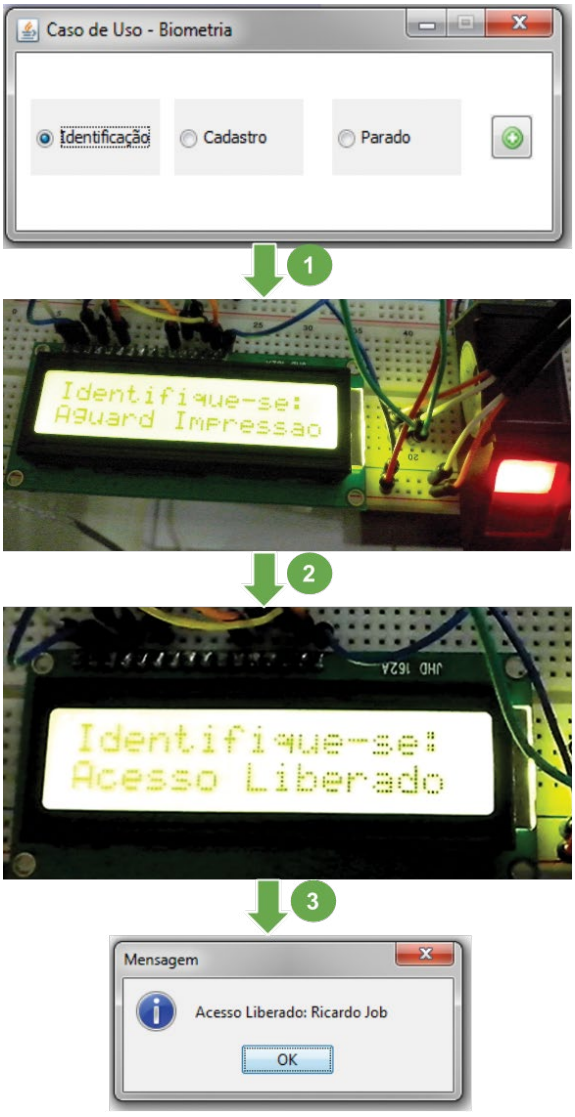
4.2.2 Modo Identificação

No modo de operação identificação, a aplicação Java envia ao Arduino um comando de ativação. A aplicação do Arduino, por sua vez, ativa o leitor biométrico e fica aguardando até que um indivíduo apresente sua impressão digital ao leitor biométrico. Se o indivíduo não for identificado, o Arduino emite um aviso no LCD com mensagem de acesso negado. Caso contrário, se o indivíduo for reconhecido, o sistema Arduino além de emitir mensagem de acesso liberado no LCD, notifica a aplicação Java com o identificador recuperado indicando permissão concedida de acesso ao ambiente restrito requisitado.

Em seguida, a aplicação Java pesquisa o identificador recebido na base de dados Postgre SQL, recupera as informações e exibe o nome do indivíduo identificado que teve acesso liberado. Em ambos os casos, os LEDs informam se o indivíduo teve ou não acesso, sendo o verde representando acesso liberado e o vermelho acesso negado.

Para exemplificar o passo a passo da execução do modo de identificação, será feita a identificação do usuário anteriormente cadastrado. Na Figura 7 são descritos os passos necessários para a identificação.

Figura 7 – Funcionamento do estudo de caso no modo identificação.



Passo 1: Ao selecionar o modo Identificação, a aplicação Java cadastra um listener para ser notificada quando um indivíduo for reconhecido pelo leitor biométrico e envia um comando para ativar o modo no Arduino.

Passo 2: Por sua vez, o Arduino emite um aviso no LCD que ativa o leitor biométrico e entra em loop. No sensor, é essa operação que o mantém ligado, e quando uma impressão digital é apresentada ele retorna seu status. Já o Arduino, fica lendo o status do leitor e verificando se foi dado o comando para encerrar o modo identificação. Quando o Arduino verifica o comando de parar, ele encerra o modo, mas quando verifica que o status do leitor foi alterado, solicita que realize o processo de comparação entre a digital apresentada e as armazenadas.

Passo 3: Caso o processo de comparação identifique o indivíduo, o Arduino envia uma mensagem para o LCD, requisita o identificador da impressão digital ao leitor e envia para a aplicação Java. Por fim, a aplicação Java emite um aviso com o nome do indivíduo e o modo de identificação recomeça o processo, até a aplicação Java enviar um comando para encerrar esse modo.

5 Conclusões

O estudo apresentou as etapas necessárias para compreensão dos Sistemas Automáticos de Impressões Digitais. Para isso, expôs inicialmente uma breve introdução à biometria e seus tipos e, em seguida, abordou os sistemas biométricos, apresentando um modelo conceitual simples envolvendo as etapas necessárias para a implementação de um AFIS. As principais contribuições da pesquisa foram o levantamento das informações da parte teórica, que aborda todo conteúdo pertinente, bem como a implementação de um estudo de caso prático que proporciona flexibilidade para criação de sistemas portáveis, que podem ser adaptados facilmente em ambientes que oferecem baixa alimentação de energia, como fechaduras ou urnas eletrônicas, a exemplo do que acontece nas eleições do Brasil, modelo para os países de primeiro mundo. Finalmente, os resultados práticos obtidos foram analisados através de um estudo de caso capaz de cadastrar e reconhecer um indivíduo utilizando um leitor de impressão digital, ligado a uma placa microcontroladora Arduino, que por sua vez é controlada por uma aplicação desenvolvida na linguagem de programação Java. Como trabalho futuro, a forma de comunicação entre o Arduino e aplicação Java pode ser alterada e utilizada a comunicação via rede.

REFERÊNCIAS

ABE, R. C. **Dispositivos Biométricos com Comunicação USB**. São Paulo: Faculdade de Engenharia de Sorocaba, 2005.

ADAFRUIT, **Adafruit Industry**. Disponível em: <http://www.adafruit.com>. Acesso em: 14 nov. 2013.

ARAUJO, C. J. AFIS – **Sistemas Automáticos de Impressões Digitais**. Brasília, 2000. Disponível em: <http://www.papiloscopistas.org/afis.html>. Acesso em: 30 jun. 2013.

ARDUINO. **Arduino**. Disponível em: <www.Arduino.cc>. Acesso 14 set. 2013.

COSTA , S. M. F. **Classificação e verificação de impressões digitais**. 2001.

COSTA, L. R., Obelheiro, R. R., Fraga, J. S. **Introdução à Biometria**. Santa Catarina: Universidade Federal de Santa Catarina, 2006.

FBI. Federal Bureau of Investigation (Departamento Federal de Investigação). Disponível em: <www.fbi.gov>. Acesso em: 30 jun. 2013.

FORUMBIOMETRIA. Disponível em: <www.forumbiometria.com/fundamentos-de-biometria/118-historia-da-biometria.html>. Acesso em: 30 jun. 2013.

GALTON, F. FINGERPRINT. Londres, 1895.

SUCUPIRA JUNIOR, L. H. R. **Uma Metodologia para Avaliação de Pacotes de Software Biométricos**. 2004. Dissertação de Mestrado – UNICAMP, São Paulo, 2004.

MARANHÃO, O. R. **Curso Básico de Medicina Legal**. 4. ed. São Paulo: Editora Revista dos Tribunais,1989.

MELLIS, D. O Hardware em 'código aberto'. **Revista Info Exame**, março, 2009. Disponível em: <http://info.abril.com.br/professional/tendencias/hadware-livre-leve-e-solto.shtml>. Acesso em: 14 nov. 2013.

PINHEIRO, J. M. **Biometria nos Sistemas Computacionais - Você é a Senha**. Rio de Janeiro: Editora Ciência Moderna LTDA., 2008.

SILVA, T. V. M. **Estudo Sobre Técnicas de Pré-Processamento e Extração de Características Utilizadas no Reconhecimento de Impressões Digitais**. Monografia, Unipê, Paraíba, 2006.

SINFIC. Disponível em: <www.sinfic.pt/>. Acesso em: 30 jun. 2013.

HONG L.; WAN Y.; JAIN A. **Fingerprint Image Enhancement:** Algorithm and Performance Evaluation. Department of Computer Science, Michigan State University, v. 20, n. 8, p. 777-789, 1998.

ZHANG, T. Y.; SUEN, C. Y. **A Fast Parallel Algorithm for Thinning Digital Patterns**. Communication of the ACM, v. 27, n. 3, p. 236-239, 1984.

AGRADECIMENTOS

Ao IFPB – *Campus* Cajazeiras pelo financiamento via Edital Bolsa PIBICT, e ao Grupo de Pesquisa em Automação pelo apoio na pesquisa.