UNIVERSIDADE FEDERAL DE OURO PRETO

ESCOLA DE MINAS

COLEGIADO DO CURSO DE ENGENHARIA DE CONTROLE E AUTOMAÇÃO – DECAT

GABRIEL NIQUINI LOPEZ

SISTEMA PARA MONITORAMENTO DE ACESSO UTILIZANDO ARDUINO E LEITURA BIOMÉTRICA

MONOGRAFIA DE GRADUAÇÃO EM ENGENHARIA DE CONTROLE E AUTOMAÇÃO

Ouro Preto, 2015

GABRIEL NIQUINI LOPEZ

SISTEMA PARA MONITORAMENTO DE ACESSO UTILIZANDO ARDUINO E LEITURA BIOMÉTRICA

Monografia apresentada ao Curso de Engenharia de Controle e Automação da Universidade Federal de Ouro Preto como parte dos requisitos para a obtenção do Grau de Engenheiro de Controle e Automação.

Orientador: Prof. Dr. Alan Kardek Rêgo Segundo

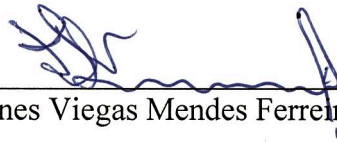
Co-orientador: Diógenes Viegas Mendes Ferreira

Ouro Preto
Escola de Minas – UFOP
Julho 2015

Monografia defendida e aprovada, em 09 de julho de 2015, pela comissão avaliadora constituída pelos professores:

Prof. Dr. Alan Kardek Rego Segundo – Orientador

Prof. Dr. Luiz Fernando Rispoli Alves – Professor Convidado



Eng. Diógenes Viegas Mendes Ferreira – Engenheiro Convidado

RESUMO

O controle de acesso à ambientes restritos é uma grande preocupação para empresas, instituições e residências. A cada dia se faz mais necessário um monitoramento mais efetivo dos acessos, assim como melhores alternativas para garantir a segurança dos usuários. O projeto proposto visa a utilização de um sensor biométrico para o acionamento de uma fechadura eletromagnética. Dessa forma, pode-se restringir o acesso e substituir a chave, evitando também que a mesma seja perdida, copiada ou transferida de usuário. É possível, ainda, um número mais significativo de usuários. Propõe-se criar um software capaz de gerencias os acessos a um determinado ambiente criando, também, um banco de dados para salvar os dados coletados para posterior análise. O sensor biométrico conecta-se ao Arduino, que faz a leitura dos dados. Através de uma comunicação serial, é possível registrar e acompanhar as informações pelo Visual Studio através de uma interface de fácil compreensão para o usuário.

Palavras-chave: Biometria, Arduino, Visual Studio, Fechadura.

ABSTRACT

The access control to restricted environments is a major concern for companies, institutions and residences. Every day becomes more necessary a more effective monitoring of access, such as better alternatives to ensure the safety of users. The proposed project aims to use a biometric sensor for triggering an electromagnetic lock. That way, you can restrict access and replace the key, also avoiding it to be lost, copied or user transferred. You can also have significantly more users. It is proposed to create software capable of managing accesses a certain environment creating also a database to save the data collected for further analysis. The biometric sensor connects to the Arduino, which reads the data. Through serial communication, you can record and track information by Visual Studio through an easy to understand user interface.

Keywords: Biometric, Arduino, Visual Studio, Lock.

LISTA DE FIGURAS

LISTA DE TABELAS

SUMÁRIO

1 INTRODUÇÃO

Sistemas de Controle de Acesso Físico visam permitir que somente usuários autorizados tenham acesso a um determinado ambiente, impedindo os usuários não autorizados. Procuram automatizar o processo de verificação de acesso ou auxiliar nas tarefas relativas à proteção patrimonial. Para serem usados para autenticação, precisam de uma base de dados contendo informações de identificação e, para o nível de permissão, informações do que o usuário pode fazer (PINHEIRO 2008, p. 23).

Para garantir o acesso de forma controlada, existem tecnologias à disposição do consumidor. Um dos recursos mais utilizados é o sensor de leitura biométrica por impressão digital, cujo grau de confiabilidade demonstrou ser superior a 99%, tornando o sistema em questão uma excelente alternativa aos métodos convencionais.

Entretanto, estabelecer uma associação entre um indivíduo e uma identidade pode ser um problema que é dividido em duas categorias: autenticação e identificação. Autenticação refere-se ao problema de confirmar ou negar uma alegada identidade de um indivíduo, enquanto identificação refere-se ao problema de estabelecer a identidade, desconhecida à partida, de um indivíduo.

O termo biometria deriva do grego *bios* (vida) e *metron* (medida) e, na autenticação, refere-se à utilização de características próprias de um indivíduo para proceder à sua autenticação e/ou identificação perante um sistema de identificação de uma organização.(MAGALHÃES; SANTOS, 2003)

Segundo Magalhães (2003), o nível de confiabilidade do sistema pode ser definido através dos valores FAR (*False Acceptance Rate* – Taxa de Falsas Aceitações) e o FRR (*False Rejection Rate* – Taxa de Falsas Rejeições). Infelizmente estas variáveis são mutuamente dependentes, não sendo possível minimizar ambas. Tenta-se, então, encontrar um ponto de equilíbrio chamado CER (*Crossover Error Rate* – Taxa de Intersecção de Erros). Quanto mais baixo for o CER mais preciso é um sistema biométrico (Figura 1.1).

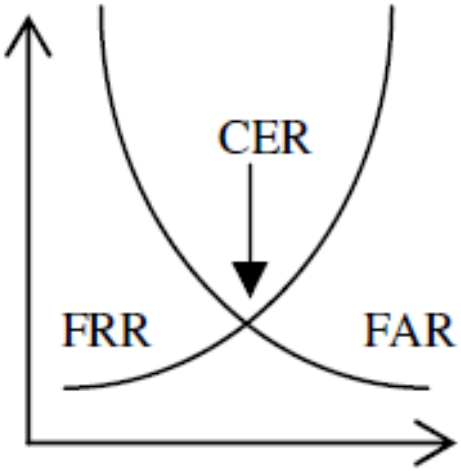


Figura 1.1: CER

Outro fator a ser considerado é o nível de conforto. De um modo geral, o sistema melhor aceito pelos utilizadores quanto menos intrusivo for, fato facilmente comprovado analisando-se as tecnologias mais e menos utilizadas, como a leitura de retina que possui um nível de intrusão superior ao reconhecimento de voz ou leitura de impressões digitais. O custo de implementação é um quesito fundamental e abrange diversos fatores, como:

- Hardware;
- Software;
- Integração com hardware/software existentes;
- Formação dos utilizadores;
- Pessoal de manutenção de Bases de Dados;
- Manutenção do sistema.

Além do custo, esses fatores também influenciarão na autenticação. O termo autenticação descreve o processo através do qual a identidade de uma pessoa ou entidade pode ser confirmada ou negada. Normalmente depende que o usuário forneça informações válidas seguidas de uma ou mais credencias de autenticação que provem sua identidade.

O sucesso de tais métodos depende de mais que apenas tecnologia. Também dependem de procedimentos e controle.

De acordo com Council (2011), os métodos de autenticação existentes envolvem um ou mais dos seguintes fatores básicos:

- Algo que o usuário sabe;

- Algo que o usuário tem;
- Algo que o usuário é (impressão digital, por exemplo).

Tecnologias de identificação por biometria de um ser vivo se baseia em uma característica física ou fisiológica (algo que a pessoa é). Essas características variam muito pouco com o tempo, e estão relacionadas à herança genética tornando-as um excelente método. Características fisiológicas podem variar de acordo com o organismo da pessoa, como batimentos cardíacos e respiração. Existem, ainda, as comportamentais ou dinâmicas que estão relacionas ao comportamento do indivíduo e têm como desvantagem a volatilidade com o tempo, como por exemplo forma de digitação, assinatura e forma de andar (LOURENÇO 2009, p. 14).

1.1 Objetivo

O projeto desenvolvido tem como objetivo criar um sistema de controle de acesso através de leitura biométrica por impressão digital e monitoramento por um sistema supervisório desenvolvido através do Visual Studio. Todo o sistema é controlado utilizando um Arduino Uno. Através do sistema desenvolvido será possível gerenciar de forma mais organizada, prática e eficaz qualquer acesso realizado ao ambiente monitorado, contribuindo para a segurança e conforto do administrador.

1.2 Metodologia Utilizada

Inicialmente foi feito o levantamento de todos os componentes e equipamentos necessários para o desenvolvimento do projeto.
A seguir, foi adquirido um sensor de leitura biométrica com comunicação serial, facilitando a interação com o Arduino.
A partir da Tabela 1.1 é possível fazer a análise do investimento necessário para o projeto.

Tabela 1.1: Análise de custo do projeto

Fechadura Eletromagnética	90 reais
Arduino Uno	55 reais
Sensor Biométrico	120 reais
Módulo Relé	20 reais
TOTAL	285 reais

Após familiarização com Arduino e sua IDE, foi necessário compreender a biblioteca utilizada para comunica-lo com o sensor e dar início à programação utilizando *pushbuttons* para testes.
Na etapa seguinte, foi feita uma pesquisa sobre programação de supervisórios em C# e deu-se continuidade com o desenvolvimento da tela de comunicação.
Tendo a tela de comunicação operando da forma esperada, foi possível trabalhar na aquisição e envio de dados entre o Arduino e o supervisório.
A última etapa consistiu em exportar os dados adquiridos para posterior análise.

2 REVISÃO BIBLIOGRÁFICA

2.1. Tecnologias de autenticação biométrica

2.1.1 Reconhecimento facial

No reconhecimento facial os problemas são essencialmente provocados por diferentes posições da cabeça. Inicialmente há a captura de uma imagem que é associada à um rosto que deve ser comparada com modelos armazenados em um banco de dados, complementada com a análise da cor da pele, detecção de linhas e outras características físicas. Esse procedimento pode resultar em problemas de reconhecimento, uma vez que a imagem obtida deve ser processada para comparação dos modelos, levando em consideração fatores que podem se alterar com o tempo, como envelhecimento, tamanho e cor do cabelo e barba. O programa deve se concentrar, então, em pontos fixos como nariz, olhos e boca, minimizando os riscos (MAGALHÃES; SANTOS, 2003).

Romano reforça as dificuldades para detectar uma face. De acordo com a autora, os rostos possuem estrutura semelhante como boca e nariz, dispostas nas mesmas configurações de espaço com texturas diferentes e uma quantidade considerável de componentes rígidos, como lábios menos ou mais carnudos. Além disso, os rostos normalmente utilizam adornos, como bigodes ou óculos, que podem estar ausentes ou presentes (quando presentes ocultam características básicas da face). Também não há como prever as condições das faces em ambientes com pouca ou muita iluminação, objetos e cores de fundo, pois pode esconder ou criar sombras no rosto, devido ao formato tridimensional da face.

2.1.2 Geometria da mão

O reconhecimento da geometria da mão resulta de uma análise das características da mão como a forma, o comprimento dos dedos e as suas linhas características. Nesse procedimento analisa-se as características a partir de um referencial fixo, assim como a análise entre cada característica.

A geométrica da mão, contudo, não é uma característica única de cada indivíduo, sendo assim, em uma grande base de dados com diversos elementos, pode não ser o meio mais confiável para controle e restrições (MAGALHÃES; SANTOS, 2003).

As principais medidas analisadas normalmente são: largura do polegar, comprimento do indicador, médio, anelar e mindinho, e largura da palma da mão. Como as características geométricas da mão individuais não são descritivas o bastante para a identificação, é necessário combinar as várias características individuais de forma que seja possível alcançar uma verificação robusta (GAVA, 2006).

2.1.3 Impressão digital

É a forma de análise por biometria mais utilizada atualmente. Possui um grande grau de confiabilidade, podendo alcançar uma precisão superior a 99%. Cada indivíduo possui uma digital que difere de qualquer outra existente, garantindo que dois usuários não possam ser confundidos.

Um problema observado nesse método se deve ao fato de não ser possível detectar de forma convencional digitais de seres vivos ou mortos, e à possiblidade de fraude com dedos de silicone, por exemplo (MAGALHÃES; SANTOS, 2003).

Gava (2006) destaca que esta técnica é a forma mais comum de identificação por biometria, um exemplo de uma aplicação é um sistema de identificação automática utilizado pela polícia em vários países tendo como inconveniente o fato dos dedos serem uma das partes do corpo mais utilizadas podendo ocorrer deformações, o que dificultara o reconhecimento das mesmas.

2.1.4 Leitura de Íris

Segundo Romano, o reconhecimento do indivíduo através da íris é uma tecnologia relativamente nova e tem se mostrado estável e precisa.

A tecnologia envolve a análise do anel colorido que cerca a pupila do olho humano e é a menos intrusiva de todas, funcionando mesmo quando o usuário utiliza óculos. Possui eficácia acima da média, sendo ideal para qualquer situação, porém, é de difícil integração com os sistemas existentes. Uma câmera de vídeo pode ser usada fazendo reconhecimento de imagem, o que impacta em um custo relativamente baixo, tendo em mente que a qualidade do vídeo influenciará na leitura realizada e no resultado da análise (MAGALHÃES; SANTOS, 2003).

2.1.5 Leitura de retina

Os sistemas biométricos baseados na leitura de retina analisam a camada de vasos sanguíneos situada na parte de trás do olho, utilizando uma fonte de luz de baixa intensidade para reconhecer opticamente padrões singulares.

Esta tecnologia pode atingir altos níveis de precisão, mas requer que o usuário foque o olhar em um receptáculo e fixe a visão por um tempo, não sendo ideal para quem utiliza óculos e podendo gerar desconforto em alguns usuários. O custo de implementação desse sensor é mais elevado e restringe sua aplicação (MAGALHÃES; SANTOS, 2003).

2.1.6 Reconhecimento de voz

O processo por reconhecimento de voz utiliza como conceito o fato de que as características físicas de cada usuário resultam em uma voz única para cada pessoa. Contudo, isso pode não permitir uma identificação em larga escala, devido à falta de informações. Estes processos fundamentam-se nas técnicas de processamento de voz e na biometria e o envolvimento do utilizador que pode utilizar uma palavra-chave ou uma sequência de palavras que forneçam elementos suficientes para uma comparação efetiva que possibilite a identificação do usuário. É um método barato e de fácil acesso, já que os microfones presentes nos computadores podem ser usados. Devido à baixa precisão dos equipamentos de reconhecimento de voz e ao fato de poder haver variações nas vozes dos usuários, seu uso passa a ser limitado (MAGALHÃES; SANTOS, 2003).

2.1.7 Keystrokes dynamics

A tecnologia denominada Keystrokes dynamics ou dinâmica de digitação, é baseada na monitorização dos padrões comportamentais do utilizador ao digitar palavras/frases passe e/ou texto durante uma sessão. No primeiro acesso, o usuário deve digitar uma frase de forma que seja possível se encontrar um padrão. A mesma frase deve ser digitada mais de uma vez, entretanto, uma única digitação pode ser suficiente para o reconhecimento do padrão. É também

possível ao sistema adaptar o modelo do padrão ao longo do tempo, de forma a ajustar-se à nova informação recolhida (MAGALHÃES; SANTOS, 2003).

Gava (2006) cita como principais características desse método a latência da digitação, que é o intervalo de tempo entre a digitação de teclas sucessivas, a duração da digitação, que é o intervalo de tempo em que uma tecla permanece pressionada e a pressão da digitação, que é a pressão aplicada em uma tecla, sendo esta uma característica analisada apenas em teclados mais específicos.

2.1.8 Assinatura manual recolhida de modo digital

É muito utilizado atualmente principalmente em cartões de crédito. Nos sistemas mais utilizados possuem a mesma função da assinatura em papel, mas com a tecnologia correta, pode-se usar padrões como velocidade de escrita e pressão efetuada pela mão como fatores determinantes para identificação do usuário (MAGALHÃES; SANTOS, 2003).

Para esta tecnologia de reconhecimento ser eficiente é necessário encontrar características da assinatura que sejam mais constantes, pois estas variam pouco na fase de cadastramento do usuário. Deve-se também considerar que a assinatura pode sofrer influência do papel, ambiente, caneta e estado emocional da pessoa (GAVA, 2006).

2.2 O Arduino

Arduino é uma plataforma eletrônica open-source baseada no uso simplificado de hardware e software (Portal ARDUINO, 2014). Por possuir uma interface mais simplificada, permite que o programador se adapte com mais facilidade. Possui como microcontrolador um ATmega328, que possui resistores de pull-up internos, facilitando a ligação de telas e sensores.

Possui 14 pinos, numerados de 0 a 13 que podem ser configurados como entradas ou saídas de forma simples através da IDE do Arduino.

Souza (2013) explica que ao ser configurado com saída, o pino se encontra em estado de baixa impedância. Dessa forma, o pino pode fornecer ou drenar corrente para um circuito externo. A corrente máxima de operação é de 40 mA por pino, sendo que a soma das correntes não pode ultrapassar 200 mA.

A Figura 2.1 representa um Arduino e a Figura 2.2 seus principais componentes.

Figura 2.1: Arduino UNO
Fonte: Arduino, 2014.

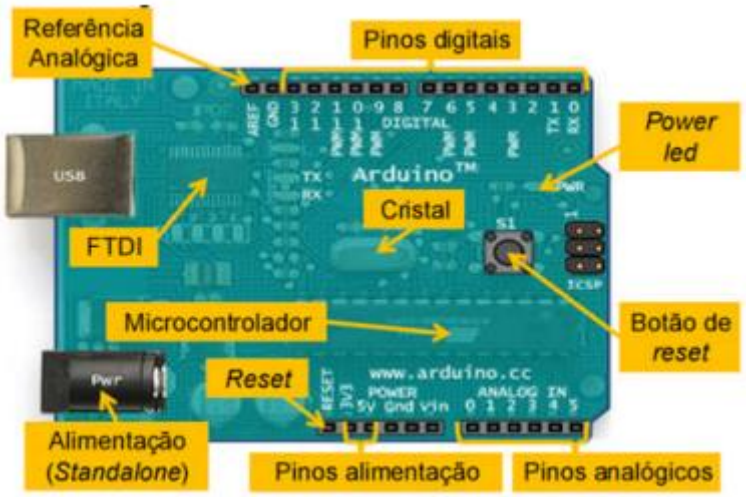


Figura 2.2: Arduino UNO

Fonte: Arduino, 2014.

Através do sistema embarcado, é possível utilizar sensores que receberão sinais e, a partir da lógica empregada pelo programador, enviarão sinais de saída para os atuadores exercerem alguma função (Figura. 2.3). No caso deste trabalho, utilizou-se como sensor um leitor biométrico, que envia, através do Arduino, um sinal de 5V para um relé que ativará uma fechadura eletromagnética.

Figura 2.3: Funcionamento do Arduino

Fonte: Arduino, 2014.

2.3 Microcontroladores

Segundo Souza (2005) apud Sanchez (2014), um microcontrolador é um dispositivo eletrônico que contém um microprocessador, memórias com funções de leitura e escrita, interfaces de entrada e saída e diversos periféricos úteis para o desenvolvimento de sistemas embarcados.
Os microprocessadores por outro lado, não costumam ter periféricos em um único componente, embora tenham capacidade de processamento maior.
Os microcontroladores são computadores criados com um propósito especifico. Possuem tamanho reduzido, baixo custo e baixo consumo de energia. Essas vantagens fazem com que sejam amplamente utilizados em diferentes setores da indústria para os mais variados fins.
A arquitetura varia entre os diferentes tipos de microcontroladores, alterando frequência de *clock*, processamento, entradas e saídas analógicas e digitais, etc.

2.3.1 Atmega328

Segundo Atmel (2015) o Atmega328 é um microcontrolador de 8 bits baseado em RISC AVR que combina memória flash 32Kb ISP com capacidade de leitura e escrita , 1Kb EEPROM, SRAM 2Kb, 23 entradas e saídas de uso geral, 32 registradores de uso geral, três temporizadores, interrupções internas e externas, USART serial programável, porta serial SPI, 6 canais de conversor A/D 10 bits, *timer watchdog* programável com oscilador interno. O dispositivo opera entre 1,8 e 5,5 volts.
Ao executar instruções poderosas em um único ciclo de *clock* , o dispositivo alcança taxas de transferência que se aproximam a um MIPS *(million instructions per second)* por MHz, equilibrando o consumo de energia e velocidade de processamento.

A pinagem no microcontrolador pode ser vista na figura 2.4.

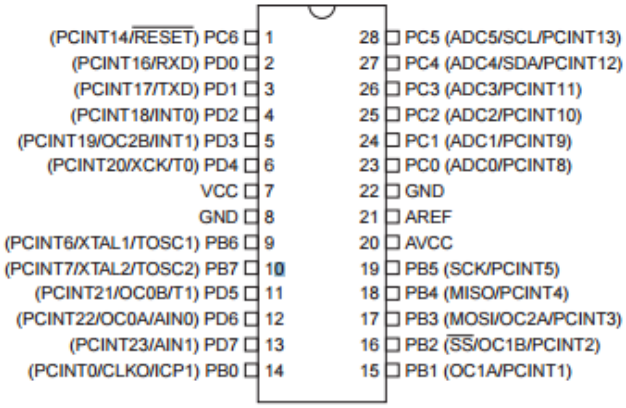


Figura 2.4: Pinagem Atmega328
Fonte: Atmel (2015)

2.4 Display LCD 16x2

O display LCD (Fig. 2.5) é um dispositivo de fácil utilização e oferece uma interface de saída simples com o usuário. Através dele, o usuário pode acompanhar todos os procedimentos e informações disponibilizadas para o usuário de forma simples e dinâmica. Permite que qualquer texto seja escrito, dispondo de duas linhas com 16 caracteres cada.

Figura 2.5: Display LCD 16x2

A Tabela 2.1 mostra as ligações a ser feitas para o funcionamento correto do display.

Tabela 2.1: Conexões LCD

Conexões LCD 16x2 - HD44780		
Pino LCD	**Função**	**Ligação**
1	Vss	GND
2	Vdd	Vcc 5V
3	V0	Pino central potenciômetro
4	RS	Pino 12 Arduino
5	RW	GND
6	E	Pino 11 Arduino
7	D0	Pino 6 Arduino
8	D1	Pino 7 Arduino
9	D2	Pino 8 Arduino
10	D3	Pino 9 Arduino
11	D4	Pino 5 Arduino
12	D5	Pino 4 Arduino
13	D6	Pino 3 Arduino
14	D7	Pino 2 Arduino
15	A	Vcc 5V
16	K	GND

Fonte: Arduino e Cia (2015)

2.5 IDE Arduino

A IDE do Arduino é um software de programação que permite uma integração fácil e rápida com o Arduino. Ele permite gerenciar um projeto, compilar, debugar e gravar o programa a qualquer momento, dentre outras funções. A Figura 2.6 mostra o espaço de trabalho utilizado na IDE.

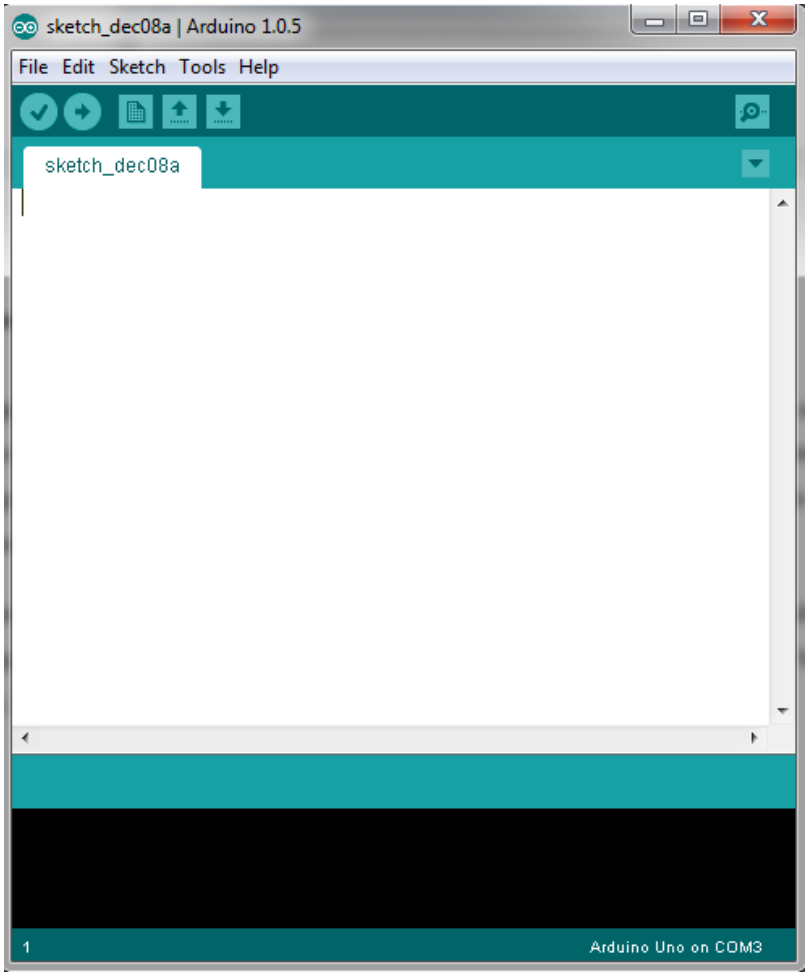


Figura 2.6: Workspace IDE

2.6 Sistema Supervisório

De acordo Magan et. al (2007) apud Rosário (2005), os sistemas supervisórios são sistemas responsáveis pelo monitoramento e controle de variáveis do sistema, tendo como principal função fornecer subsídio ao operador para controlar ou monitorar um processo automatizado mais rapidamente, permitindo a leitura das variáveis em tempo real e o gerenciamento e controle do processo automatizado. O sistema de supervisão atua através de dispositivos automatizados que são monitorados e podem sofrer intervenções de computadores com funções lógicas pré-programadas ou de operadores.

O supervisório permite a operação e visualização através de telas gráficas elaboradas para qualquer processo industrial ou comercial, independentemente do tamanho de sua planta. O trabalho do projetista consiste basicamente na elaboração das telas gráficas, de acordo com o

processo a ser controlado, da configuração dos comandos e da indicação para a boa operação da planta ou sistema (JURIZATO; PEREIRA, 2003).

2.6.1 Visual Studio C#

O C# é uma linguagem de programação criada para o desenvolvimento de uma variedade de aplicações que executam sobre o .NET Framework. É uma linguagem simples, poderosa, com tipagem segura e orientada a objetos.

Visual C# é uma implementação da linguagem C# criada pela Microsoft. O Visual Studio possui um editor de código completo, compilador, modelos de projetos, designers, assistentes de código, um depurador e outras ferramentas. A biblioteca de classes do .NET Framework fornece acesso a vários serviços do sistema operacional e outras classes úteis e bem estruturadas que aceleram significativamente o ciclo de desenvolvimento (MICROSOFT, 2015).

O software possui uma interface simples e de fácil entendimento. Através de sua *toolbox* (Fig. 2.7), torna possível adicionar diversos elementos à interface de acordo com a preferência do usuário e os requisitos do projeto.

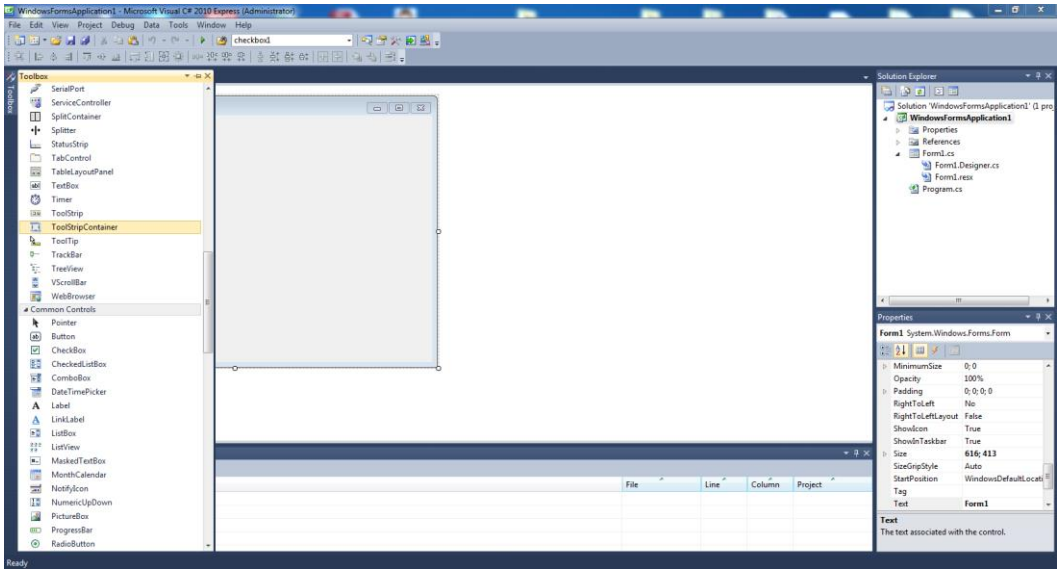


Figura 2.7: Interface Visual Studio C#

2.7 Módulo Relé

Um módulo relé (Fig. 2.8) consiste em uma placa que possibilita conectar o Arduino diretamente a um relé sem necessidade de um circuito auxiliar. Permite que se use lógica NA (normalmente aberto) e NF (normalmente fechado) enviando um sinal digital de 5v através de

uma das saídas do Arduino, tornando possível realizar o chaveamento responsável pelo acionamento da fechadura eletromagnética.

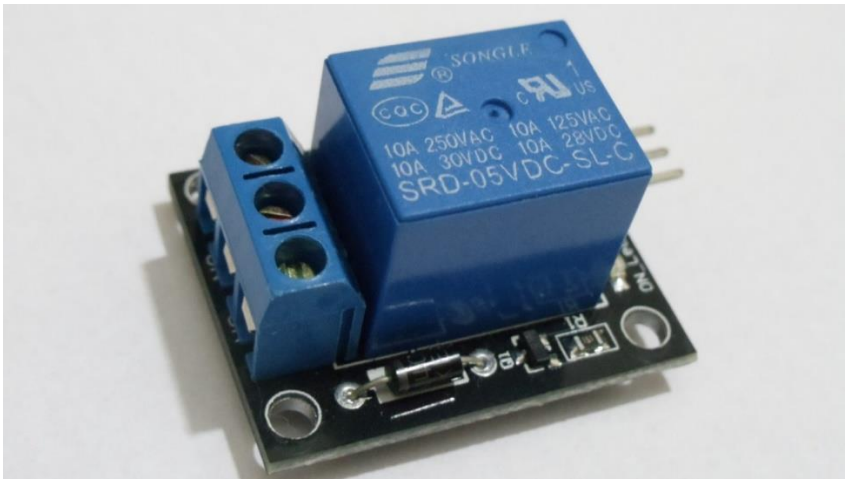


Figura 2.8: Módulo relé.
Fonte: Arduino e Cia (2015)

A Figura 2.9 representa um projeto de módulo relé concebido através do software *Proteus.*

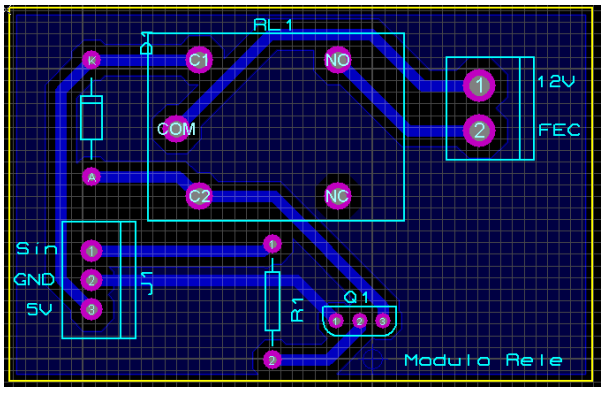


Figura 2.9: Módulo Relé

Através desse dispositivo, é possível acionar a fechadura 12V. Ao confirmar a identidade do usuário através da leitura da impressão digital, um sinal é enviado pelo Arduino ao módulo relé e, nesse momento, ocorre um chaveamento interno que permite que 12V de uma bateria auxiliar sejam transferidos para a fechadura durante um tempo pré-determinado, fazendo com que a mesma seja acionada. O desenho esquemático pode ser visto na figura 2.10.

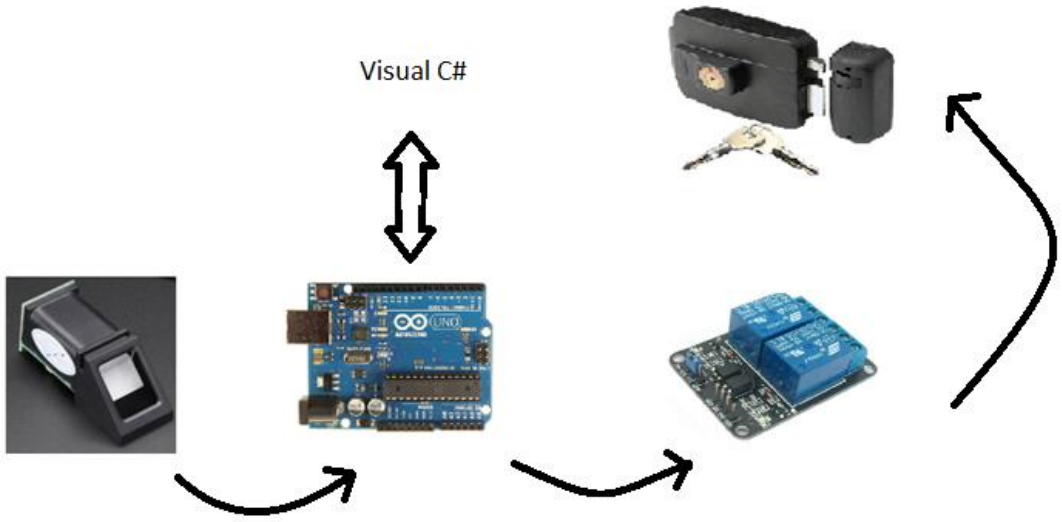


Figura 2.10: Desenho esquemático

2.8 Sensor Biométrico

No projeto foi utilizado um sensor biométrico com comunicação serial (Fig. 2.11), para fazer a leitura das impressões digitais. Possui precisão superior a 99%, sendo assim um meio muito confiável para validação de usuários.

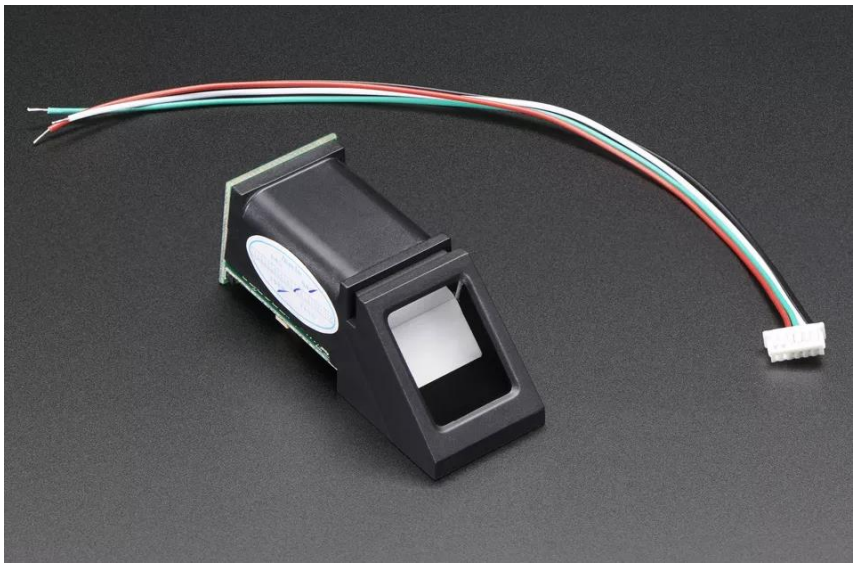


Figura 2.11: Sensor Biométrico
Fonte: Adafruit (2015)

2.8.1 Especificações Técnicas

Na Tabela 2.2 encontra-se o esquema de ligações utilizado para operação do sensor:

Tabela 2.2: Sistema de ligação do sensor

1	Vin	Alimentação	Fio vermelho
2	TD	Saída de Dados	Fio verde
3	RD	Entrada de Dados	Fio branco
4	GND	Terra	Fio preto
5	NC	Não conectado	

O nível de segurança é dividido em 5 graduações, sendo cinco o parâmetro do modelo utilizado. O parâmetro controla o valor limite correspondente de busca de impressões digitais e de harmonização. No nível 1, FAR (*False Acceptance Rate*) é o maior e FRR (*False Rejection Rate*) o menor, entretanto, no nível 4, FAR é o menor e FRR o maior (ZHIANTEC, 2008).
O sensor utilizado tem a vantagem de ser compacto, e de fácil utilização como pode ser visto na Figura 2.12. Além disso, possui memória não volátil, o que garante que os dados salvos não serão perdidos mesmo com uma eventual falta de energia, conferindo segurança e confiabilidade ao sistema.

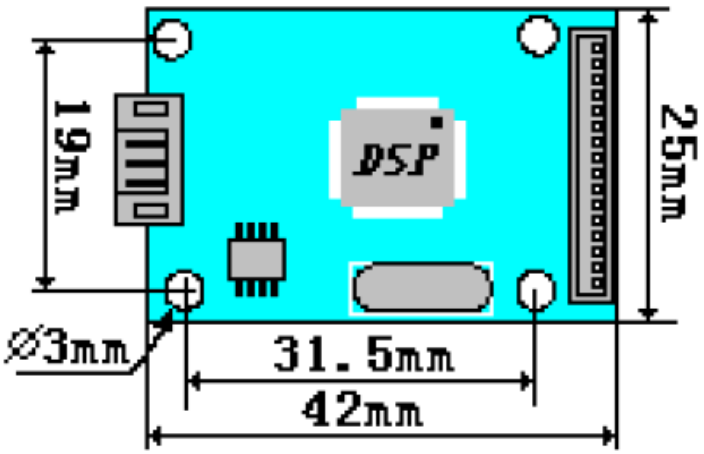


Figura 2.12: Dimensões da placa do sensor.
Fonte: ZHIANTEC (2008)

A Tabela 2.3 contém as especificações técnicas disponibilizadas pelo fabricante.

Tabela 2.3: Especificações técnicas

Tensão de Alimentação	3.6 - 6.0VDC
Corrente de Operação	120mA max
Corrente de Pico	150mA max
Tempo de aquisição da digital	<1.0 seconds
Tamanho do vidro	14mm x 18mm
Arquivo Assinatura Lida	256 bytes
Arquivo Template	512 bytes
Capacidade de armazenamento	162 templates
FAR (*False Acceptance Rate*)	<0.001% (Security level 3)
FRR (*False Reject Rate*)	<1.0% (Security level 3)
Interface	TTL Serial
Taxa de transmissão	9600, 19200, 28800, 38400, 57600 (padrão)
Temperatura de operação	-20C to +50C
Humidade de operação	40%-85% RH
Dimensões	56 x 20 x 21.5mm
Peso	20 grams

2.8.2 Princípio de Operação

O processamento de leitura biométrica é composta de duas partes: cadastro e verificação, que pode ser 1:1 ou 1:N. O usuário necessita fornecer a digital duas vezes. O sistema processa as duas imagens, gera um template da digital baseado nos resultados processados e armazena o template. Quando houver necessidade de comparação para validação, será gerado um novo template para ser comparado com templates da biblioteca. A comparação será feita até que o resultado 1:1 seja encontrado, ou que toda a biblioteca seja verificada, retornando o resultado positivo ou negativo (ZHIANTEC, 2008).

São usados dois tipos de leitores: óptico e capacitivo. O leitor óptico é formado por um módulo chamado ‘dispositivo de carga acoplado’, no qual está presente uma série de diodos sensíveis à luz (*photosites*), e um conversor de imagem analógico-digital. Os *photosites* reagem ao estímulo de fótons luminosos, enviando um sinal elétrico, que registrará a seção da imagem captada em um pixel. A combinação entre pixels resultará na imagem da digital, que será avaliada pelo sistema utilizado.

A tecnologia de leitura capacitativa faz uso da corrente elétrica ao invés de luz para formar as imagens para avaliação. Em seu interior, circuitos semicondutores interagem com a superfície do dedo, que com seu deslocar sobre essa região promovem uma tensão distinta em cada área pressionada. Essa tensão mapeada é verificada pelo processador, que avaliará as variações da pele, de vale ou sulco, para gerar a imagem digital.

2.9 Comunicação Serial

O conceito de comunicação serial é simples, sendo uma aplicação facilmente implementada. A porta serial envia e recebe bytes de informação um bit de cada vez, podendo operar em conjunto com um protocolo de comunicação verificando o recebimento correto dos dados. Embora esta seja mais lenta que a comunicação paralela, que permite a transmissão de um byte inteiro por vez, ela é mais simples e pode ser utilizada em distâncias maiores. Por exemplo, a IEEE 488 sobre especificações para comunicação paralela diz que o cabeamento entre equipamentos não pode ter mais que 20 metros no total, com não mais que 2 metros entre dois dispositivos. Já a comunicação serial pode se estender até 1200 metros.

Normalmente, a serial é usada para transmitir dados ASCII. A comunicação é completada usando 3 linhas de transmissão: Terra, Transmissão, Recepção. Visto que a serial é assíncrona, a porta está apta a transmitir dados em uma linha enquanto recebe dados em outra. É importante ressaltar que os dispositivos que estão se comunicando devem possuir as mesmas configurações. As características mais importantes são taxa de transmissão (*baud rate*), bits de dados (*data bits*), bits de parada (*stop bits*), e paridade.

2.9.1 Taxa de Transmissão (*Baud rate*)

Uma medida de velocidade para comunicação. Isto indica o número de bits transmitidos por Segundo. Por exemplo, 300 baud são 300 bits por Segundo. Quando nos referimos a um ciclo de clock nós medimos a taxa de transmissão. Altas taxas de transmissão são utilizadas para comunicação de dispositivos quando os dispositivos estão próximos.

2.9.2 Bits de Dados (*Data bits*)

Quando o computador envia um pacote de informação, a quantidade de dados pode não ser um 8 bits completo. Os valores padrão para pacotes de dados são 5, 7, e 8 bits. Qual configuração você deve escolher depende de qual informação você está transferindo. Um pacote refere-se a

uma transferência de byte único, incluindo bits de início/fim, bits de dados, e paridade. Como o número atual de bits depende do protocolo selecionado, o termo pacote é utilizado para cobrir todas as instâncias.

2.9.3 Bits de parada (*Stop bits*)

Usado para sinalizar o fim da comunicação para um único pacote. Os valores típicos são 1, 1.5, e 2 bits. Uma vez que os dados são cronometrados através da linha e cada dispositivo possui seu próprio clock, é possível os dois dispositivos virem a estar ligeiramente fora de sincronia. Portanto, os bits de parada não só indicam o fim da transmissão, mas também dão aos computadores alguma margem de erro nas velocidades de clock.

2.9.4 Paridade

A paridade é uma forma simples de verificação de erro que é utilizada na comunicação serial. Há quatro tipos de paridade: par, ímpar, marcada e espaçada. Para paridade par e ímpar, a porta serial irá definir o bit de paridade (o ultimo bit depois dos bits de dados) para um valor que garanta que a transmissão tenha um número par ou ímpar de bits de lógica alta. As paridades marcada e espaçada não verificam realmente os bits de dados, mas simplesmente define o bit de paridade alto para paridade marcada ou baixo para paridade espaçada. Isto permite ao dispositivo receptor saber o estado de um bit de modo que habilita o dispositivo determinar se um ruído está corrompendo o dado ou se os *clocks* do transmissor e receptor estão fora de sincronia. (NATIONAL INSTRUMENTS, 2013)

3 DESENVOLVIMENTO

A Figura 3.1 mostra a montagem do protótipo do sistema desenvolvido, que inclui um Arduino Uno, um leitor biométrico, uma *protoboard*, um display lcd 16x2, um potenciômetro e fios e botões para testes.

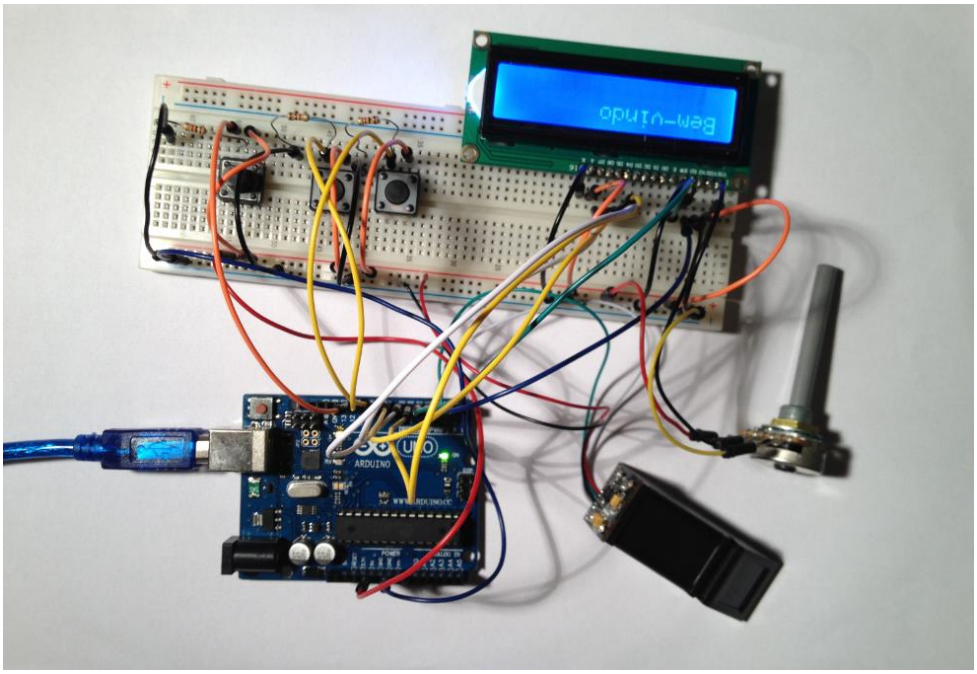


Figura 3.1: Protótipo do sistema

O supervisório desenvolvido para o monitoramento de entradas e controle de acessos pode ser visto na Figura 3.2:

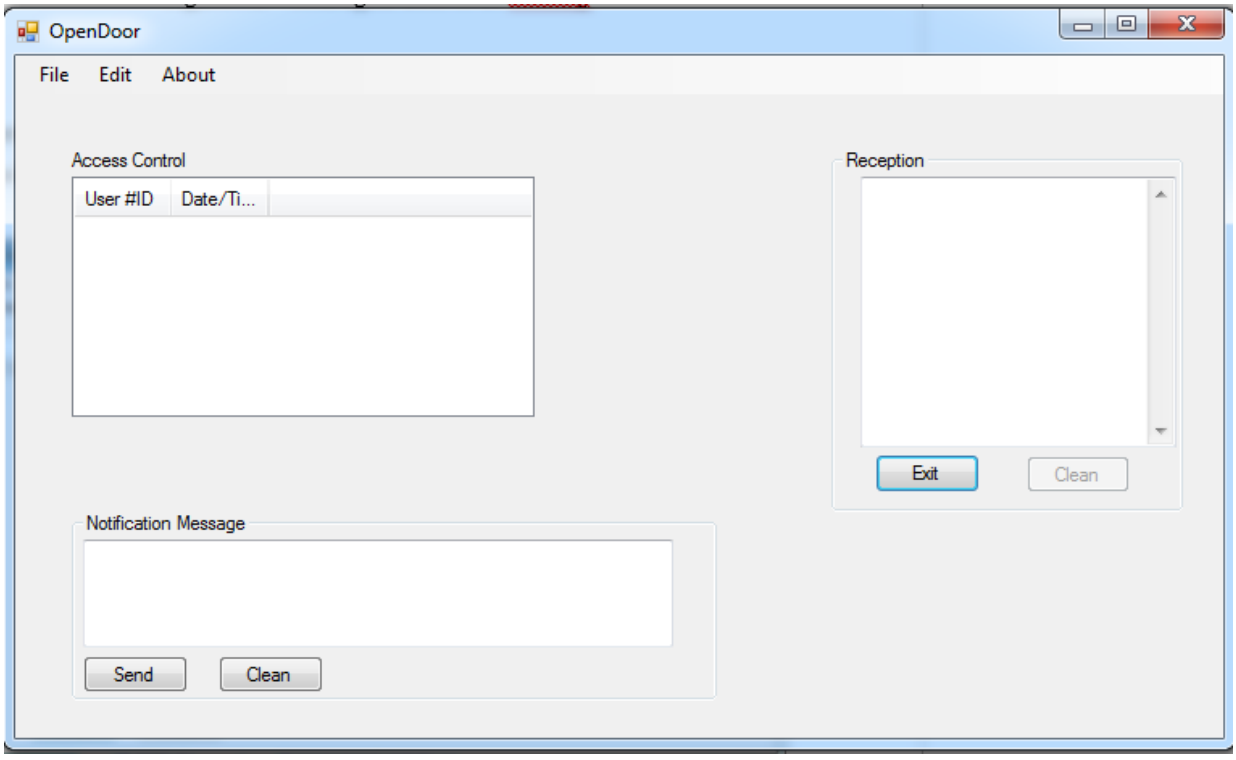


Figura 3.2: Tela inicial do sistema supervisório

Para conectar o microcontrolador ao computador e ter acesso às funcionalidades do supervisório, é necessário fazer um ajuste nas configurações da comunicação serial através de uma aba desenvolvida para edição (Fig. 3.3).

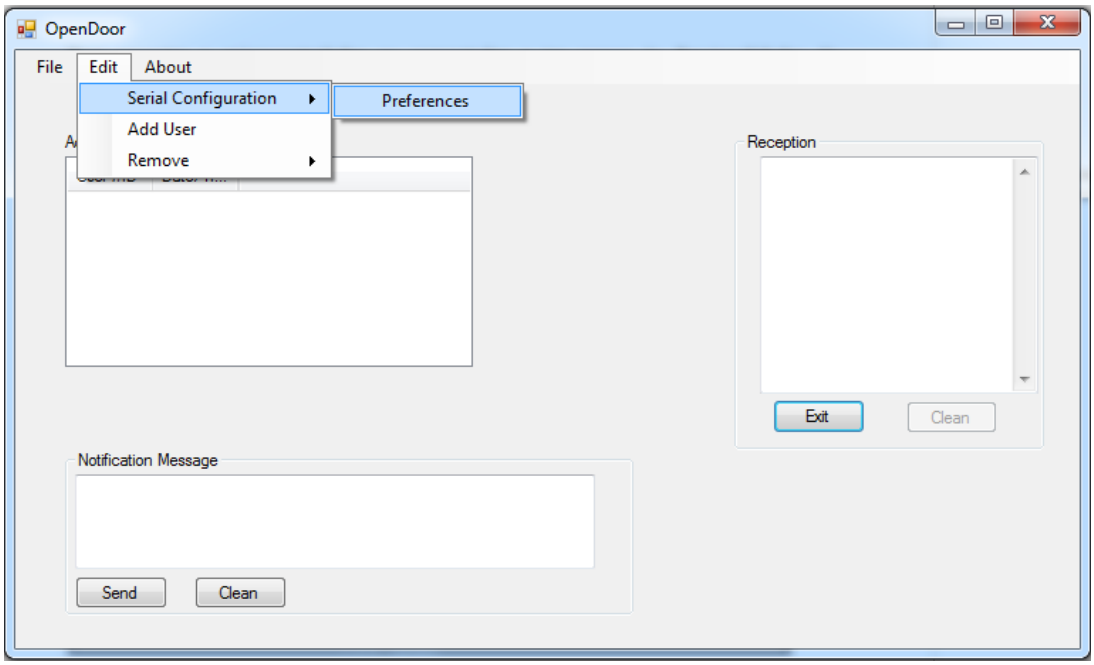


Figura 3.3: Menu para alterar preferências para comunicação serial.

Ao selecionar a opção "*Preferences*", o software automaticamente procurará por alguma porta serial que esteja disponível para conexão e, caso não haja, exibirá uma janela de alerta (Fig. 3.4).

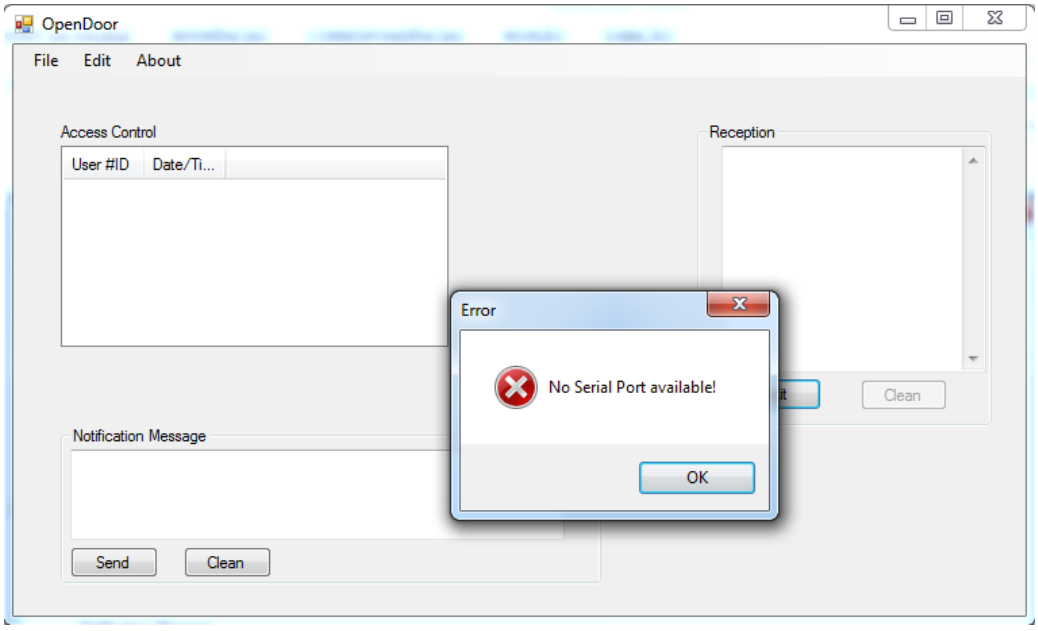


Figura 3.4: Mensagem de alerta

Caso uma porta serial esteja disponível, será necessária a configuração para conexão (Fig. 3.5) e, posteriormente, abertura da porta para que o sistema supervisório passe a operar.

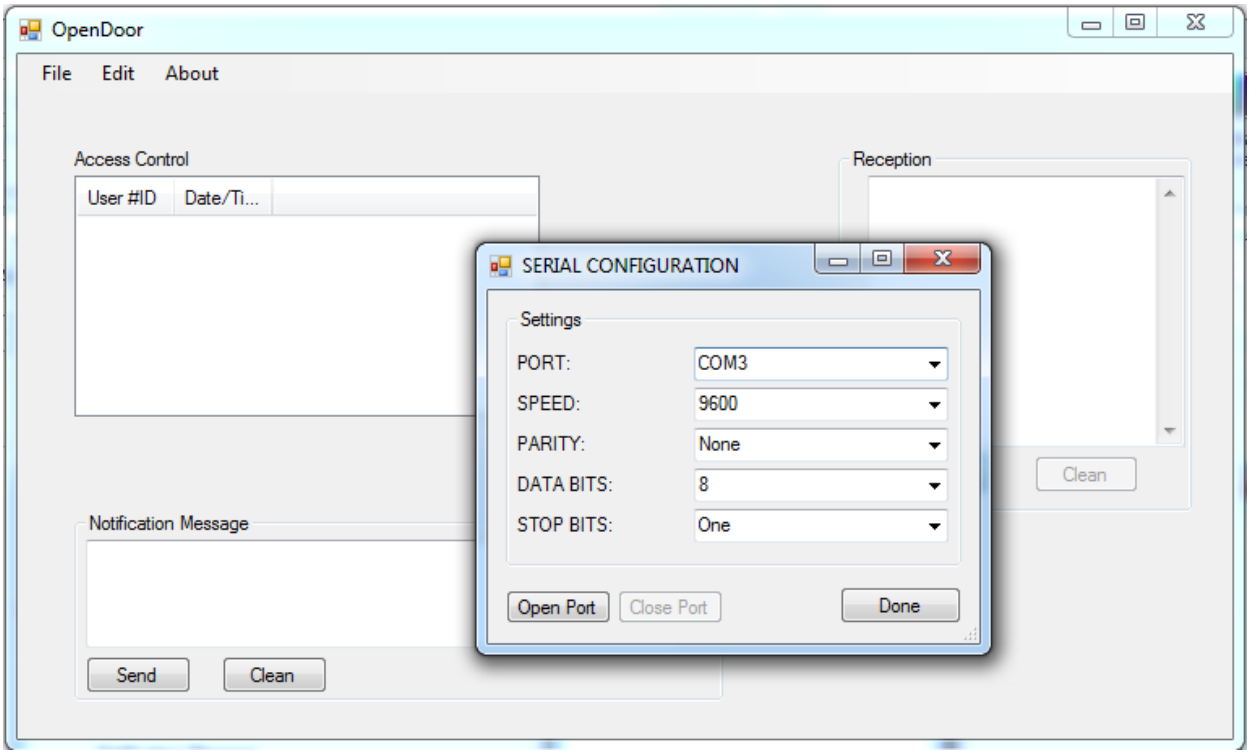


Figura 3.5: Ajuste de preferências para comunicação serial.

Pode-se acompanhar o cadastro de um usuário sendo feito através da janela "*Reception*" (Fig. 3.6), assim como pelo display lcd. Inicialmente é dado um número de identificação único e ainda não utilizado para o usuário. Em seguida, a imagem da digital é capturada e convertida em um template que é armazenado para comparações. É necessária uma segunda captura para validar a digital, e caso coincida com a primeira captura, é armazenada finalizando o cadastro.

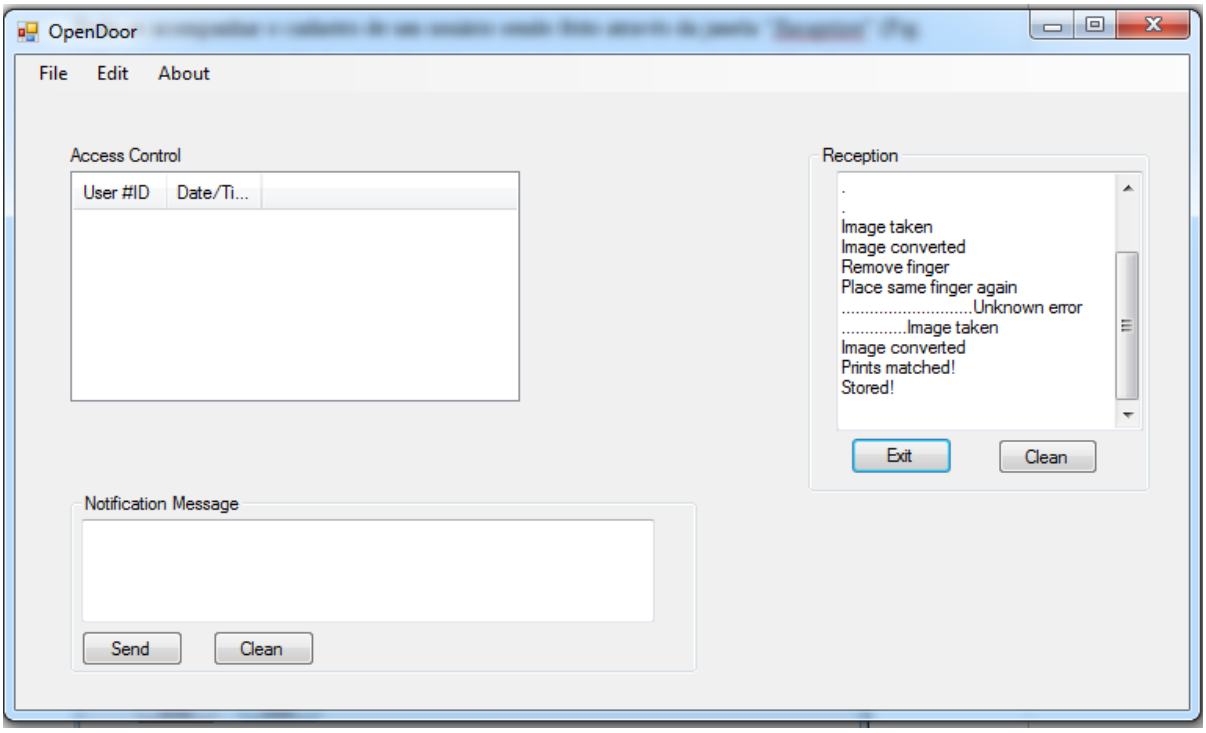


Figura 3.6: Acompanhamento de cadastro de usuário.

Através da aba "*Edit*", é possível selecionar a função "*Remove User*" (Fig. 3.7). Dessa forma, é possível eliminar definitivamente uma digital cadastrada na memória do sensor.

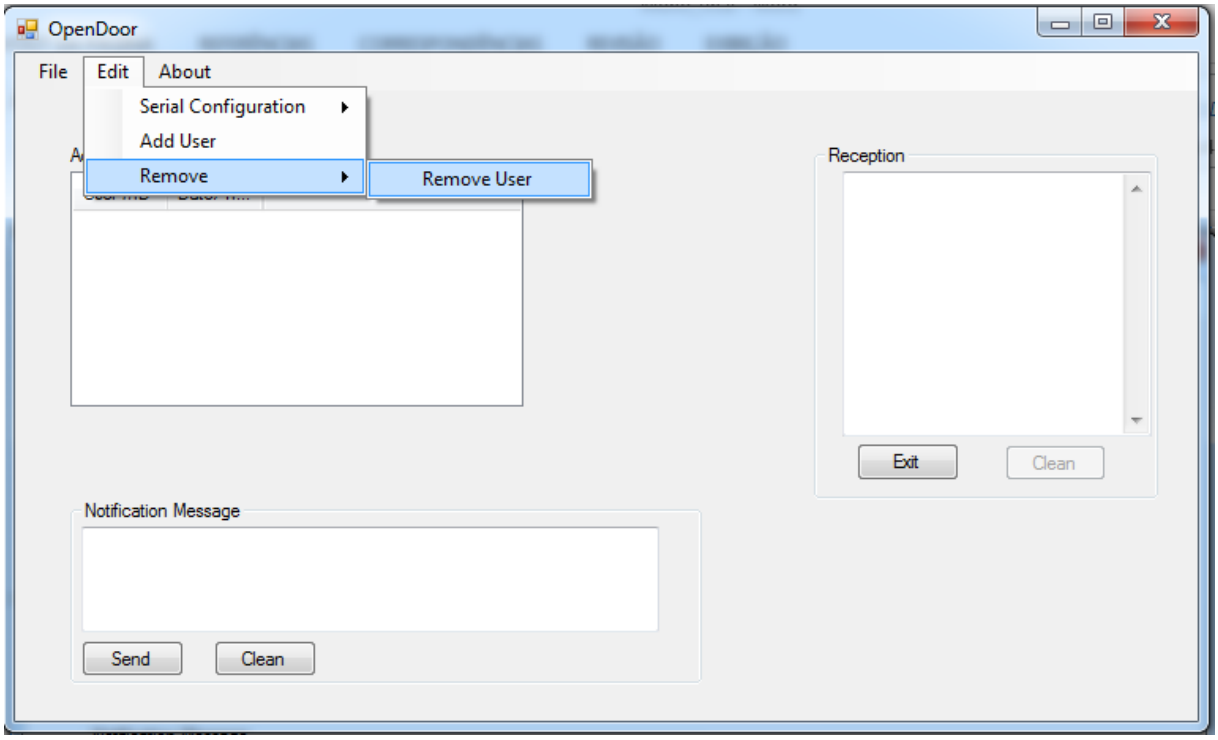


Figura 3.7: Função Remover Usuário

O próximo passo a se seguir para remover o usuário é identifica-lo pelo seu número de identificação, que deve ser digitado no campo que se abrirá na tela principal (Fig. 3.8).

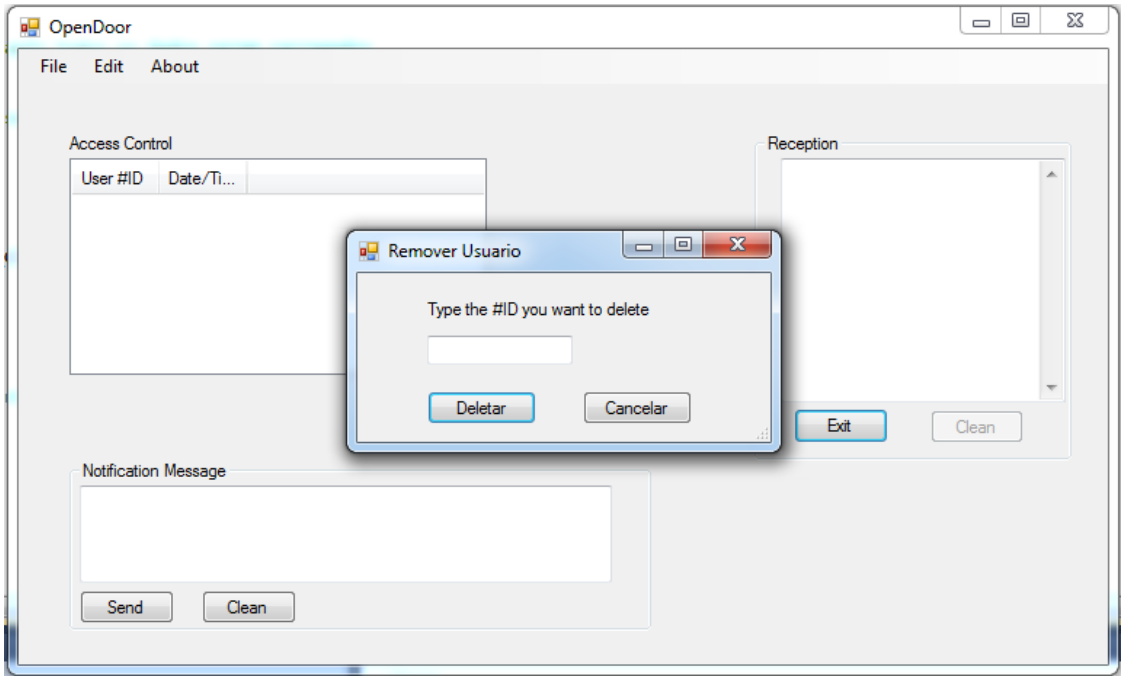


Figura 3.8: Segundo passo para remoção de usuário

Em seguida, uma janela de alerta aparecerá e, caso deseje confirmar a ação, basta selecionar a opção “Sim”. Caso contrário, é dada a opção de cancelar o procedimento (Fig. 3.9).

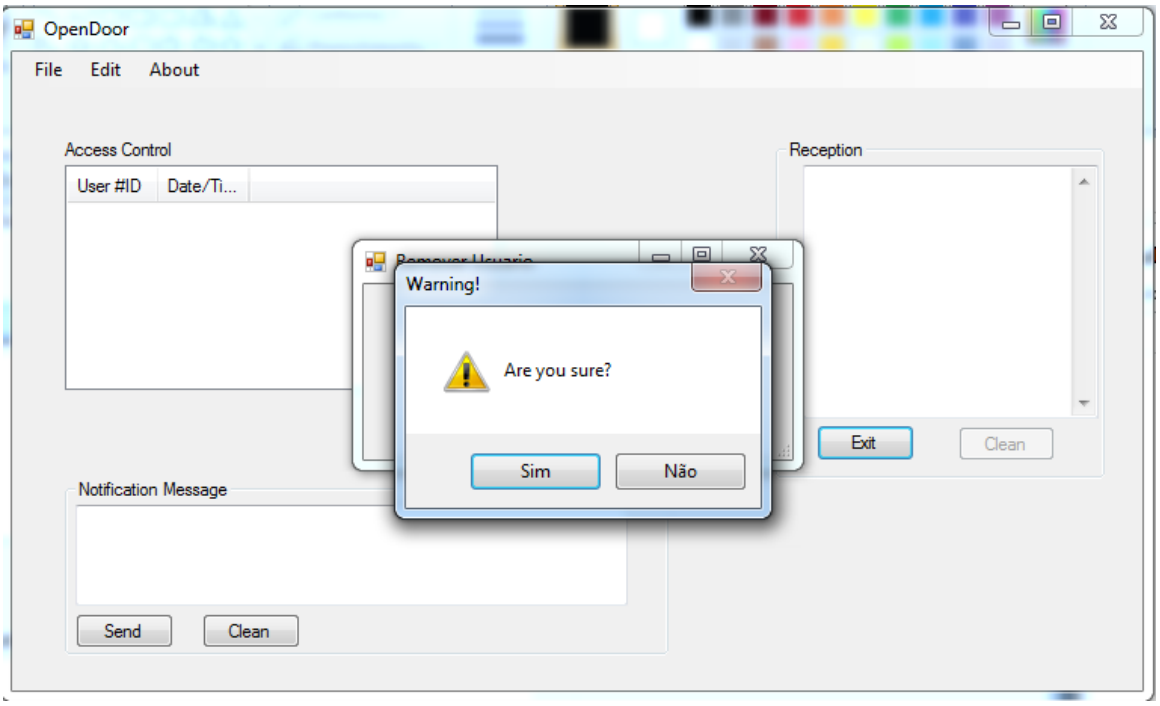


Figura 3.9: Janela de alerta.

A cada acesso realizado e autorizado, a lista responsável pelo controle de acessos será atualizada, informando o número de identificação do usuário, o dia e o momento do acesso, como pode ser visto na Figura 3.10. Ao mesmo tempo, a informação recebida pela serial pode ser vista na janela "*Reception*".

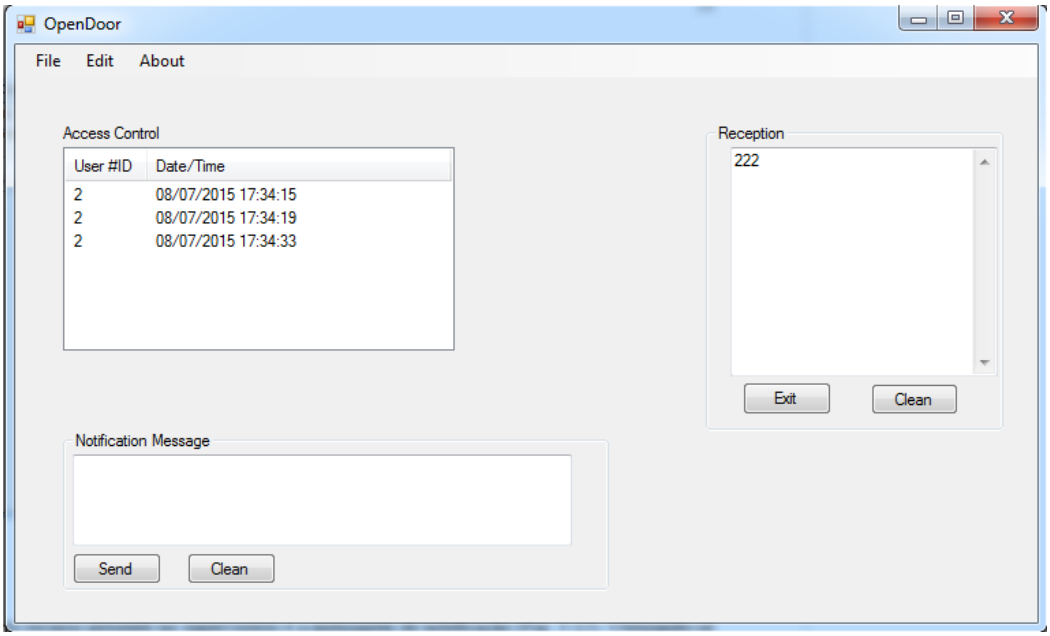


Figura 3.10: Lista com acessos realizados.

Outro recurso presente no supervisório é a mensagem de notificação (Fig. 3.11). Utilizando-se a respectiva "*toolbox*" é possível enviar uma mensagem para ser exibida no display lcd. Para que o envio da mensagem seja confirmado, deve-se selecionar o botão "*Send*", e para limpar a mensagem tanto do supervisório quanto do display, seleciona-se "*Clean*".

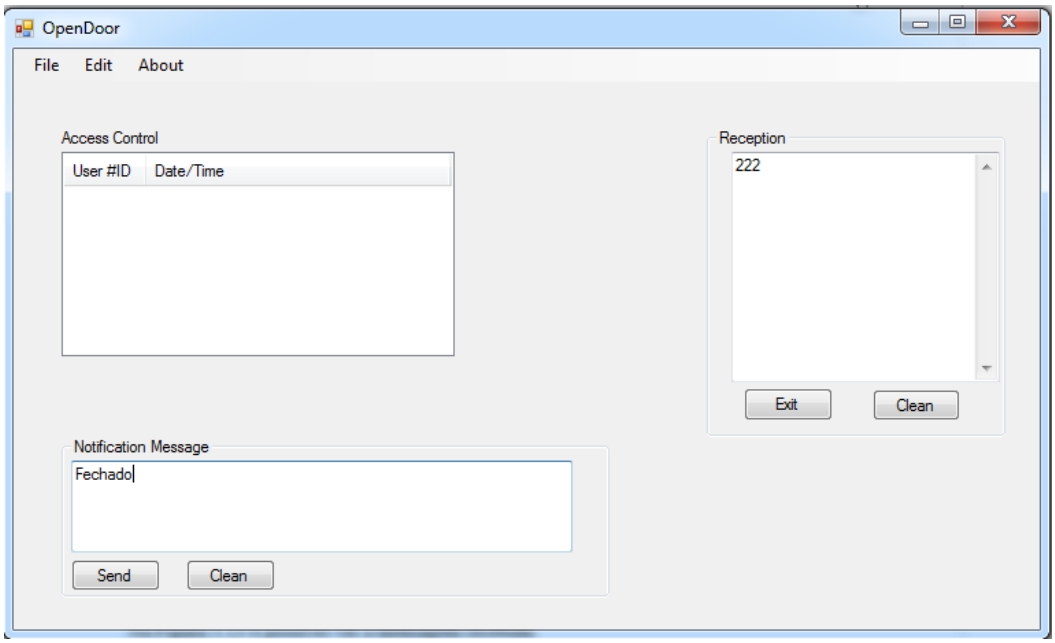


Figura 3.11: Mensagem de notificação.

Na Figura 3.12 é possível ver a mensagem recebida.

Figura 3.12: Mensagem recebida.

Finalmente, é dada a opção de exportar os dados para um arquivo .txt (Fig. 3.13). A seguir, um arquivo será criado de acordo com a vontade do usuário (Fig. 3.14). Dessa forma é possível armazenar informações para uso posterior do administrador.

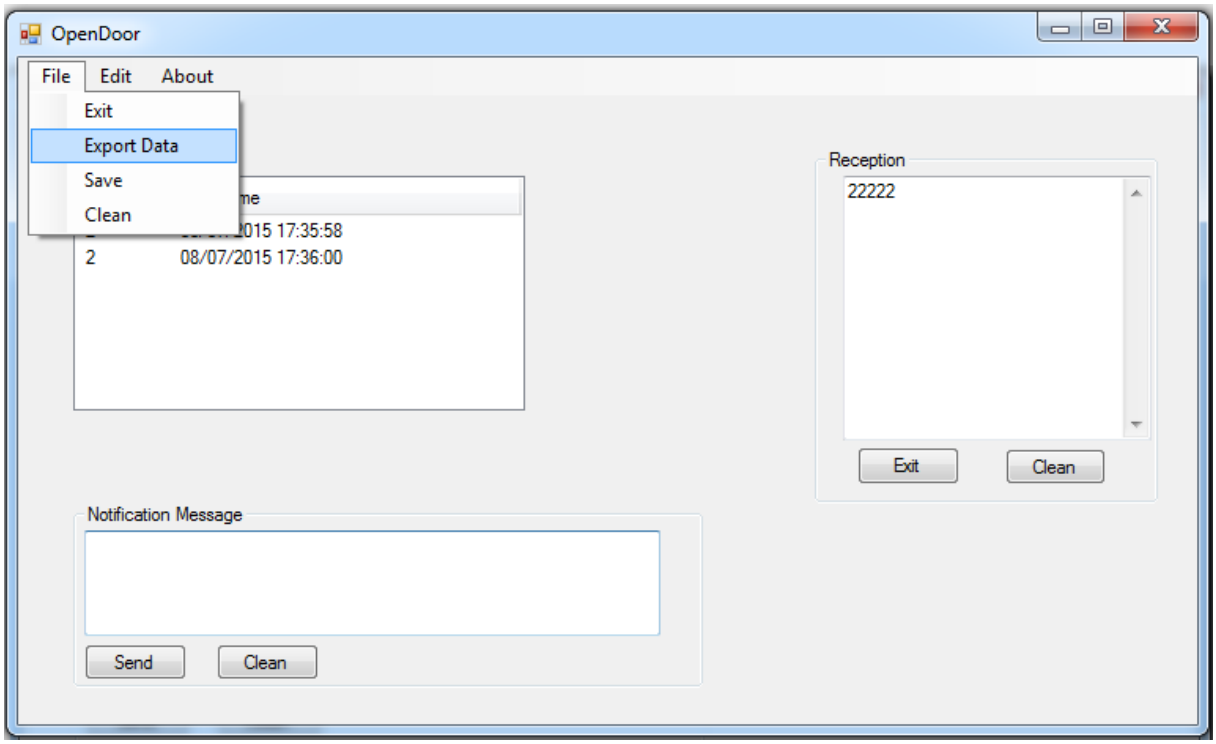


Figura 3.13: Exportar Dados.

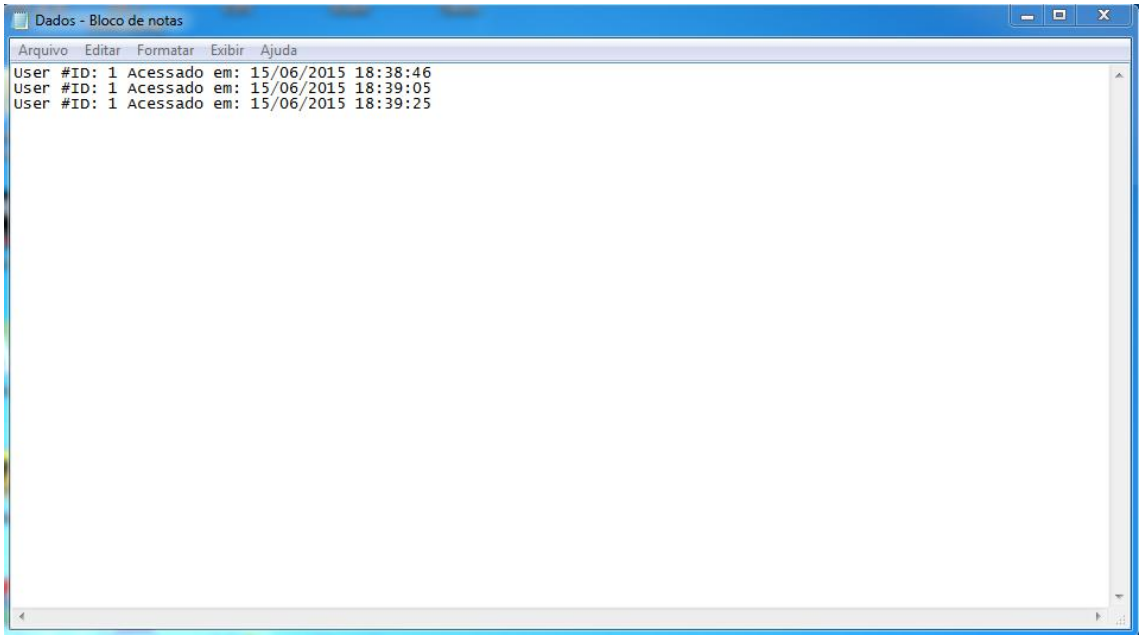


Figura 3.14: Arquivo .txt criado

A aba "*About*" (Fig. 3.15) mostra informação do autor e finalidade do projeto.

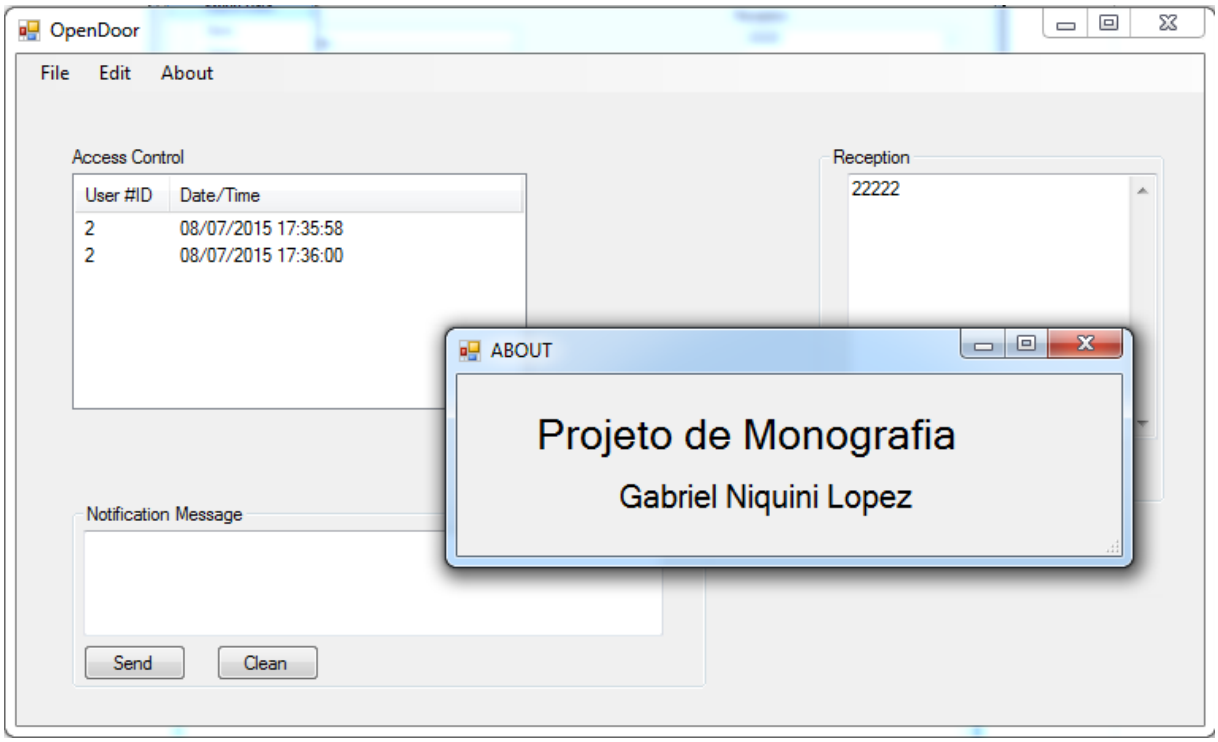


Figura 3.15: Aba "*About*"

4 CONCLUSÃO

Os sistemas de controle de acesso por leitura biométrica oferecem uma alternativa à fechadura convencional, aumentando a segurança, comodidade e praticidade para o usuário.

Com o avanço da tecnologia, esses sistemas vêm se tornando mais econômicos e de fácil acesso ao público, se tornando uma tendência para as residências e ambientes controlados.

O sistema de leitura de impressões digitais especificamente, se demonstrou ser de fácil entendimento, ótima velocidade de leitura, extremamente confiável e de baixo custo, sendo, assim, um projeto de alta viabilidade.

5 SUGESTÕES PARA TRABALHOS FUTUROS

Com o decorrer do desenvolvimento do projeto, novas ideias surgiram com o propósito de oferecer melhorias e agregar mais valor ao sistema desenvolvido.

Como sugestão principal, propõe-se a instalação do sistema em um laboratório da UFOP, de forma que será possível identificar e corrigir falhas, além de permitir a percepção de outras melhorias.

Sugere-se o desenvolvimento de um aplicativo para smartphone para monitoramento remoto de acessos e a inclusão de uma ficha de cadastro incluindo dados pessoais e uma foto. Além disso, para cada tentativa de acesso, seria tirada uma foto que seria armazenada para uso do administrador.

Como sugestão final, propõe-se a criação de um banco de dados contendo o histórico de cada usuário.

REFERÊNCIAS

ADAFRUIT. Disponível em: <http://www.adafruit.com/products/751>. Acesso em: 20 mar. 2015.

ARDUINO E CIA. Disponível em: www.arduinoecia.com.br. Acesso em: 08 jul. 2015.

ATmega328. Disponível em: <http://www.atmel.com/pt/br/devices/ATMEGA328.aspx>. Acesso em: 1 jun. 2015.

COUNCIL, F. F. I. E. Authentication in an Internet Banking Environment. v. 1, n. 703, p. 1–14, 2011.

GAVA, Érika Aparecida. SISTEMAS BIOMÉTRICOS COM ÊNFASE NA TÉCNICA DINÂMICA DA DIGITAÇÃO (KEYSTROKE DYNAMICS). 2006.

JURIZATO, L. A.; PEREIRA, P. S. R. Sistemas supervisórios. v. 7778, p. 105–114, 2003.

LOURENÇO, G. F. F**. Dissertação de Mestrado - Reforço da Segurança das Biométricas utilizando Codificação de Fonte Distribuída.** Instituto Superior Técnico da Universidade de Lisboa. Lisboa, Portugal, 2009.

MAGALHÃES, P. S.; SANTOS, H. D. DOS. Biometria e autenticação. **Actas da 4a CONFERÊNCIA DA ASSOCIAÇÃO PORTUGUESA DE SISTEMAS DE INFORMAÇÃO CAPSI 2003**, v. 2003, p. 2–9354, 2003.

MAGAN, M. V. INTERFACE GRÁFICA PARA COMUNICAÇÃO COM. p. 0–3, 2007.

MICROSOFT. Disponível em: <https://msdn.microsoft.com/pt-br/library/kx37x362.aspx>. Acesso em: 15 jun, 2015.

NATIONAL INSTRUMENTS. Disponível em: <http://digital.ni.com/public.nsf/allkb/32679C566F4B9700862576A20051FE8F>. Acesso em: 19 mai 2015.

OLIVEIRA, A.S.; ANDRADE, F.S. Sistemas Embarcados Hardware e Firmware na Prática. EdÉrica, São Paulo: 2006.

PINHEIRO, J. M. **Biometria nos Sistemas Computacionais**. 1ª Edição. Ciência Moderna, 2008. ISBN: 978-85-7393-738-1

Portal ARDUINO. Disponível em: <http://www.arduino.cc> Acesso em: 10 mai, 2015.

ROMANO, Simone Maria Viana. Sistemas Biométricos aplicados a Segurança da Informação: uma abordagem conceitual sobre os principais dados biométricos.

ROSÁRIO, João Maurício. **Princípios de Mecatrônica**. 1.ed. São Paulo: Prentice Hall, 2005. 355p.

SANCHEZ, M. S. **Monitoramento de temperatura, umidade, luminosidade, nível de ruído e teor de amônia em biotérios utilizando Arduino.** 2014. 103 f. Monografia de graduação, Universidade Federal de Ouro Preto, Ouro Preto, 2014.

SANTOS, F. K.; DA SILVA V.; MARIANA; SANTOS, S. S.; UBIRATAN; JUNIOR O.; JARDENES, F.; LIMA DOS SANTOS, D. **Um componente de software para integrar leitores de biometria a um sistema de controle de acesso**, Pará: 2009.

SANTOS, K. de F. et al. Um componente de software para integrar leitores de biometria a um sistema de controle de acesso. In: **CONGRESSO DE PESQUISA E INOVAÇÃO DA REDE NORTE E NORDESTE DE EDUCAÇÃO TECNOLÓGICA**. 2009.

SILVA, A. P. G; SALVADOR, M. **O que são sistemas supervisórios?.** Elipse Software Ltda, 10 out. 2004. Disponível em: <http://www.elipse.com.br/download/artigos/rt025.04.pdf> Acesso em: 10 de junho de 2014.

SILVA, L. G. C., et al. **Certificação Digital - Conceitos e Aplicações**. Editora Ciência Moderna, 2008. ISBN: 978-85-7393-655-1.

SOUZA F. **Arduino – Primeiros Passos**. Disponível em: <http://www.embarcados.com.br/arduino-primeiros-passos/>. Acesso em: 02 de jun 2014.

SOUZA, F. Arduino – **Entradas e saídas digitais**. Disponível em: <http://www.embarcados.com.br/arduino-entradasaidas-digitais/>. Acesso em: 10 jun 2015.

ZHIANTEC. **ZFM-20 Series Fingerprint Identification Module User Manual**, 2008.