UNIVERSIDADE DE SÃO PAULO
ESCOLA POLITÉCNICA
DEPARTAMENTO DE ENG. DE ENERGIA E AUTOMAÇÃO ELÉTRICAS

RICARDO JANES

ESTUDO SOBRE SISTEMAS DE SEGURANÇA EM INSTALAÇÕES ELÉTRICAS AUTOMATIZADAS

São Paulo
2009

RICARDO JANES

ESTUDO SOBRE SISTEMAS DE SEGURANÇA EM INSTALAÇÕES ELÉTRICAS AUTOMATIZADAS

Dissertação apresentada à Escola Politécnica da Universidade de São Paulo para a obtenção do título de Mestre em Engenharia.

São Paulo
2009

RICARDO JANES

ESTUDO SOBRE SISTEMAS DE SEGURANÇA EM INSTALAÇÕES ELÉTRICAS AUTOMATIZADAS

Dissertação apresentada à Escola Politécnica da Universidade de São Paulo para a obtenção do título de Mestre em Engenharia.

Área de Concentração:
Sistemas de Potência

Orientador: Prof. Dr.
Augusto Ferreira Brandão Júnior

São Paulo
2009

FICHA CATALOGRÁFICA

Janes, Ricardo
Estudo sobre sistemas de segurança em instalações elétri - cas automatizadas / R. Janes. -- São Paulo, 2009.
121 p.

Dissertação (Mestrado) - Escola Politécnica da Universidade de São Paulo. Departamento de Engenharia de Energia e Auto- mação Elétricas.

1. Automação predial 2. Instalações prediais de segurança 3. Biometria I.Universidade de São Paulo. Escola Politécnica. Departamento de Engenharia de Energia e Automação Elétricas II. t.

DEDICATÓRIA

À Dinah, minha esposa, por sua presença ao meu lado nas inúmeras horas dedicadas à elaboração deste trabalho, sempre demonstrando apoio, incentivo e amor.

AGRADECIMENTOS

Ao Prof. Dr. Augusto Ferreira Brandão Júnior, pelas diretrizes seguras, orientação, supervisão, confiança, paciência e oportunidade que me concedeu para o desenvolvimento desta pesquisa e por todo o apoio prestado durante estes anos.

À Escola Politécnica da Universidade de São Paulo, pela oportunidade de realização deste trabalho.

Aos professores do curso de pós-graduação da Escola Politécnica da Universidade de São Paulo, pelo apoio, colaboração, sugestões e discussões levantadas ao longo do período de pesquisa, fundamentais na elaboração e consolidação do trabalho.

À minha família e meus amigos, pela paciência, ajuda, apoio e carinho.

A todos que direta ou indiretamente contribuíram para a elaboração deste trabalho.

“Tudo tem seu tempo e até certas manifestações mais vigorosas e originais entram em voga ou saem de moda, mas a sabedoria tem uma vantagem: é eterna.”

(Baltasar Gracián)

RESUMO

Este trabalho apresenta um estudo sobre os principais sistemas de segurança utilizados em instalações elétricas automatizadas, com enfoque no controle de acesso físico, utilizando tecnologias biométricas. São apresentadas neste trabalho as principais características dos sistemas de segurança aplicados à detecção e combate de incêndios, ao controle do acesso físico, ao controle interno e externo da segurança, como circuitos fechados de televisão e controle de segurança perimetral, e as tecnologias biométricas que podem ser usadas para o controle de acesso de pessoas. É apresentado o desenvolvimento de um protótipo de baixo custo, utilizando tecnologia biométrica para o controle de acesso físico, assim como as principais vantagens e desvantagens, algoritmos e relações custo-benefício para o uso de biometria em sistemas de segurança. O estudo mostra que o uso da biometria como ferramenta para a melhoria dos sistemas de segurança existentes é uma tendência mundial, no entanto, existe uma preocupação crescente sobre a confidencialidade das informações biométricas das pessoas.

Palavras-chave: Automação predial. Automação elétrica. Sistemas de segurança. Biometria. Instalações prediais de segurança.

ABSTRACT

This work presents a study of the main security systems used in automatized electric installations, with approach in the physical access control, using biometric technologies. The main characteristics of the security systems applied to the detection and fire combat, to the physical access control, to the internal and external security control, as closed-circuits television and perimetral security control, and the biometric technologies are presented in this work that can be used for the people access control. The development of a low cost prototype is presented, using biometric technology for the physical access control, as well as the main advantages and disadvantages, algorithms and cost-benefit relations for the use of biometry in security systems. The study shows that the use of the biometry as tool for the existing security systems improvement is a world-wide trend, however, an increasing concern exists of the people biometric information confidentiality.

Keywords: Building automation. Electric automation. Security systems. Biometry. Building security installations.

LISTA DE ILUSTRAÇÕES

LISTA DE ABREVIATURAS E SIGLAS

2D	Duas dimensões ou bidimensional
3D	Três dimensões ou tridimensional
AAM	Active appearance model
ABS	Acrylonitrile butadine styrene
AC	Alternating current
AND	Lógica booleana “e”
CCD	Charge coupled device
CD	Compact disk
CDROM	Compact disk ready only memory
CLP	Controlador lógico programável
CFTV	Circuito fechado de televisão
DAT	Digital audio tape
DC	Direct current
DETRAN	Departamento de trânsito
DNA	Deoxyribonucleic acid
EBGM	Elastic bunch graph matching
EEPROM	Electrically erasable programmable ready only memory
EER	Equal error rate
EM	Expectation-maximization
EP	Evolutionary pursuit
FAR	False accept rate
FRR	False reject rate
GLP	Gás liquefeito de petróleo
GMM	Gaussian mixture models
HD	Hard disk
HMD	Hole mounted device
HMM	Hidden Markov model
IBI	Intelligent Building Institute
ICA	Independent Component Analysis
IP	Internet Protocol

LDA	Linear discriminant analysis
LED	Light emitting diode
OPC	OLE for process control
PCA	Principal Component Analysis
PVC	Polyvinyl choryde
PIN	Personal identification number
RAM	Random access memory
RFID	Radio frequency identification
RISC	Reduced instructions set computer
SMD	Surface mounted device
SVM	Support vector machine
TSE	Tribunal Superior Eleitoral
USB	Universal serial bus
VESDA	Very early smoke detection
VHS	Video home system
XOR	Lógica booleana “ou exclusive”

SUMÁRIO

1 INTRODUÇÃO

A automação industrial surgiu no período da revolução industrial, e teve como principal foco a preparação de máquinas que executassem o mesmo trabalho realizado por um operário, mas com maior velocidade, eficiência e precisão. A partir da década de 80, as principais tecnologias utilizadas na automação industrial deram início à domótica. Este termo resulta da junção da palavra latina “Domus”com robótica, que significa controle automatizado da casa. A domótica é hoje uma tecnologia que visa principalmente simplificar a vida diária das pessoas, proporcionando benefícios e satisfazendo as suas necessidades de conforto, segurança, comunicação e uso racional de energia. A automação aplicada às instalações prediais deram início neste mesmo período. De acordo com o IBI - *Intelligent Building Institute* (1987), os edifícios inteligentes são aqueles que oferecem ambiente produtivo e econômico através da otimização de quatro elementos básicos:

a) Estrutura: componentes estruturais do edifício, elementos de arquitetura, acabamento de interiores e móveis;
b) Sistemas: controle de ambiente, calefação, ventilação, ar-condicionado, luz, segurança e energia elétrica;
c) Serviços: comunicação de voz, dados, imagens, limpeza;
d) Gerenciamento: ferramentas para controlar o edifício, bem como das inter-relações entre eles.

O conceito de domótica foi aplicado nos primeiros edifícios inteligentes, e compreende as seguintes áreas de uma forma integrada:

a) **Conforto**: automação das funções domésticas, controle de iluminação e ar condicionado;
b) **Gestão Energética**: controle e racionalização de consumo de recursos naturais, como água e energia elétrica;

c) **Comunicações:** são consideradas as comunicações internas com o exterior, com o objetivo de integrá-las da forma mais eficiente e global;
d) **Segurança**: visa controlar a segurança patrimonial (intrusão), e técnica (sistemas contra incêndios, inundações, etc).

Verifica-se que de uma forma generalizada, atualmente os prédios tem um controle efetivo da iluminação dos ambientes de uso comum, do ar condicionado, principalmente em edifícios comerciais, do uso dos elevadores, controle e racionalização do consumo de água e energia elétrica e da segurança, entretanto observa-se que na maioria dos casos, tais instalações e serviços funcionam de forma totalmente independente umas das outras, sendo geralmente instaladas em fases diferentes na construção predial, visando assim manter a modernidade das edificações. Para os edifícios em construção que visam atingir um nível de excelência nos termos de edificações inteligentes, e para aqueles que pretendem melhorar suas instalações, se faz necessário amplo estudo de todas as tecnologias existentes na área de automação predial, para que a aplicação do projeto em um edifício tenha uma relação custo-benefício atraente ao mercado nacional. Neste trabalho, o foco dos estudos será a automação dos sistemas de segurança. O termo “instalações automatizadas” é aplicado nesta dissertação visando identificar qualquer ambiente que possa ter seus sistemas de segurança automatizados através da instalação de equipamentos de alta tecnologia, como portos, aeroportos, bancos, universidades e outros, utilizando os mesmos recursos aplicados nos edifícios inteligentes.

1.1 Objetivos

Em uma instalação automatizada, os sistemas de segurança podem ser divididos em diversas áreas de aplicação, como por exemplo: sistemas de detecção e combate a incêndios, sistemas de controle de acesso físico e lógico e sistemas de controle interno e externo da segurança. Como as tecnologias existentes e os fabricantes dos equipamentos para cada área são diferentes, não existem estudos ou documentações que façam uma análise global de toda a infra-estrutura da

segurança de uma instalação automatizada. Assim, os principais objetivos deste trabalho são:

a) Levantar as principais características, vantagens e desvantagens, e relações custo-benefício dos diversos sistemas de segurança aplicados à detecção e combate a incêndios, ao controle de acesso físico utilizando biometria e cartões, ao controle interno e externo da segurança (circuito fechado de televisão, segurança perimetral), dando enfoque principalmente às tecnologias biométricas e suas aplicações no controle de acesso físico;

b) Construir um protótipo utilizando uma tecnologia biométrica para o controle de acesso físico de pessoas em um ambiente educacional.

1.2 Metodologia e estrutura do trabalho

As informações necessárias à pesquisa, contidas nesta dissertação, foram obtidas em diversas fontes, tais como:

a) Dissertações, teses e artigos publicados na área;
b) Pesquisa na internet;
c) Consulta a fabricantes e manuais dos equipamentos;
d) Participação em feiras na área de segurança;
e) Normas e artigos técnicos de órgãos reguladores;
f) Entrevistas com especialistas na área;
g) Livros e revistas especializadas.

O capítulo 2 apresenta um estudo sobre os sistemas de detecção e alarme a incêndios, mostrando os principais tipos de detectores de calor, de fumaça, e outros modelos, além de um resumo sobre as normas técnicas relativas ao tema.

O capítulo 3 apresenta um estudo sobre as tecnologias utilizadas no controle do acesso, com enfoque ao acesso físico. Neste capítulo são apresentadas várias tecnologias biométricas em uso, e a utilização dos cartões eletrônicos.

O capítulo 4 apresenta diversas aplicações tecnológicas da biometria, voltadas à área de segurança, no Brasil e no mundo.

O capítulo 5 apresenta a segurança aplicada ao controle interno das instalações automatizadas. Os sistemas de circuito fechado de televisão são apresentados, e o enfoque neste capítulo se dá no controle perimetral, mostrando as principais tecnologias utilizadas.

O capítulo 6 apresenta um estudo de caso, que consiste em um protótipo utilizando tecnologia biométrica para o controle do acesso físico em um ambiente educacional.

O capítulo 7 concluirá o estudo realizado e apresentado nesta dissertação, após o término do trabalho.

2 SISTEMAS DE DETECÇÃO E ALARME DE INCÊNDIOS

Um sistema de detecção e alarme de incêndios é definido por: *"Sistema constituído pelo conjunto de elementos planejadamente dispostos e adequadamente interligados, que fornece informações de princípios de incêndio, por meio de indicações sonoras e visuais, e controla os dispositivos de segurança e de combate automático instalados no prédio."* (NBR 9441, 1998). Este conjunto de elementos é basicamente formado por um equipamento central de controle, normalmente microprocessado, e diversos sensores e atuadores, capazes de:

a) Alertar o operador do sistema sobre qualquer irregularidade;
b) Gerenciar alarme de incêndio orientando usuários sobre rotas de fugas em função da posição geográfica da ocorrência;
c) Supervisionar níveis de caixas d'água do edifício;
d) Proceder a desenergização do setor danificado, impedindo curto-circuitos que possam contribuir para o alastramento do incêndio;
e) Posicionar os elevadores no andar térreo, ou qualquer outro andar que dê acesso ao usuário à rota de fuga, posicionando-o posteriormente no andar imediatamente abaixo ao atingido, evitando o aumento do incêndio pelo poço do elevador;
f) Acionar o sistema de insuflamento de ar nas escadas de emergência, impedindo que estas sejam invadidas pela fumaça;
g) Informar aos setores responsáveis pelo combate ao incêndio, através de telefone ou rádio;
h) Pressurizar a linha de água de hidrantes e *sprinklers* (difusores de água instalados no teto do pavimento).

Para que o sistema de detecção e alarme a incêndios atenda aos requisitos da norma NBR 9441/1998, o mesmo deve conter:

a) Instalação de uma central principal, concentrando todos os alarmes e controles;

b) Detecção automática de anormalidades nos ambientes supervisionados;
c) Acionadores manuais localizados em pontos estratégicos, para que pessoas possam solicitar socorro;
d) Indicação de rotas de fuga para as pessoas nas áreas de perigo.

Um sistema completo de detecção e alarmes de incêndios é composto por uma central microprocessada e diversos equipamentos detectores, formando laços. O número de dispositivos detectores instalados em um laço depende das características da central de controle utilizada, porém a norma NBR 9441/1998 estabelece um número máximo de vinte dispositivos por laço.

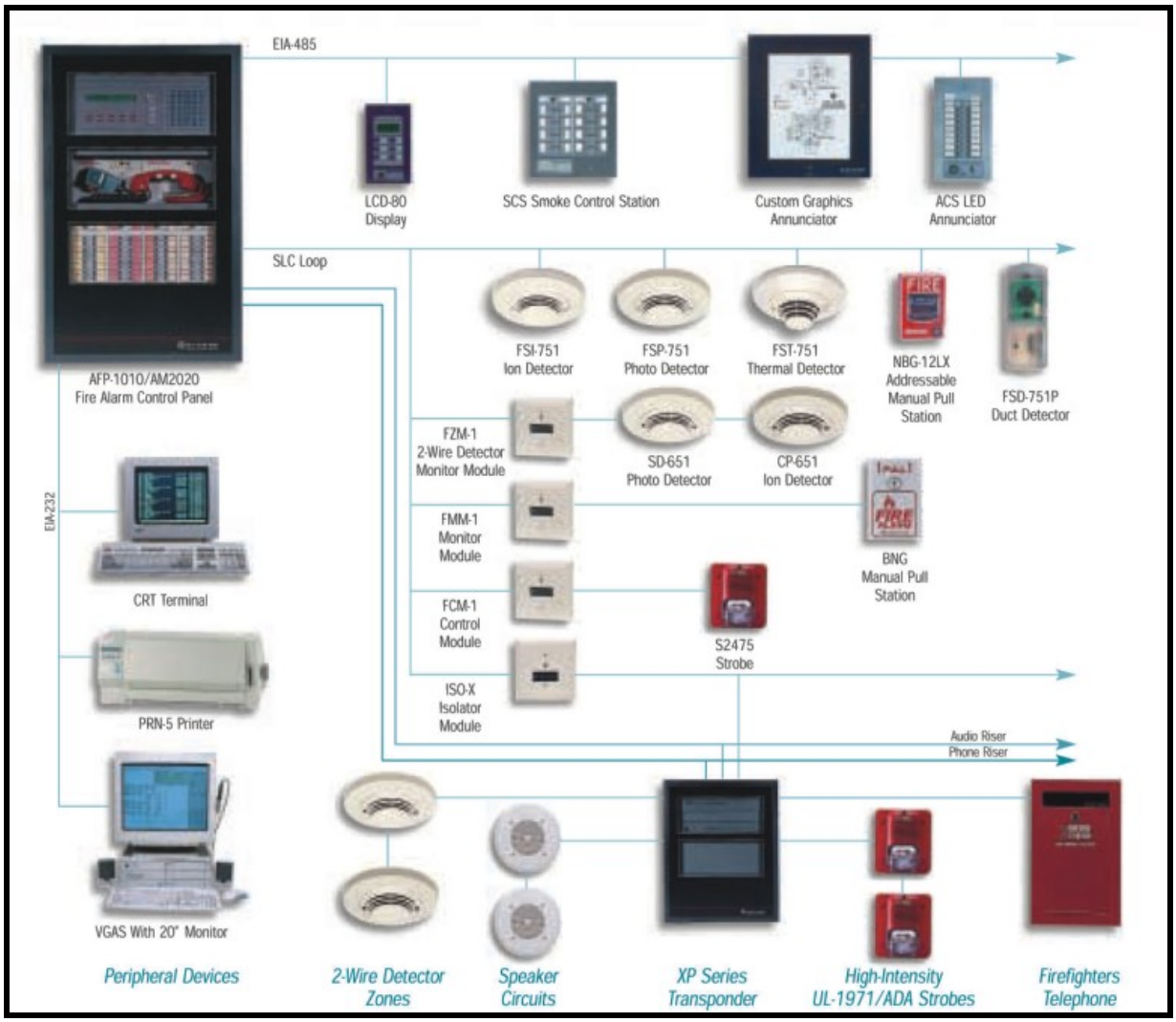


Figura 2.1 – Sistema de detecção e alarme a incêndios

2.1 Tipos de detectores de incêndio

De acordo com a Norma NBR 11836/1992, os detectores pontuais formam os laços de controle e são dispositivos que registram e analisam automaticamente a presença ou variação de certos fenômenos físicos ou químicos, transmitindo estas informações à Central de Controle, e são agrupados em detectores:

a) De temperatura;
b) Lineares;
c) De fumaça;
d) Por aspiração;
e) Multisensores.

2.1.1 Detectores de temperatura

Sua ativação ocorre quando a temperatura ambiente ou o gradiente da temperatura ultrapassa um valor pré-determinado. Podem ser classificados como detectores térmicos ou velocimétricos.

2.1.1.1 Detectores térmicos

São fabricados com um termistor interno, responsável pela medição da temperatura do ambiente onde são instalados. Estes dispositivos devem ser instalados em ambientes onde a ultrapassagem de determinada temperatura indique seguramente um princípio de incêndio. Os detectores térmicos só passam para o estado de alarme com temperaturas pré-estabelecidas. Os detectores de temperatura em geral possuem largas aberturas para facilitar a entrada do ar, que deve circular em seu interior, entrando em contato com o termistor interno.

Figura 2.2 – Detector térmico de temperatura

2.1.1.2 Detectores velocimétricos

Os detectores de temperatura velocimétricos podem ser ajustados e constituem-se de um par de termistores calibrados, o qual o primeiro está exposto à temperatura ambiente e o segundo está selado em uma câmara de construção especial para que o gradiente de temperatura neste elemento seja maior. Em condições normais, os dois termistores registram temperaturas iguais, mas na ocorrência de incêndio, o termistor exposto registrará um aumento de temperatura rapidamente, causando desbalanceamento em relação ao termistor selado, fazendo com que o dispositivo acione seu estado de alarme. São utilizados onde o ambiente está sujeito à presença de fumaça ou poeira e onde o gradiente da temperatura indique um princípio de incêndio (8 ºC a 10 ºC por minuto), por exemplo, em salas de aquecimento, cozinhas e lavanderias. Este tipo de equipamento foi idealizado para detectar o fogo assim que a temperatura aumentar rapidamente, mas também existe um limite máximo fixo, no qual o detector passará ao estado de alarme, mesmo que o aumento de temperatura tenha sido lento. Sua funcionalidade o caracteriza como dispositivo de dupla ação.

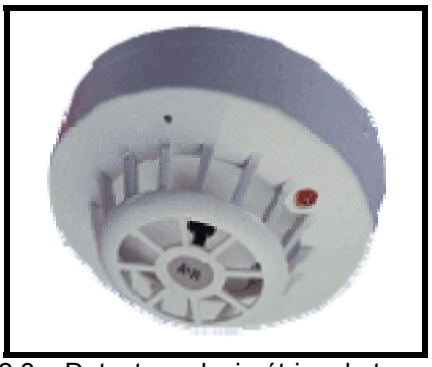


Figura 2.3 – Detector velocimétrico de temperatura

2.1.2 Detectores lineares de temperatura

Consistem em um cabo que tem em sua construção física, pequenos sensores de temperatura, que são alocados em intervalos regulares como um barramento de dados e de alimentação. Este cabo é um sistema integrado de aquisição e barramento, e tem grande resistência à poluição ambiente. (SECURITON, 2007).

Figura 2.4 – Detector linear de temperatura

O monitoramento dos sinais dos sensores no cabo é realizado pela central de controle de forma contínua, efetuando o registro dos últimos valores medidos. Uma lógica de avaliação, interna à central, usa os valores obtidos para determinar quando deve indicar uma falha ou alarme.

Um *software* especial é utilizado para configuração, e o sistema pode ser conectado a um microcomputador ou ao painel de controle de incêndio. Este tipo de detector pode ser usado principalmente para medidas em longas distâncias, por exemplo:

a) Túnel para automóveis, trens e metrôs;
b) Estacionamentos e plantas refrigeradas;
c) Linhas de manufatura, refinarias;
d) Plantas de incineração, linhas de gás e aquecimento.

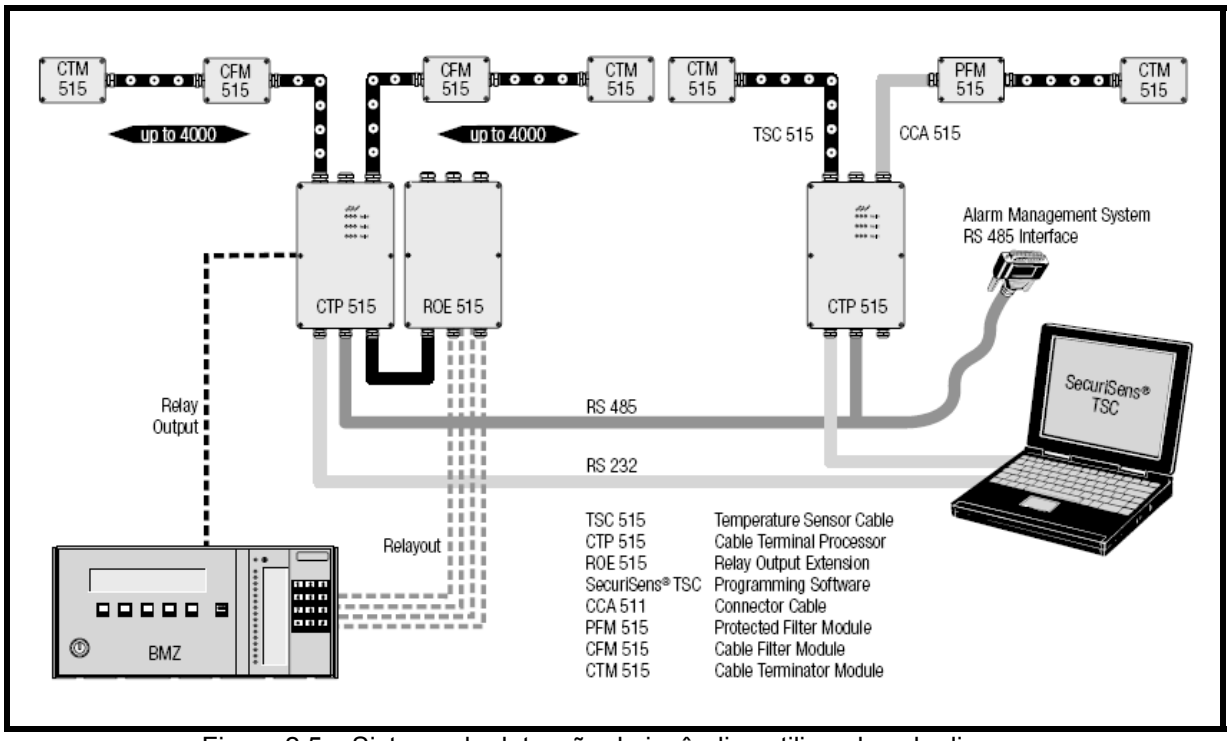


Figura 2.5 – Sistema de detecção de incêndios utilizando cabo linear

2.1.3 Detectores de fumaça

São dispositivos responsáveis pela detecção de partículas ou gases, visíveis ou não, e de produtos da combustão, provenientes da queima de diversos componentes no local da instalação dos mesmos. Os detectores de fumaça têm sua ação prejudicada se no ambiente em que o mesmo for instalado tiver um grande fluxo de ar, portanto, em ambientes com ar condicionado ou ventilação forçada, o detector deve ser instalado próximo ao retorno deste fluxo. Existem vários tipos de detectores de fumaça, específicos para cada produto da combustão. Podem ser classificados como detectores iônicos e óticos.

2.1.3.1 Detectores iônicos de fumaça

São dispositivos responsáveis pela detecção de produtos de combustão visíveis ou invisíveis, tendo como princípio de funcionamento a detecção iônica. Em seu interior,

têm-se duas câmaras, sendo a primeira uma câmara de referência, montada com uma lâmina de ***Americium 241*** de baixa atividade, e a segunda, uma câmara de análise. Quando o dispositivo é ligado, existe o fluxo de corrente elétrica entre as câmaras, e assim que a fumaça entra no detector, seja ela visível ou não, fará com que o fluxo de corrente entre as câmaras diminua, e então o dispositivo detectará esta variação, fazendo com que o circuito entre em estado de alarme. (EZALPHA, 2006).

Figura 2.6 – Detector iônico de fumaça

2.1.3.2 Detectores óticos de fumaça

Este tipo de dispositivo é responsável por detectar apenas a fumaça visível. Baseia-se na técnica de dispersão de luz. No interior de uma câmara em forma de labirinto, responsável pela exclusão de qualquer luz de origem externa, existe um emissor de luz pulsante do tipo *led*, emitindo luz infravermelha e um foto-diodo, responsável por detectar a luz emitida pelo *led.* A luz emitida pelo *led* não é registrada pelo foto-diodo, pois os mesmos não estão em alinhamento, mas na presença de fumaça, o impulso do *led* se dispersa, fazendo com que a luz atinja o foto-diodo, e este, se acionado por mais de dois pulsos (seguintes), coloca o detector no estado de alarme.

Figura 2.7 – Detector ótico de fumaça

2.1.4 Detectores por aspiração

Estes dispositivos contam com unidades de controle próprias, que visam detectar um incêndio em seu estágio incipiente ou pré-combustão. Nesses sistemas o ar é aspirado através de dutos para dentro de uma câmara sensível, onde é analisada a quantidade de partículas de fumaça em suspensão. São indicados para casos em que se exija uma antecipação muito grande de um incêndio. Em edifícios de alto padrão, estes dispositivos podem ser utilizados visando melhorar o aspecto estético, com a diminuição de detectores espalhados ao longo do teto. Este sistema também é conhecido por seu termo em inglês como VESDA (*Very Early Smoke Detection*). (EQUIPEX, 2007).

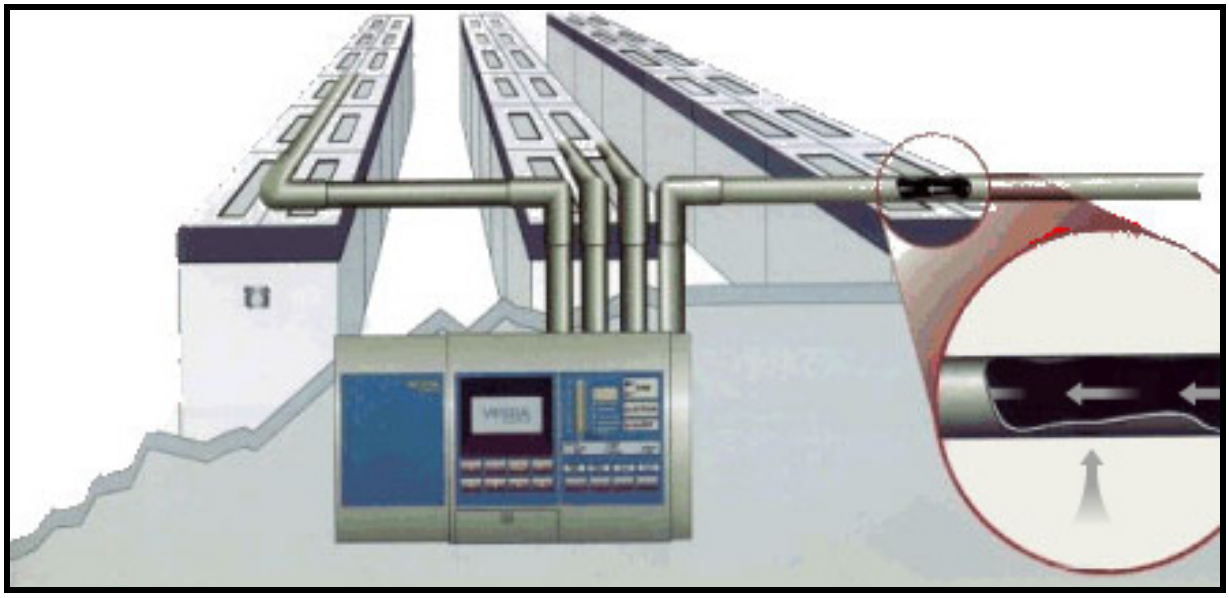


Figura 2.8 – Detector de fumaça por aspiração

2.1.5 Detectores *Multisensor*

A tecnologia *multisensor, ou* sensores híbridos de incêndio, combinam em um único detector todas as funções específicas dos detectores convencionais iônicos, ópticos e térmicos, permitindo a detecção de incêndios de diferentes procedências e características com maior sensibilidade.

Cada detector *multisensor* possui um microprocessador que filtra sinais não típicos de um incêndio e diminui alarmes falsos simultaneamente, oferecendo a vantagem de um sistema de detecção analógica.

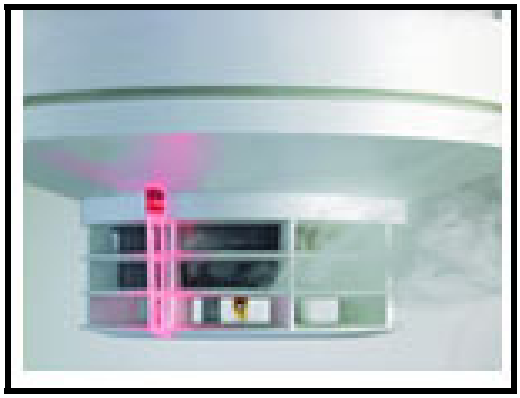


Figura 2.9 – Detector multisensor

2.2 Acionadores Manuais

São dispositivos destinados a transmitir a informação de emergência, quando acionados manualmente. Estes equipamentos devem possuir as seguintes características:

a) Ser compatível, lógica e eletricamente, com o circuito de detecção;
b) Ser instalada em caixa pintada nas cores padronizadas, com tampa frontal de proteção em vidro não removível e transparente;
c) Ter acionamento através de alavanca frontal sem retorno, ou botão com travamento;
d) Possuir contatos resistentes à degradação de queima por centelhamento;
e) Possuir dispositivo de segurança que impeça o acionamento acidental.

Devem ser instalados em locais de maior probabilidade de trânsito de pessoas em caso de emergência, tais como: nas saídas de áreas de trabalho, áreas de lazer, em corredores, saídas de emergência para o exterior, etc. A distância máxima a ser percorrida em qualquer ponto da área protegida, até o acionador manual mais próximo, não deve ser superior a 16 metros e a distância entre acionadores manuais não deve ultrapassar 30 metros. Os dispositivos do sistema de detecção

capazes de identificar individualmente o dispositivo acionado, interligado a uma central, são denominados como endereçáveis. Esta característica tem se tornado muito comum e de grande utilidade nos procedimentos de operação e manutenção do sistema. Essa funcionalidade pode ajudar na localização mais precisa dos pontos de monitoração de focos de irregularidades. (NBR 13848/1997).

Figura 2.10 – Acionador manual de alarme de incêndios

2.3 Centrais de controle e supervisão

Os sistemas de detecção e alarmes de incêndios são controlados principalmente por centrais de controle e supervisão microprocessadas, mas também podem ser utilizados Controladores Lógicos Programáveis (CLPs), no entanto, este equipamento tem seu uso mais específico para aplicações industriais.

A central de controle e supervisão é destinada a processar e supervisionar os sinais provenientes dos detectores, e dispositivos de campo, convertendo-os em sinalizações adequadas, comandando e controlando os demais componentes do sistema de detecção e alarmes, bem como suas interfaces com outros sistemas.

As interfaces para os dispositivos desse sistema são:

a) Interface com sensores óticos de fumaça e termo-velocimétricos (detector atua com variações rápidas de temperatura);
b) Interface com botoeiras de alarme;
c) Saída para sirene;
d) Saída para sistema de combate;

e) *Reset* de laço de sensores convencionais;
f) Bloqueio do sistema de ar condicionado;
g) Interface com sistema de automação de *site*.

As principais indicações luminosas da central são:

- ✓ Fogo Geral;
- ✓ Defeito Geral;
- ✓ Pré-alarme;
- ✓ Defeito de laço no *display*;
- ✓ Sistema ligado;
- ✓ Alarme de defeito no *display*;
- ✓ Falta de alimentação;
- ✓ Avanço no *display*;
- ✓ Defeito no sistema.

As centrais devem estar localizadas em áreas de rápido acesso, como salas de controle, salas de segurança ou bombeiros, portaria principal de edifícios, sob vigilância constante de operadores habilitados e treinados. Em ambientes não assistidos, devem ficar junto à central de automação da estação, próximas aos quadros de energia AC e DC, tipicamente situados próximos à porta de entrada da estação. No interior das centrais só poderão ser instaladas baterias seladas.

A área de instalação da central não deve estar próxima a materiais inflamáveis ou tóxicos, deve ser ventilada e protegida contra a penetração de gases e vapores. O local de instalação da central deve ter rotas de fuga seguras para os operadores. O local da instalação da central deve permitir a rápida comunicação entre este e o Corpo de Bombeiros ou Brigada de Incêndio. Deve-se prever um espaço livre mínimo de um metro quadrado em frente à central, destinado à manutenção preventiva e corretiva.

Na atuação de um detector, a central deve comandar automaticamente o desligamento do sistema de ventilação, ar condicionado e o fechamento dos *dampers* corta-fogo, da área em alarme. Em estações não assistidas o sistema de combate automático de incêndio deverá temporizar aguardando um comando do

centro de operação para inibir a liberação do gás de extinção de incêndio. Não ocorrendo a inibição local ou remota, o sistema irá liberar toda carga do gás, sinalizando ao centro de operação o evento. (NBR 9441/1998).

Figura 2.11 – Centrais de controle e supervisão

2.4 Normas relativas à prevenção de incêndios

Abaixo, são apresentadas as principais normas relativas à prevenção de incêndios, para posterior aprofundamento nos estudos sobre este tema:

- ✓ NBR 10897 - Proteção contra Incêndio por Chuveiro Automático;
- ✓ NBR 10898 - Sistemas de Iluminação de Emergência;
- ✓ NBR 11742 - Porta Corta-fogo para Saída de Emergência;
- ✓ NBR 12615 - Sistema de Combate a Incêndio por Espuma.
- ✓ NBR 12692 - Inspeção, Manutenção e Recarga em Extintores de Incêndio;
- ✓ NBR 12693 - Sistemas de Proteção por Extintores de Incêndio;
- ✓ NBR 13434: Sinalização de Segurança contra Incêndio e Pânico - Formas, Dimensões e cores;
- ✓ NBR 13435: Sinalização de Segurança contra Incêndio e Pânico;
- ✓ NBR 13437: Símbolos Gráficos para Sinalização contra Incêndio e Pânico;
- ✓ NBR 13523 - Instalações Prediais de Gás Liquefeito de Petróleo;
- ✓ NBR 13714 - Instalação Hidráulica Contra Incêndio, sob comando.
- ✓ NBR 13714: Instalações Hidráulicas contra Incêndio, sob comando, por Hidrantes e Mangotinhos;

- ✓ NBR 13932 - Instalações Internas de Gás Liquefeito de Petróleo (GLP) - Projeto e Execução;
- ✓ NBR 14039 - Instalações Elétricas de Alta Tensão
- ✓ NBR 14276: Programa de brigada de incêndio;
- ✓ NBR 14349: União para mangueira de incêndio - Requisitos e métodos de ensaio
- ✓ NBR 5410 - Sistema Elétrico.
- ✓ NBR 5419 - Proteção Contra Descargas Elétricas Atmosféricas;
- ✓ NBR 5419 - Sistema de Proteção Contra Descargas Atmosféricas (Pára-raios).
- ✓ NBR 9077 - Saídas de Emergência em Edificações;
- ✓ NBR 9441 - Sistemas de Detecção e Alarme de Incêndio;
- ✓ NR 23, da Portaria 3214 do Ministério do Trabalho: Proteção Contra Incêndio para Locais de Trabalho;
- ✓ NR 23, da Portaria 3214 do Ministério do Trabalho: Proteção Contra Incêndio para Locais de Trabalho.

2.5 Instruções Técnicas válidas apenas para São Paulo

Abaixo, são apresentadas as instruções técnicas relativas ao controle e prevenção de incêndios, válidas somente no Estado de São Paulo:

- ✓ Instrução Técnica CB-01-33-94: Transição do DE 20.811/83 para o DE 38069/93;
- ✓ Instrução Técnica CB-02-33-94: Proteção Contra Incêndio para Estruturas Metálicas;
- ✓ Instrução Técnica CB-04-33-95: Sobre Procedimento Simplificado para aprovação e vistoria;
- ✓ Instrução Técnica CB-01-33-96: Auto de Vistoria do Corpo de Bombeiros;
- ✓ Instrução Técnica CB-05-33-97: Procedimentos para análise de Proposta de Proteção Contra Incêndio;
- ✓ Instrução Técnica CB-06-33-97: Alarme de Incêndio em Edificações;
- ✓ Instrução Técnica CB-07-33-97: Saídas de Emergência em Edificações;

- ✓ Instrução Técnica CB-08-33-98: Sistemas de Mangotinhos;
- ✓ Instrução Técnica CB- 9-33-98: Tubulação de Cobre nos Sistemas de Hidrantes;
- ✓ Instrução Técnica CB- 010-33-99: Pressurização de Escadas de Segurança;
- ✓ Instrução Técnica CB-011-33-99: Segurança Estrutural dos Edifícios - Resistência ao Fogo dos Elementos Construtivos;
- ✓ Instrução Técnica CB - 012-33-99: Procedimentos para Avaliação de Proposta de Proteção contra Incêndio e Vistoria de Instalações de GLP com Abastecimento a Granel;
- ✓ Instrução Técnica nº. CB-013-33-00: Utilização de Tubulação de Aço Galvanizado de Diâmetro Nominal de 50 mm;
- ✓ Instrução Técnica n.ºCB-014-33-00: Dimensionamento de Lotação e Saídas de Emergência em recintos de eventos desportivos e de espetáculos Artístico-Culturais.

3 CONTROLE DE ACESSO

O controle de acesso pode ser dividido em duas categorias:

a) Controle do acesso físico – se refere ao controle da entrada de pessoas em clubes, bancos, residências, museus, *shopping centers*, eventos esportivos, hospitais, prisões, edifícios e escolas;
b) Controle do acesso lógico – refere-se ao controle do acesso aos computadores, redes de computação, telefones móveis, *e-mail*, dados confidenciais e serviços bancários (informática).

O controle de acesso físico pode ser obtido através de pessoas, como por exemplo um segurança; através de meios mecânicos como fechaduras e chaves; ou através de outros meios tecnológicos, como sistemas baseados em cartões de acesso e utilização de *tokens*. Em todos os casos, o controle realizado envolve liberação do bloqueio físico e a detecção da passagem da pessoa. Os dispositivos mecânicos mais utilizados atualmente para o controle de acesso físico são as catracas e os torniquetes. Existem ainda as cancelas, que são utilizadas para o controle de acesso de veículos. A liberação mecânica destes dispositivos depende basicamente da identificação e autenticação do usuário. Neste trabalho, o estudo terá maior concentração no controle do acesso físico de pessoas, através da utilização de tecnologias biométricas como forma de identificar e autenticar os usuários, para que meios mecânicos liberem sua passagem.

Figura 3.1 – Catraca e torniquete utilizados no controle de acesso

3.1 Biometria - Sistemas biométricos

Biometria pode ser definida como sendo as mensurações fisiológicas e as características de comportamento que podem ser utilizadas para verificação de identidade de um indivíduo. Permite identificar uma pessoa pela análise das características físicas individuais tais como impressões digitais, contornos da face, geometria da mão, reconhecimento da íris, retina e voz, etc. (LIU, 2001). Os equipamentos responsáveis por efetuar a leitura destas características e interpretá-las, reconhecendo assim a pessoa que utiliza o dispositivo, geralmente visam implementar sistemas de segurança voltados ao controle de acesso. Para que a leitura de uma característica física ou biológica humana seja caracterizada como biometria, devem ser respeitados os seguintes requerimentos:

a) Universalidade: cada pessoa obrigatoriamente deve possuir a característica em estudo;
b) Distinção: essa característica deve ser suficientemente diferente de uma pessoa para outra, em termos de característica;
c) Permanência: as características devem ser suficientemente invariantes durante certo período de tempo;
d) Coletabilidade: a característica pode ser medida quantitativamente.

Ainda existem outros fatores que devem ser considerados em um sistema biométrico, como:

a) Desempenho: a leitura da característica, seu reconhecimento e precisão, e a velocidade de todo o processamento do sinal, devem ser levados em consideração;
b) Aceitabilidade: indica o nível de aceitação da pessoa em utilizar a tecnologia de identificação biométrica;
c) Segurança: o sistema deve ser avaliado para identificar se existem métodos fraudulentos que possam causar uma falsa identificação. (RIHA; MATYAS, 2000).

A verificação por biometria por ser efetuada de dois modos:

Autenticação – modo 1:1

O algoritmo recebe um número de identificação (*PIN – Personal identification number*), por digitação em um teclado convencional, ou por leitura de cartões magnéticos, por código de barras, *smartcards* e outros, e em seguida a leitura de alguma característica biométrica, e então busca em um banco de dados de informações biométricas a imagem previamente armazenada, associada àquele número, para posteriormente comparar as imagens e determinar se elas são da mesma pessoa.

Identificação – modo 1: N

O algoritmo recebe a característica biométrica e pesquisa em um banco de dados de biometria se existe previamente cadastrada uma característica que tenha correspondência com aquela recebida. Quando encontra, retorna uma chave que permite a identificação da pessoa. Este método de verificação se torna mais lento devido à busca da similaridade da imagem em todo o banco de dados, portanto, a velocidade da validação está vinculada à quantidade de informações armazenadas.

Os algoritmos trabalham com taxas de coincidência entre duas imagens, ou seja, a partir de uma determinada taxa de coincidência, o algoritmo considera que ambas pertençam à mesma pessoa. Esta taxa jamais será de 100% e é uma característica de cada algoritmo. (JAIN; BOLLE; PANKANTI, 1999).

A determinação desta taxa é feita a partir da medição de dois parâmetros: a taxa de falso aceite *(False Accept Rate FAR)* e a taxa de falsa rejeição *(False Reject Rate FRR)*. Quando se aumenta o percentual de coincidência, a taxa de falso aceite cai, mas a taxa de falsa rejeição aumenta, e vice-versa.

O *Equal Error Rate (EER)* ou taxa de erro igual é o ponto da curva em que a taxa de falso aceite é igual à taxa de falsa rejeição, ou seja, FRR é igual ao FAR. Este é um

parâmetro importante na avaliação de algoritmos de reconhecimento e identificação biométrica, pois quanto menor a EER, melhor o algoritmo. (BLEUMER, 2000).

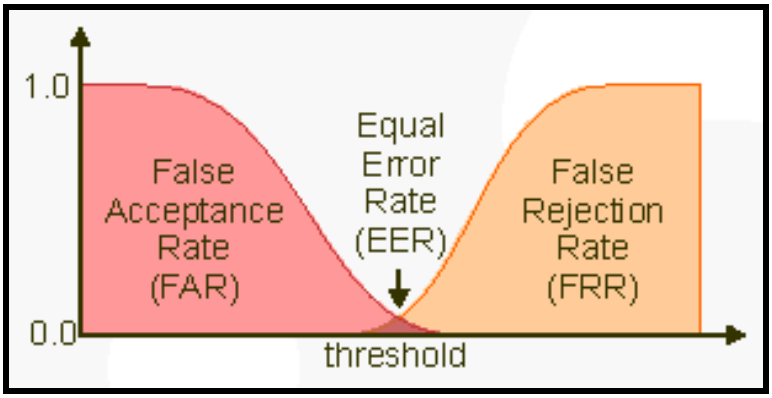


Figura 3.2 – Curva FRRxFAR

3.1.1 Reconhecimento da Impressão Digital

As principais técnicas de identificação de uma impressão digital consistem em captura da imagem, através de um equipamento específico (*scanners*), armazenamento desta imagem e posterior identificação de algumas características. Os principais leitores utilizados são:

a) Ópticos: ao colocar-se o dedo em uma base de vidro, uma luz é emitida sobre o dedo, e a imagem é capturada por um *scanner* óptico;

b) Ultrassom: neste equipamento, a leitura é feita por emissão de ultrassom, e um leitor calcula os tempos de retorno do sinal emitido, transformando estes sinais em imagem;

c) Capacitivos: o dedo é colocado diretamente sobre uma pastilha de silício, e um circuito eletrônico capta as minúcias (detalhes) do dedo, gerando uma imagem a partir deste detalhamento.

3.1.1.1 Algoritmo de identificação da impressão digital

A análise consiste em verificar a posição das minúcias, tais como bifurcações e terminações dos sulcos, e também verificar os arcos e voltas que aparecem no dedo, utilizando para isso algoritmos. Grande parte dos algoritmos trabalha com o princípio de extração dos pontos de minúcias ou pontos característicos. Após a extração, são calculadas as relações entre as distâncias destes pontos; cada algoritmo possui a sua base de cálculo, seja por análise dos pontos entre si ou por agrupamentos de pontos para análise de semelhanças de triângulos com os ângulos internos. (MALTONI; MAIO; JAIN; PRABHAKAR, 2003).

.

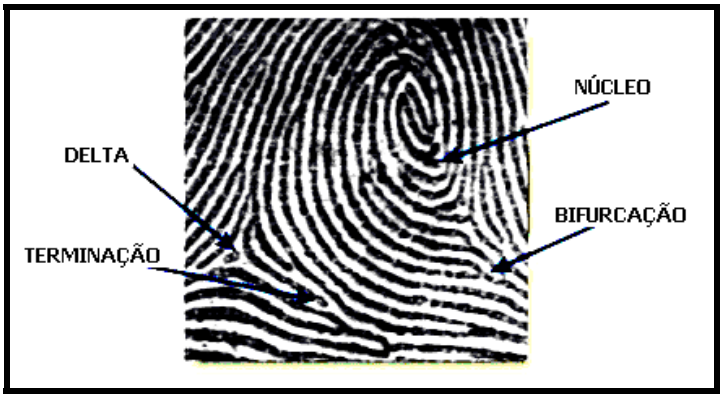


Figura 3.3 – Minúcias características de uma impressão digital

A impressão digital, após ser coletada, é tratada utilizando-se filtros específicos para tratamento de imagens, gerando assim um *template* na cor preta.

Figura 3.4 – Imagens da análise de uma impressão digital

A próxima etapa consiste em binarizar a imagem (branco e preto), fazendo com que as linhas sejam reduzidas a um único *pixel* de largura.

Com essa imagem, o algoritmo agora localiza os pontos de minúcias, analisando cada *pixel* para verificar se este é preto ou branco. Se houver um pixel branco sem vizinhos, o algoritmo interpreta que existe um ponto terminal. Caso um ponto branco possua três pontos vizinhos, o algoritmo interpreta que existe uma bifurcação.

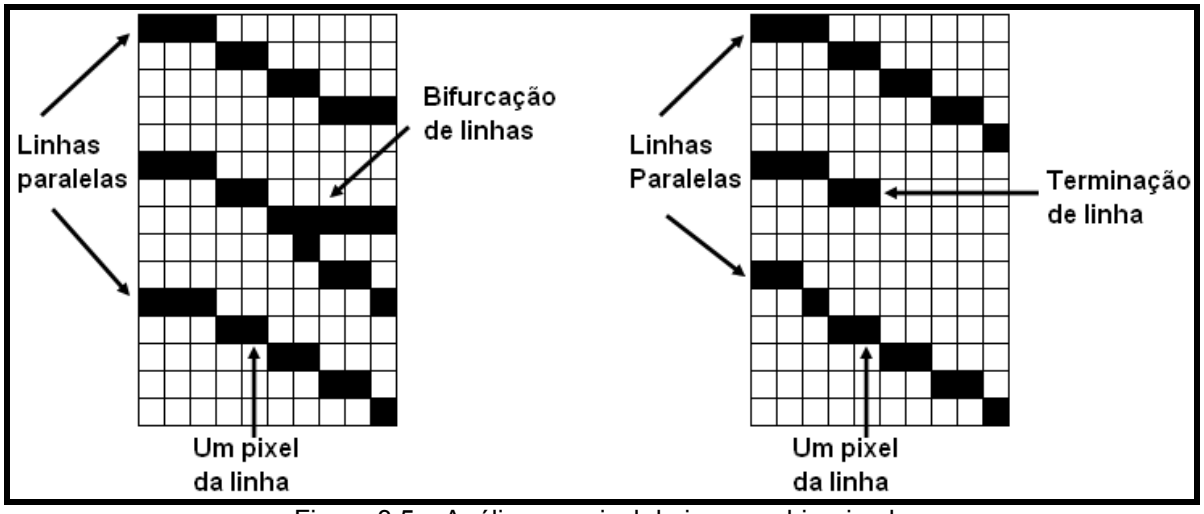


Figura 3.5 – Análise por pixel da imagem binarizada

Depois de analisada toda a imagem, deve-se comparar os pontos de minúcias encontrados com os pontos cadastrados no banco de dados anteriormente, para verificação da similaridade entre as imagens. Uma impressão digital tem em média 50 pontos de minúcias, e são necessários cerca de 10 pontos em comum para que o algoritmo valide a leitura.

Os problemas que podem ocorrer na verificação das características biométricas da impressão digital estão vinculados à qualidade da imagem gerada na leitura, e este podem ser: rotação do dedo no momento da leitura, pequenos ferimentos no dedo, cicatrizes provenientes de ferimentos causados após o cadastramento da impressão digital, ressecamento da pele, sujeira no leitor, entre outros fatores. (BOLZANI, 2004).As principais vantagens dos sistemas de leitura de impressão digital são rapidez na leitura e interpretação dos dados, baixo custo vinculado à tecnologia, tamanho reduzido dos leitores e baixo nível de intrusão aos usuários.
As desvantagens estão na variação da leitura do dedo, causando “falsos negativos”, e principalmente na vulnerabilidade do sistema.

3.1.2 Reconhecimento da íris

A íris é o anel colorido que circunda a pupila do olho, e apesar de ser externamente visível, é um componente interno do olho. Cada íris possui uma estrutura única, caracterizando um padrão complexo. Pode ser uma combinação de características específicas como coroa, glândula, filamentos, sardas, sulcos radiais e estrias. Estas características são altamente complexas e únicas, e a probabilidade de duas íris serem idênticas é estimada em cerca de 1 em 10^{78}. O processo de reconhecimento inicia com a aquisição de uma fotografia da íris tirada sob uma iluminação infravermelha, pois as íris de pigmentação escura revelam maior complexidade quando sob este tipo de iluminação, apesar de ser possível utilizar uma luz visível. A fotografia resultante é analisada utilizando algoritmos específicos, normalmente patenteados, que localizam a íris e extraem a informação necessária para criar uma amostra biométrica. (DAUGHMAN, 1994)

O sistema pode ser utilizado por pessoas que utilizam lentes de contato, mas óculos escuros devem ser evitados no momento da leitura da íris. Por não ser invasiva, esta tecnologia tem melhor aceitação pelo usuário, pois requer uma menor interação do mesmo. A íris não pode ser modificada por cirurgia plástica. A identificação por análise da íris gera aproximadamente 600 pontos, enquanto que a média de minúcias geradas por uma impressão digital é de 50, portanto, este processo é mais preciso, no entanto, o custo ainda é elevado para uma utilização em larga escala.

O processo de leitura da íris consiste em:

a) Detectar a presença do olho na imagem;
b) Localizar os limites interiores e exteriores da Íris;
c) Detectar e excluir as pálpebras se forem indutoras de erro;
d) Definir um sistema de coordenadas 2D, o qual é mapeado o padrão da íris e gerado o seu código;
e) O Código da Íris pode ser armazenado em código hexadecimal em um banco de dados ou outro tipo e mídia. Uma vez no banco de dados, o código é usado como base para a comparação contra a íris capturada pela câmera no processo de identificação de uma pessoa.

Abaixo, pode-se ver na figura o detalhamento de um olho humano. A íris é a área verde azulada. As outras estruturas visíveis são a pupila (círculo preto no centro) e a esclera (parte branca do olho) ao redor da íris. A córnea está presente nesta foto, mas não é possível vê-la, por ser transparente. (WILDES, 1997).

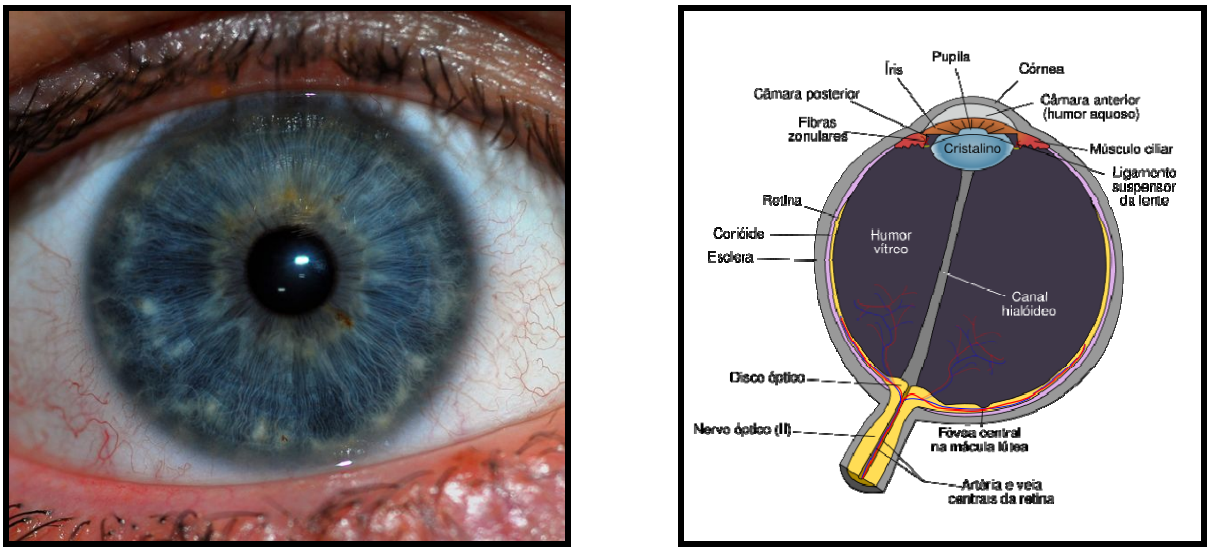


Figura 3.6 – Estrutura do olho humano

3.1.2.1 Algoritmo de reconhecimento da íris

O algoritmo desenvolvido por Daughman consiste basicamente em adquirir a imagem da íris, processar os dados da imagem adquirida e separar a imagem da íris de outras imagens, como o resto do olho, cílios e pálpebras. Filtros específicos são aplicados para excluir todas as partes desnecessárias no processo de identificação.

O foco da íris é realizado através da localização do raio da íris e da pupila e das coordenadas do centro da imagem. Deve-se levar em consideração que o centro da pupila não é necessariamente o centro da íris, e esta variação pode chegar a até 0,8mm. Para adquirir as fronteiras da íris e separá-la da pupila, Daughman propôs a seguinte integral parametrizada:

$$\max_{(r,x_0,y_0)} \left| G_\sigma(r) * \frac{\partial}{\partial r} \oint_{r,x_0,y_0} \frac{I(x,y)}{2\pi r} dS \right| \qquad (1)$$

O termo ***I(x, y)*** representa a imagem capturada através da câmera, e ***2πr*** é a medida da circunferência da imagem adquirida. Os parâmetros ***r, x_o e y_0*** são respectivamente o raio da imagem e as coordenadas cartesianas do centro da imagem.

A equação proposta por Daughman tem a finalidade de localizar a imagem da íris, separando-a da pupila, para que possa ser utilizada futuramente na identificação da pessoa. A função ***Gσ*** serve para suavizar possíveis ruídos que possam ter surgido durante o processo de aquisição da imagem. A próxima etapa do algoritmo é a codificação e digitalização da imagem, para que seu armazenamento possa ser realizado por um microcomputador, e posteriormente, utilizado para a comparação na identificação do usuário.

A codificação da íris utiliza a função conhecida como *Wavelets* 2D de Gabor, que reconhece a íris por vetores e adquire as informações relevantes da imagem, como orientação, freqüência espacial e posicionamento. Com essas informações é possível mapear o código da Íris. Abaixo, segue a fórmula utilizada para estimar o código de uma íris e a imagem de uma representação pictórica de um código de Íris.

$$h_{\{\mathrm{Re,Im}\}} = \mathrm{sgn}_{\{\mathrm{Re,Im}\}} \int_{\rho}\int_{\phi} I(\rho,\phi) e^{-i\omega(\theta_0-\phi)} \cdot e^{-(r_0-\rho)^2/\alpha^2} e^{-(\theta_0-\phi)^2/\beta^2} \rho d\rho d\phi \quad \textbf{(2)}$$

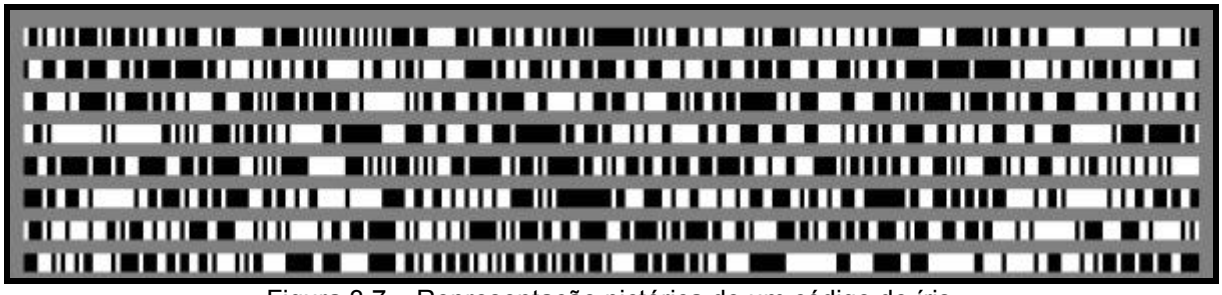


Figura 3.7 – Representação pictórica de um código de íris

Na fórmula acima, ***h{Re, Im}*** representa um número complexo. O termo ***I(ρ,ϕ)*** representa a imagem da íris em um sistema de coordenada pseudo-polar adimensional que é adquirida convertendo-se as coordenadas em um plano cartesiano para um plano polar, ou esférico.

O par ***(r, θ)*** na equação são as coordenadas polares de cada região da íris para as quais a função ***h*** é computada. Com a conversão para o sistema pseudo-polar, a dilatação da íris é corrigida, de forma que não prejudique o seu reconhecimento. As letras gregas ***α e β*** são parâmetros multi-escalares das *wavelets* 2D e ***ω*** é a freqüência do *wavelet.*

Utilizando o quadrante de fase de demodulação da íris obtêm-se as partes imaginária e real da fórmula da *wavelet* 2D. No final do processo, 256 *bytes* são gerados, e alguns sistemas mais modernos geram 512 *bytes* de informação, os quais representarão a imagem da íris, no entanto, geralmente são gerados mais 256 (ou 512) *bytes* conhecidos como máscara, que tem a finalidade de definir fatores prejudiciais na identificação da íris, tais como: reflexos, lentes de contato, cílios e pálpebras.

As informações sobre a fase são utilizadas para o reconhecimento de íris, porém as informações sobre amplitude não são utilizadas, pois são menos relevantes e dão menos informações. Uma vantagem da utilização da fase é que independente da qualidade ou do foco da imagem, os ângulos permanecem os mesmos. Isso faz com que a comparação entre dois códigos de íris diferentes, mas ambos de imagens ruins possam ser diferenciados facilmente.

Também existem formas de converter as diferentes imagens circulares adquiridas para padrões normalizados, de forma a facilitar a comparação. Para esse processo também são considerados os efeitos externos, como pálpebras, cílios e reflexos, além dos internos, como diferenças de centro entre pupila e íris. Diversos filtros e *wavelets* são utilizados para normalização da imagem da íris. Como resultado, diversos padrões são adquiridos e armazenados no sistema.

Figura 3.8 – Centralização de coordenadas da íris – normalização

Após a codificação e digitalização da íris, o próximo passo para que seja realizada a identificação do indivíduo é a comparação da informação captada com um banco de dados de íris armazenadas anteriormente. Na comparação de dados, é feito um teste de independência estatística entre dois códigos de íris diferentes. O teste de independência retorna um valor positivo sempre que dois códigos de íris de olhos diferentes são comparados e retorna um valor negativo sempre que duas versões de códigos da mesma íris são comparadas. O teste de independência estatística é implementado utilizando-se lógica booleana XOR (XOU, OU exclusivo).

O XOR é aplicado nos 2048 *bits* (ou 4096 *bits*) do código de íris, enquanto uma lógica booleana AND (E) é aplicada nos *bits* de máscara correspondentes. O XOR garante que não haverá diferença entre dois *bits* correspondentes, enquanto o AND garante que não haverá problemas com cílios, pálpebras, reflexos e outros fatores externos. Os resultados adquiridos são utilizados para o cálculo da distância de *Hamming*. Esse cálculo define a porcentagem de diferença entre o código de duas íris quaisquer. Normalmente, se aceita um padrão de 50% de *bits* semelhantes entre dois códigos de íris diferentes (HD = 0,5). Abaixo segue a fórmula para o cálculo da distância de *Hamming*, o qual maskA e codeA são o código de máscara de um olho A e o código de íris para o mesmo olho A, respectivamente (Idem para um olho B).

$$HD = \frac{\left\| (codeA \otimes codeB) \cap maskA \cap mask\,B \right\|}{\left\| maskA \cap maskB \right\|} \qquad \textbf{(3)}$$

Pode-se analisar que quanto maior a distância de *Hamming*, maior é a probabilidade de se aceitar duas íris diferentes como sendo iguais e quanto menor a distância de *Hamming,* maior é a probabilidade de se comparar erroneamente a mesma íris.

3.1.3 Reconhecimento da retina

A biometria da retina é baseada na análise da camada dos vasos sanguíneos na base (fundo) dos olhos.

Para isto, utiliza-se uma luz de baixa intensidade normalmente proveniente de um *laser*, e uma câmera, para que seja realizada uma varredura, para encontrar os padrões singulares da retina, portanto a confiabilidade desse método se deve ao fato da estrutura dos vasos sanguíneos estarem relacionadas com os sinais vitais da pessoa, e assim, o dispositivo leitor não conseguirá definir o padrão da retina de uma pessoa se esta estiver sem vida. A aceitabilidade da tecnologia é baixa porque requer que o usuário olhe em um visor e focalize um determinado ponto, trazendo alguma dificuldade se o usuário estiver de óculos.

Alguns médicos especialistas em olhos afirmam que as características da retina não são estáveis e que existem algumas doenças que podem alterar seu formato, portanto, ainda existem estudos para analisar a utilização deste tipo de tecnologia no controle de acesso. A análise realizada por algoritmo específico encobre 900 pontos distintos, portanto, a tecnologia tem uma ótima precisão, se comparada com a análise de cerca de 50 pontos da biometria por identificação de impressão digital, e a análise de cerca de 600 pontos da biometria por identificação da íris.

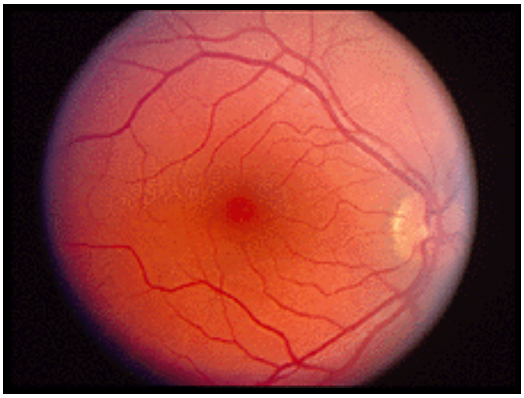


Figura 3.9 – Foto de uma retina humana

3.1.3.1 Algoritmo de reconhecimento da retina

O primeiro passo para se identificar uma retina é a definição na captura da imagem. Dividindo-se o padrão da imagem em padrão RGB, verifica-se que a cor verde

apresenta o maior contraste para a verificação dos vasos sanguíneos, portanto, esta é a cor definida para a captura da imagem, como mostrado na figura abaixo:

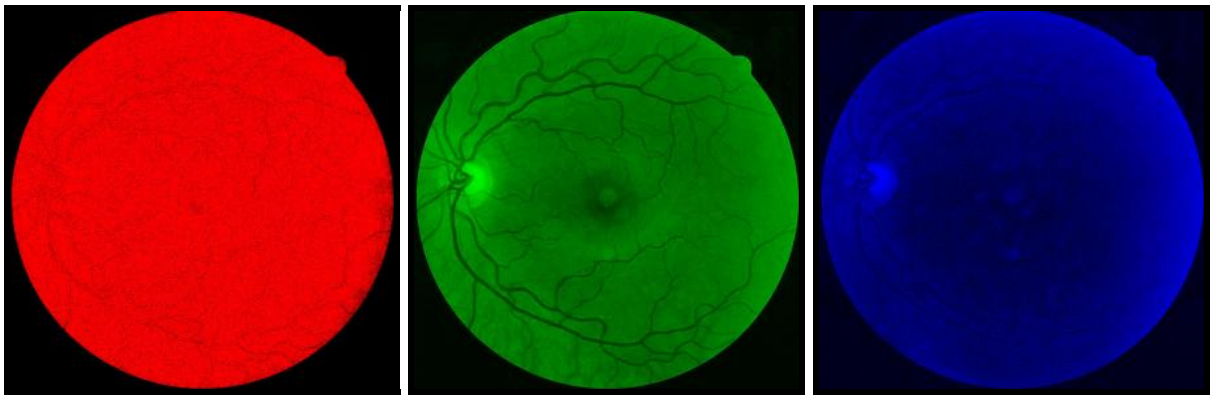


Figura 3.10 – Fotos de uma retina humana com filtros RGB

Após a captura da imagem, a transformada contínua de *Wavelet* é utilizada na detecção de singularidades, como bordas em sinais, extraindo frequências instantâneas e realizando análise fractal e multi-fractal.

Abaixo, tem-se a expressão que representa a transformada de *wavelet*:

$$T\psi(b,\theta,a)(x) = C_{\psi}^{-1/2}\frac{1}{a}\int \psi^{*}(a^{-1}r-\theta(x-b))f(x)d^{2}x \quad \textbf{(4)}$$

Os termos ***CΨ, Ψ, b, θ*** e ***a*** denotam a constante de normalização, a *wavelet* analisadora, o vetor de deslocamento, o ângulo de rotação e o parâmetro de dilatação, respectivamente. ***Ψ**** denota o complexo conjugado da *wavelet* analisadora, e uma das mais utilizadas nas tecnologias biométricas é a *wavelet* analisadora de Morlet, que tem a capacidade de detectar estruturas em muitas direções e de responder a freqüências específicas. A *wavelet* Morlet em duas dimensões é definida como:

$$\psi_{M}(x) = \exp(jk_{0}\cdot x)\exp(-\frac{1}{2}\left|Ax\right|^{2} \quad \textbf{(5)}$$

O termo j é a raiz quadrada de -1 e $A = diag\left[\varepsilon^{\frac{1}{2}},1\right]$ com $\varepsilon \geq 1$. ***A*** é uma matriz diagonal 2X2, que define o alongamento do filtro em dada direção. Na equação, $\boldsymbol{k_o}$ é um vetor que define a freqüência da exponencial complexa.

Após aplicar a equação procurando o módulo máximo das transformadas para todas as orientações, tem-se a figura abaixo:

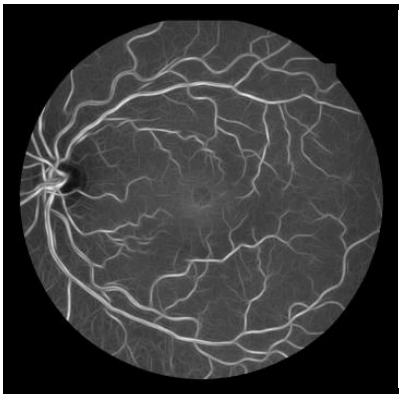


Figura 3.11 – Imagem da retina após aplicação da transformada *wavelet*

A próxima etapa do algoritmo consiste em normalizar a imagem adquirida. Cada medida usada como característica possui escala e dimensionalidade próprias, o que poderá gerar desigualdade entre a influência de cada característica durante o processo da classificação.

Considerando os elementos do espaço de características como variáveis aleatórias, podemos aplicar uma transformação nesses elementos para obter um novo tipo de variável aleatória relativizada que seja mais apropriada para o processo de classificação. Um modo de obter uma nova variável aleatória de média zero e desvio padrão unitário, além de tirar a dimensionalidade das características, é a aplicação da transformação normal ao espaço de características, definida como:

$$\hat{X}_j = \frac{X_j - \mu_j}{\sigma_j} . \qquad \textbf{(6)}$$

O termo $\boldsymbol{x_j}$ representa a j-ésima característica assumida por cada pixel, $\boldsymbol{\mu_j}$ é a média dos valores dessa característica e $\boldsymbol{\sigma_j}$ o seu desvio padrão. Após a análise e geração de uma imagem pelo classificador, gerado pelo resultado da aplicação da *wavelet*, a saída gerada pelo classificador é uma imagem binária onde cada *pixel* está rotulado como existência ou não de um vaso sanguíneo.

Para alguns vasos, apenas sua parte mais externa foi classificada, o que torna necessário um pós-processamento. Finalmente, a estrutura que deverá ser usada para qualificar os vasos da imagem é o esqueleto da segmentação, obtido através

de um algoritmo multi-escala baseado em dilatações e que deverá permitir a análise de suas formas e a comparação entre conjuntos de imagens de fundo óptico de maneira padronizada. Abaixo, tem-se a imagem de retina antes e após o processamento:

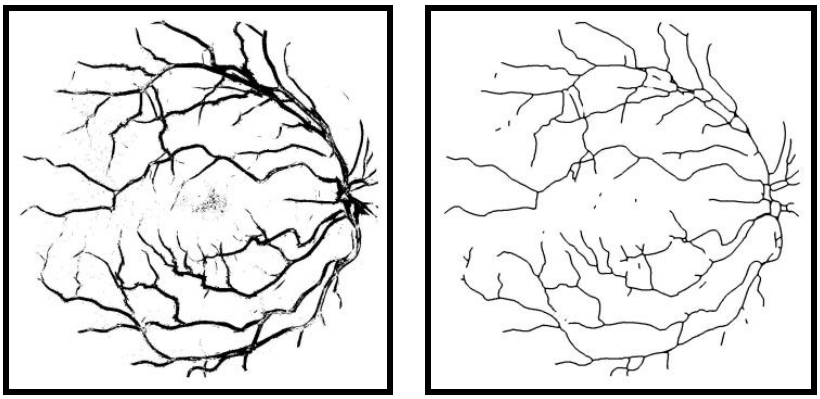


Figura 3.12 – Imagem da retina antes e após o processamento

Com estas imagens, o próximo passo é binarizar (digitalizar) a imagem, gerando *bytes* que serão posteriormente comparados com um banco de dados específico. O processo de binarização já foi comentado neste trabalho, no algoritmo de identificação biométrica de impressão digital.

3.1.4 Reconhecimento da geometria da mão

Esta tecnologia tem por finalidade a leitura das características físicas da mão de uma pessoa, baseando-se no fato de que não existem duas pessoas com mãos idênticas e de que o formato da mão não sofre mudanças significativas após certa idade.

A leitura é realizada de forma tridimensional, no entanto, as características únicas podem variar devido a diversos fatores como mudança de peso ou artrite, sujeira nas mãos ou cortes, e por este motivo, esta tecnologia não é utilizada para identificação, e sim para autenticação, caracterizando a verificação biométrica tipo 1:1.

As dimensões da mão, como o tamanho do dedo, largura e área são as principais características utilizadas na análise. Para isto, o equipamento leva cerca de dois segundos na captura da imagem de uma mão e produz a análise resultante. A imagem capturada ocupa pouco espaço para armazenamento, portanto, o número de pessoas cadastradas em um único equipamento é elevado, fazendo com que este tipo de tecnologia seja largamente utilizada em locais de grande movimentação e acesso tais como universidades, clubes, etc.

O principal problema no uso desta tecnologia está no posicionamento correto da mão, como por exemplo a rotação indevida, e para isto, existem, no equipamento, pinos de alinhamento, que obrigam o usuário a colocar corretamente sua mão no interior do leitor.

Para a captura da imagem, o usuário posiciona sua mão no leitor, alinhando os dedos com auxílio dos pinos, e uma câmara posicionada acima da mão captura a imagem. Medidas tridimensionais de pontos selecionados são tomadas e o sistema extrai as informações para determinar comprimento, largura, grossura e curvatura da mão e dos dedos e traduz essas informações para um padrão numérico, criando um identificador matemático único na criação do modelo. Um típico modelo requer cerca de nove *bytes* de armazenamento. (SANCHEZ-REILLO; GONZÁLES-MARCOS, 2000).

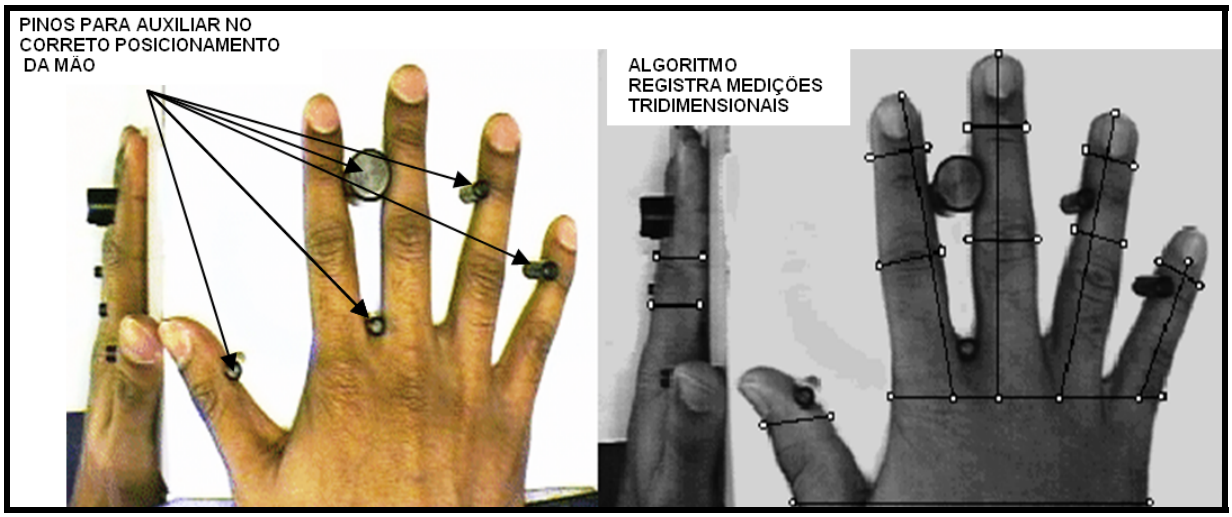


Figura 3.13 – Posicionamento da mão no leitor biométrico

A segurança contra fraudes neste sistema se baseia no fato de que é praticamente impossível obter secretamente informações sobre a geometria da mão de uma

pessoa, ao menos que haja sua cooperação. Quanto à estabilidade, deve-se ressaltar que a geometria da mão muda de acordo com a idade e, ocasionalmente, com a perda ou ganho de peso.

Figura 3.14 – Leitor de geometria da mão

3.1.4.1 Algoritmo de reconhecimento da geometria da mão

Após a aquisição de uma imagem tridimensional da mão, esta é pré-processada para que somente a informação de imagem da mão seja analisada, eliminando ruídos na imagem, bem como a figura dos pinos do dispositivo de alinhamento dos dedos. O primeiro passo do algoritmo de reconhecimento da geometria da mão é a binarização, e para isso utiliza-se o módulo (função) ***im2bw*** do *software* MATLAB.

No processo de binarização, adota-se nível lógico “0” para todos os *bits* com fator de luminância baixo (*pixels* pretos) e nível lógico “1” para todos os *bits* com fator elevado de luminância (*pixels* brancos). O nível escolhido é um valor normalizado da intensidade obtido por método de Otsu, que escolhe o ponto inicial para minimizar a variação entre os *pixels* pretos e brancos. Os efeitos do espelhamento do fundo da imagem e os ruídos geram falsas informações na imagem. A função ***imfilter*** do *software* MATLAB é usada para remover toda esta falsa informação e definir os limites do contorno da mão. A função fornece a filtragem de imagens multidimensionais. A função do ***imfilter*** computa o valor de cada pixel da saída usando a aritmética de ponto flutuante, com dupla precisão.

O pré-processamento simplifica a aplicação do algoritmo e permite iniciar a captura das características da mão. Um algoritmo para a extração de características, baseado em contar distâncias dos *pixels* em áreas específicas da mão, é utilizado. O algoritmo procura os *pixels* brancos entre dois pontos dados e computa uma distância usando princípios geométricos.

O resultado é um vetor de vinte e um elementos, como pode ser visto na figura abaixo. Cada um dos dedos é medido em três comprimentos diferentes. O dedo polegar é medido em dois comprimentos. O comprimento de todos os dedos é obtido. São realizadas duas medições da palma da mão.

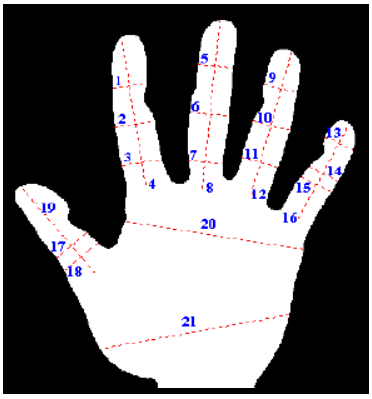


Figura 3.15 – Vetores gerados no algoritmo

Os vetores obtidos através do método citado anteriormente devem ser comparados com um banco de dados previamente gerado para que possa ser efetuada a autenticação do usuário que requisita o acesso ao ambiente. Esta comparação é feita utilizando normalmente os métodos da distância Euclidiana, distância de Hamming e modelo de mistura Gaussiana. A distância Euclidiana, considerada a técnica mais utilizada para estes tipos de algoritmo, executa suas medidas com a seguinte equação:

$$d = \sqrt{\sum_{i=1}^{L} (x_i - t_i)^2} \qquad \textbf{(7)}$$

Onde ***L*** é a dimensão dos vetores da imagem adquirida, $\boldsymbol{x_i}$ são os componentes das características dos vetores da imagem adquirida, e o $\boldsymbol{t_i}$ é o componente dos vetores do modelo. O modelo neste caso é representado então como um conjunto gerado pela composição dos vetores da imagem.

A distância de Hamming não mede a diferença entre os componentes dos vetores da imagem adquirida, mas número de componentes que diferem em suas dimensões, pois tipicamente todos os componentes diferem entre amostras do mesmo usuário, então dessa forma é necessário seguir outra aproximação para o cálculo usado para a distância Euclidiana.

Baseado na suposição de que os componentes da imagem seguem a distribuição normal, utiliza-se nos cálculos, além das medições previamente captadas da imagem da mão, um fator do desvio padrão das amostras. No processo de comparação, o número de componentes dos vetores gerados fora do modelo padrão da imagem, são contados, obtendo assim a distância de Hamming. A fim de obter melhores resultados do que em aproximações como a distância Euclidiana e a distância de Hamming, a técnica dos modelos Gaussianos de mistura (GMM) pode ser executada para o bloco do reconhecimento. GMM é a técnica do reconhecimento de teste padrão que usa uma aproximação por métodos estatísticos.

O vetor de cada medida da mão pode ser descrito pela distribuição normal, igualmente chamada distribuição Gaussiana. Cada medida da mão pode então ser definida por dois parâmetros: meio (médio) e desvio padrão (variabilidade). Deve-se supor que o vetor da medida é a variável aleatória discreta ***x*.** Para o caso geral, onde o vetor é multidimensional, a função de densidade da probabilidade da distribuição normal é uma função Gaussiana, como descrita na fórmula abaixo:

$$p(x,\mu,\Sigma) = \frac{1}{\sqrt{(2\pi)^L |\Sigma|}} \exp^{\frac{(x-\mu)^T}{2\Sigma(x-\mu)}} \qquad \textbf{(8)}$$

Onde $\boldsymbol{\mu}$ é o meio, ou a imagem adquirida, $\boldsymbol{\Sigma}$ é a matriz de co-variância e ***L*** é uma dimensão dos vetores adquiridos. Se for levado em consideração que a medida da variável aleatória não é caracterizada somente com distribuição Gaussiana simples, pode-se então definir o conjunto como componentes Gaussianas múltiplas. GMM é uma distribuição probabilística, resultante da combinação de outras distribuições

Gaussianas, e sua fórmula aplicada ao algoritmo de reconhecimento da geometria da mão, pode ser vista abaixo:

$$p(x) = \sum_{j=1}^{J} \pi^{(j)} p(x, \mu^{(j)}, \Sigma^{(j)}) \quad \textbf{(9)}$$

Onde ***J*** é o número de misturas Gaussianas e $\boldsymbol{\pi}^{(j)}$ é o peso de cada mistura. Depois que GMM é executado, o modelo de cada usuário terá os valores finais do $\boldsymbol{\pi}^{(j)}$, $\boldsymbol{\mu}^{(j)}$, $\boldsymbol{\Sigma}^{(j)}$ e ***J***, o que aumenta extremamente o tamanho da base de dados. A tabela abaixo mostra as diferenças no tamanho dos arquivos gerados em cada uma das técnicas citadas anteriormente:

Método utilizado	Imagem adquirida	Distância Euclidiana	Distância de Hamming	GMM
Tamanho do modelo gerado	**1,395 MB**	**352 B**	**520 B**	**1,209 kB**

Tabela 1 - Comparação entre métodos estatísticos

Para estimar os parâmetros da densidade de uma estatística de um modelo GMM, o algoritmo conhecido como método de Expectativa-maximização (EM) para avaliação do conjunto (EM) é adotado. O EM é o melhor algoritmo conhecido para resolver problemas da avaliação do parâmetro de GMM. Cada uma das iterações do EM consiste em duas etapas – estimação, ou avaliação e maximização. A maximização amplia uma função de probabilidade que seja refinada em cada iteração executada pela etapa de avaliação.

Os parâmetros de GMM podem ser divididos em dois grupos: um grupo que contém os termos $\boldsymbol{\pi}^{(j)}$ e outro grupo que contém os termos $\boldsymbol{\mu}^{(j)}$ e $\boldsymbol{\Sigma}^{(j)}$. O grupo que contém os termos $\boldsymbol{\pi}^{(j)}$ é responsável pela importância de densidades individuais da mistura através das probabilidades prévias. Após a inicialização dos parâmetros, a iteração do EM é a seguinte:

a) O passo de avaliação determina a melhor suposição da função $\boldsymbol{h_n^{(j)}(x_t)}$, que é a função para cada elemento de ***x*** e de cada mistura, conforme fórmula abaixo:

$$h_n^{(j)}(x_t) = \frac{p(x_t / \delta^{(j)} = 1, \phi_n{}^{(j)})\pi_n^{(j)}}{\sum_{k=1}^{J} p(x_t / \delta^{(k)} = 1, \phi_n{}^{(k)})\pi_n^{(k)}} \quad \textbf{(10)}$$

Onde $x_t / \delta_j = 1$ define que x_t é gerado pela primeira mistura j, φ_j é a função de densidade associada à primeira mistura j.

A etapa de maximização amplia a função para encontrar novos parâmetros $\pi^{(k)}$, $\mu^{(k)}$ e $\Sigma^{(k)}$ usando para isto as três equações citadas anteriormente, neste mesmo capítulo. Em seguida, o algoritmo realiza a etapa de avaliação novamente, passo a passo, até alcançar a convergência das informações.

$$\mu^{(k)} = \frac{\sum_{t=1}^{T} h_n^{(k)}(x_t) x_t}{\sum_{t=1}^{T} h_n^{(k)}(x_t)} \quad \textbf{(11)}$$

$$\sum{}^{(k)} = \frac{\sum_{t=1}^{T} h_n^{(k)}(x_t)(x_t - \mu^{(k)})(x_t - \mu^{(k)})^T}{\sum_{t=1}^{T} h_n^{(k)}(x_t)} \quad \textbf{(12)}$$

$$\pi^{(k)} = \frac{1}{T}\sum_{t=1}^{T} h_n^{k}(x_t) \quad \textbf{(13)}$$

Após a convergência dos parâmetros com os parâmetros iniciais do modelo, as distribuições Gaussianas múltiplas podem ser descritas por uma única função. Na figura abaixo, pode-se analisar que a função GMM tem sete misturas e dois vetores de dimensão. O eixo vertical representa a densidade da probabilidade, e os parâmetros nos eixos horizontais são observações dos vetores bidimensionais. (VARCHOL, 2007)

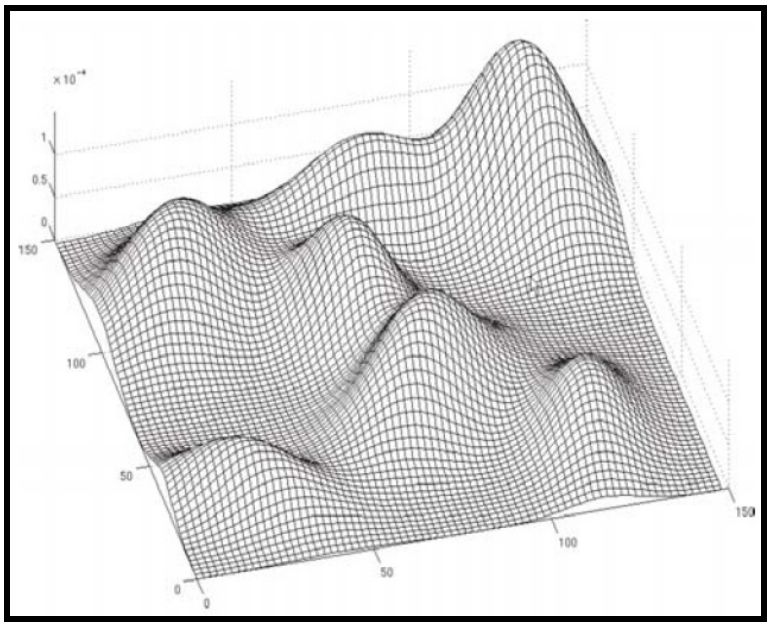


Figura 3.16 – Modelo GMM – superposição de sete distribuições Gaussianas

3.1.5 Reconhecimento da voz

O som da voz humana é causado pela ressonância nas cordas vocais. O comprimento da corda vocal, o formato da boca e as cavidades nasais são importantes na determinação da voz de uma pessoa. O som é medido quando afetado por essas características específicas. A técnica de medição da voz pode usar tanto métodos dependentes de texto ou não, ou seja, a voz pode ser capturada com um usuário falando uma senha específica de frases combinadas, palavras ou números (dependente), ou qualquer forma de frase, palavras ou números (independente).

Atualmente, as técnicas dependentes de texto são dominantes nos sistemas comerciais disponíveis de identificação da fala. Barulhos e interferências no ambiente onde está o equipamento de leitura e interpretação da voz afetam o desempenho dos sistemas de identificação da fala. A seguir, tem-se o processo básico de identificação da fala:

a) Captura: o usuário deve falar em um microfone, uma frase previamente selecionada (dependente) ou uma frase randômica (independente). Este

processo geralmente é repetido algumas vezes para se construir um perfil da voz, eliminando assim ruídos indesejados;

b) Extração: o equipamento biométrico extrai o sinal único da voz e então um *template* é criado;
c) Comparação: a verificação um-para-um (1:1) é o método preferencial. O usuário fala em um microfone; o novo exemplo de voz é então comparado com o *template* armazenado.

A forma da onda das frases é medida usando-se análises de Fourier para encontrar o espectro de freqüências que amostram as características da voz, e em seguida, a comparação é baseada nas duas formas de onda características da fala humana:

a) Análise Cepstral - análise que permite representar as similaridades entre duas ondas de voz como uma simples distância euclidiana, que será convertida em um “match score”;
b) *HMM score* - probabilidade de uma onda ter sido gerada pela mesma fonte que outra forma de onda *template*.

As principais limitações no uso desta tecnologia é que a voz muda durante o tempo devido a vários fatores, tais como envelhecimento natural, *stress*, resfriados, rouquidão, e que o sistema pode ser enganado por uma voz previamente gravada. (FAUNDES-ZANUY, 2005).

O tempo médio para cadastro de voz é de três minutos, e a verificação é realizada em cerca de meio minuto, mostrando assim que é uma tecnologia de rápida utilização. O nível de intrusão ao usuário é baixo, mas deve-se evitar a utilização em ambientes com nível de ruído elevado, pois o mesmo influencia na leitura da voz. (RABINER; SCHAFER, 1978).

3.1.6 Reconhecimento facial

A tecnologia de reconhecimento facial tem por finalidade reconhecer a identidade de pessoas através da análise da face. Fazendo uso de *software* e algoritmos

específicos, um computador localiza faces humanas num dado campo visual através de câmaras e compara com uma determinada base de dados previamente construída. (VICTOR; BOWYER. SARKAR, 2002).

Para reconhecer o rosto de uma pessoa, os programas tecnicamente mapeiam a geometria e as proporções da face. São registrados vários pontos delimitadores na face, os quais permitem definir proporções, distâncias e forma de cada elemento do rosto e, com base nesses dados, iniciar as comparações. Os pontos principais são: olhos, nariz, queixo, maçãs do rosto, orelhas, lábios, boca, sombrancelha, e a relação entre eles.

A tecnologia de reconhecimento facial leva em conta as medidas do rosto que nunca se alteram, mesmo que a pessoa seja submetida a cirurgias plásticas. As medidas básicas são: Distância entre os olhos; Distância entre a boca, nariz e os olhos; Distância entre olhos, queixo, boca e linha dos cabelos. A câmera captura uma fotografia do rosto humano, que é mapeada em uma série de 128 números, conhecidos como coeficientes. Esses são processados de forma a compor um arranjo único e bidimensional, da disposição de áreas claras e escuras do rosto.

Também pode-se fazer um teste opcional de expressões faciais, para diminuir a possibilidade de fraudes. O reconhecimento facial em 2D possui algumas limitações, ao nível das imagens que captura, pois pode confundir a pessoa através das expressões faciais, pêlos e óculos dificultando a identificação. No entanto, com o desenvolvimento da tecnologia em 3D, muitas dessas dificuldades deixam de existir. (ACHERMANN; JIANG; BUNKE, 1997).

Principais características da tecnologia:

a) Alta aceitabilidade, pois a fotografia é aceita de forma generalizada em diversos locais como forma de identificação;
b) Não intrusiva – o usuário não tem que interagir com nenhum equipamento durante um periodo de tempo significativo;
c) Podem ser criados *templates* faciais sem a presença física do individuo, no caso da tecnologia em 2D;

d) A verificação humana do *template* biométrico contra a pessoa/fotografia existente é relativamente simples e habitual para as entidades responsáveis pelo controle de fronteiras.

Deve-se levar em consideração, antes da escolha desta tecnologia, que o custo ainda é elevado, devido ao uso de sistemas informatizados de alta tecnologia, tem baixa confiabilidade e o tempo de leitura e pesquisa são elevados. (JAIN; HALICI; HAYASHI; LEE; TSUTSUI, 1999).

Figura 3.17 – Utilização de *software* para reconhecimento facial

3.1.6.1 Algoritmo de reconhecimento facial

A tecnologia biométrica de reconhecimento facial utiliza diversos algoritmos para que possam ser efetuadas a captura da imagem e comparação com um banco de dados.

Os principais algoritmos são:

PCA (Principal component analysis)

Dada uma representação vetorial de apenas uma dimensão, de cada imagem aquisitada da face de uma pessoa, a análise do componente principal (PCA) tende a encontrar um subespaço tridimensional cujos vetores da base correspondam ao sentido máximo da variação no espaço de imagem original.

ICA (Independent component analysis)

A análise de componente independente (ICA) minimiza ambas as dependências de segunda ordem e ordens superiores nos dados de entrada e tenta encontrar uma base se for estatisticamente independentes.

LDA (Linear Discriminant Analysis)

A análise por LDA consiste em encontrar os vetores no espaço subjacente que melhor se discriminam entre as classes.

EP (Evolutionary Pursuit)

A análise por EP baseia-se na aproximação adaptável de procura pelo melhor arranjo de vetores da imagem adquirida, a fim de maximizar uma função de aptidão, medindo ao mesmo tempo a exatidão da classificação e a habilidade geral do sistema. Trata-se de um algoritmo de perseguição de melhor característica vetorial para a análise e comparação de dados.

EBGM (Elastic Bunch Graph Matching)

Todos os rostos humanos compartilham de uma estrutura topológica similar. As faces são representadas como gráficos, com os nós posicionados em pontos específicos como, por exemplo, o nariz, e bordas etiquetadas com vetores de distância bidimensional.

Cada nó contém um conjunto de quarenta coeficientes complexos do *wavelet* de Gabor em escalas e em orientações diferentes (fase, amplitude). O reconhecimento é baseado em gráficos etiquetados. Um gráfico etiquetado é um conjunto dos nós conectados por bordas, o qual os nós são etiquetados como jatos, e as bordas são etiquetadas como distâncias.

Método Trace Transform

É uma ferramenta para o processamento de imagem que pode ser usada para reconhecer objetos sob transformações, por exemplo, rotação e translação. Diferentes traços podem ser produzidos a partir de uma imagem usando diferentes funções de traço, neste algoritmo.

AAM (Active Appearance Model)

Trata-se de um modelo estatístico integrado que combina um modelo de variação da forma de uma face (imagem adquirida) com um modelo das variações das imagens adquiridas em um banco de dados, em um *frame* pré-normalizado.

Método Reconhecimento Facial 3D

O rosto humano é uma superfície que se encontra no espaço tridimensional. Conseqüentemente o modelo 3D deve ser o melhor modelo para representar as faces, e para verificar diversas variações faciais, tais como a pose, a iluminação, rotação, entre outros. A principal característica desta aproximação é a habilidade de comparar os dados independentes das superfícies de deformações naturais resultante das expressões faciais.

Primeiramente, a imagem da escala e a textura da face são adquiridas. Em seguida, a imagem da escala é pré-processada, removendo determinadas partes tais como o cabelo, que pode complicar o processo de reconhecimento. Finalmente, um formulário canônico da superfície facial é computado. Tal representação é insensível às orientações principais e às expressões faciais, simplificando assim significativamente o procedimento do reconhecimento. O próprio reconhecimento é executado nas superfícies canônicas.

Método Bayesian Framework

Trata-se de um algoritmo que considera uma medida probabilística da similaridade de imagens, e julga que as diferenças da intensidade da imagem são características de variações típicas na aparência de um indivíduo. Duas classes de variações faciais da imagem são definidas: variações intrapessoais e variações extrapessoais. A similaridade entre as faces é medida usando a regra Bayesian.

SVM (Support Vector Machine)

Dado um conjunto de pontos que pertencem a duas classes, uma máquina de sustentação do vetor (SVM) encontra o plano superior que separa a maior fração possível de pontos da mesma classe no mesmo lado, enquanto maximiza a distância de uma ou outra classe ao plano superior. O APC é usado primeiramente para extrair características de imagens da face e as funções da discriminação entre cada par de imagens são realizadas por SVMs.

HMM (Hidden Markov Models)

Este algoritmo é um conjunto dos modelos estatísticos usados para caracterizar as propriedades estatísticas de um sinal. HMM consiste em dois processos relacionados:

- ✓ Uma cadeia de Markov sendo a base, inobservável com um número finito de estados e uma matriz de probabilidade de transição de estados e uma distribuição de probabilidade do estado inicial;
- ✓ Um conjunto de funções de densidade da probabilidade associadas com cada estado.

3.1.7 Reconhecimento da dinâmica da assinatura

Esta tecnologia visa verificar a assinatura manuscrita através da análise do ato de escrever, a pressão aplicada à caneta, a velocidade e o ritmo da escrita, pois a simples assinatura, de forma estática, é facilmente copiável, apesar de existirem sistemas biométricos que realizam este tipo de análise. Estes sistemas também registram a seqüência da escrita, e o detalhamento da assinatura (como se adicionam pontos e traços ao escrever ou a pausa existente entre a escrita de duas palavras). Os equipamentos utilizados baseiam-se em *scanners* compostos por diversos sensores que reconhecem o ângulo, pressão e direção da escrita, realizada sobre uma área pré-determinada do equipamento. Através de análise algorítmica, é realizada a análise da assinatura, em seguida a comparação com a assinatura pré-armazenada em um banco de dados, e a comprovação ou não do usuário em questão. (LAMONDON; PARIZEAU, 1988)

3.1.8 Tecnologias biométricas em estudo

Outras tecnologias estão em fase de estudo para a implementação de sistemas biométricos. Entre eles, pode-se citar a análise do formato do ouvido, transpiração, cheiro do corpo, brilho da pele, análise de DNA, impressão da palma da mão, matriz da unha e salinidade. Ainda não existem equipamentos comercialmente divulgados que utilizem estas tecnologias.

3.1.9 Considerações finais sobre biometria

Considerando as principais características de cada tecnologia biométrica aplicada à área de segurança, pode-se levantar as seguintes vantagens e desvantagens:

- **Reconhecimento da impressão digital:**

Vantagens: Dispositivos com alto grau de facilidade de uso por parte do usuário, baixo custo para implementação da tecnologia, o equipamento não ocupa grandes espaços físicos, a impressão digital nunca muda.
Desvantagens: A leitura por parte de alguns usuários tem conotação criminal, causando certo incômodo em sua utilização; o desempenho do equipamento fica prejudicado nos casos de pele seca, com óleo, suja ou com cortes; o contato dos dedos com o leitor biométrico é considerado anti-higiênico em alguns países asiáticos, devido à possibilidade de contaminação por diversas doenças.

- **Reconhecimento da íris:**

Vantagens: Esta tecnologia tem uma taxa de precisão maior que a leitura do DNA humano, sendo considerada a biometria mais precisa atualmente; é feita a identificação do usuário, portanto a autenticação é dispensada, fazendo com que a tecnologia seja extremamente rápida.

Desvantagens: Alto custo para a implementação e desconforto ao usuário são as principais desvantagens.

- **Reconhecimento da retina:**

Vantagens: A precisão é extremamente elevada, e as características da retina permitem analisar se a pessoa está viva no momento da leitura, evitando assim atos criminosos com o olho humano.
Desvantagens: Existe desconforto com a luz gerada pelo equipamento para a realização da leitura da retina, e também existe a necessidade de se retirar óculos no momento da utilização do equipamento.

- **Reconhecimento da geometria da mão:**

Vantagens: Alta velocidade na leitura e comparação dos dados biométricos; as condições da pele não afetam a qualidade da leitura.
Desvantagens: As dimensões físicas do equipamento leitor são elevadas, se comparado à outras tecnologias disponíveis; também é considerado um equipamento anti-higiênico em alguns países asiáticos.

- **Reconhecimento da voz:**

Vantagens: Baixo custo para a implementação e sua principal utilização se baseia em aplicações com voz, por exemplo, em telefonia.
Desvantagens: Baixa precisão, pois ruídos externos podem afetar a leitura da voz, e condições físicas do usuário podem afetar a voz, como por exemplo rouquidão causada por resfriados.

- **Reconhecimento facial:**

Vantagens: O reconhecimento facial pode ser realizado sem o conhecimento do usuário, como por exemplo em portos e aeroportos, ou em qualquer local com grandes multidões; os algoritmos utilizam lógicas que eliminam as possibilidades de

fraude, identificando o usuário mesmo que a pessoa altere algumas características físicas, como cabelo, barba, etc.

Desvantagens: Como a tecnologia utiliza câmeras para a captura da imagem, é necessário iluminação adequada e o ambiente deve ser controlado.

- **Reconhecimento da dinâmica da assinatura:**

Vantagens: A tecnologia pode ser usada em equipamentos portáteis para o controle do acesso lógico, como em *laptops*.

Desvantagens: Baixa precisão

Dentre os diversos tipos de tecnologia aplicadas à leitura biométrica, voltadas à área de segurança, pode-se levantar alguns dados. A tabela abaixo mostra uma comparação entre os sistemas biométricos existentes, em termos de parâmetros que caracterizam o equipamento como sendo biométrico, tais como universalidade, unicidade, permanência e coletabilidade. (SERPRO, 2006)

TIPOS DE BIOMETRIA	Universalidade	Unicidade	Permanência	Coletabilidade
Impressão Digital	MÉDIA	ALTA	ALTA	MÉDIA
Íris	MÉDIA	MÉDIA	MÉDIA	ALTA
Retina	ALTA	ALTA	MÉDIA	BAIXA
Geometria da mão	ALTA	ALTA	ALTA	MÉDIA
Identificação da fala	MÉDIA	BAIXA	BAIXA	MÉDIA
Reconhecimento facial	ALTA	BAIXA	MÉDIA	ALTA
Dinâmica da assinatura	BAIXA	BAIXA	BAIXA	ALTA

Tabela 3.1 – Parâmetros das tecnologias biométricas

A tabela seguinte apresenta outros parâmetros que podem ser considerados na escolha de uma tecnologia biométrica, como desempenho, aceitabilidade por parte dos usuários e nível de segurança do equipamento:

TIPOS DE BIOMETRIA	Desempenho	Aceitabilidade	Segurança
Impressão Digital	ALTO	MÉDIA	ALTA
Íris	MÉDIO	MÉDIA	MÉDIA
Retina	ALTO	BAIXA	BAIXA
Geometria da mão	ALTO	BAIXA	ALTA
Identificação da fala	BAIXO	ALTA	BAIXA
Reconhecimento facial	BAIXO	ALTA	BAIXA
Dinâmica da assinatura	BAIXO	ALTA	BAIXA

Tabela 3.2 – Parâmetros de qualidade de tecnologias biométricas

Após consultar diversos fabricantes de equipamentos biométricos, os custos aproximados foram levantados, e são apresentados no gráfico abaixo:

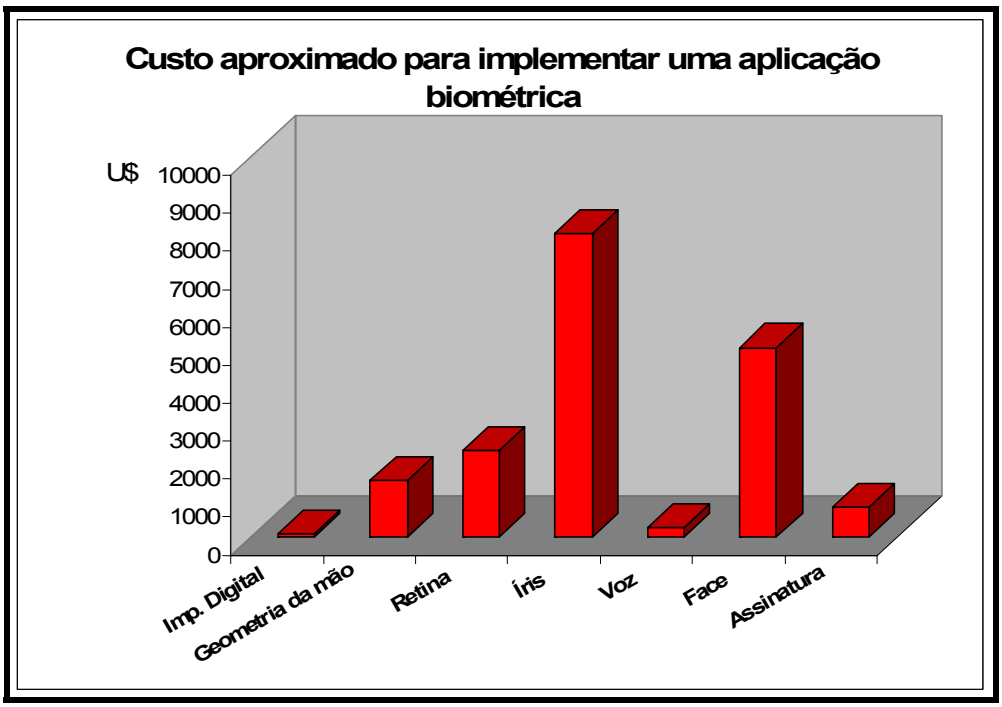


Gráfico 3.1 – Custos para implementação de biometria

O gráfico abaixo apresenta uma comparação entre tecnologias biométricas incluindo preço, precisão do sistema, facilidade de implantação e conveniência para o usuário. (DGV, 2006).

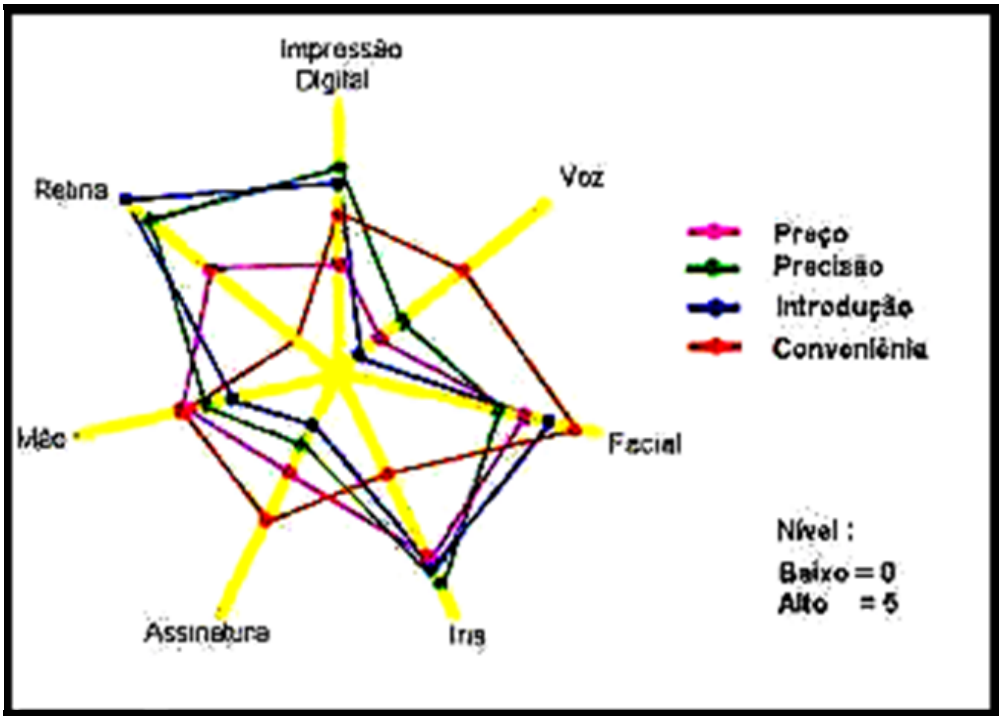


Gráfico 3.2 – Comparação entre tecnologias biométricas

3.2 Cartões inteligentes – *SMART CARD*

Os cartões inteligentes, também conhecidos comercialmente como *Smart Cards*, são produzidos a partir de uma matriz de plástico, semelhante a um cartão de crédito, com um microchip embutido em seu interior, e em alguns modelos com contatos elétricos expostos em sua superfície para que o acesso ao conteúdo do microchip possa ser realizado.

O conceito de *Smart Card* foi patenteado no Japão, em 1970, pelo Dr. Kunitaka Arimura. Os predecessores do cartão inteligente foram principalmente os cartões com códigos de barra e os cartões com tarja magnética.

O custo aproximado de um cartão inteligente varia de US$2.00 a US$10.00. Esta variação se dá de acordo com a capacidade de armazenagem e de processamento de informações.

Figura 3.18 – Exemplos de *Smart Card*

3.2.1 Tipos de cartões inteligentes

Apesar de existir muitos tipos de cartões, a classificação de cada um é realizada de acordo com a forma de conexão que existirá entre o cartão e o dispositivo leitor, e as duas principais formas de conexão são:

- ✓ Por contato físico;
- ✓ Sem contato físico.

Abaixo, tem-se o resultado do estudo de ambos os tipos de cartões existentes:

3.2.1.1 Cartões inteligentes por contato físico

Trata-se dos cartões que são inseridos em um equipamento leitor, onde existem contatos elétricos móveis, responsáveis pela conexão elétrica com os terminais do cartão, para que possa ser efetuada a leitura ou escrita de informações. Existem tipicamente dois modelos de cartão inteligente por contato físico: os cartões com

memória interna EEPROM e os cartões com microcontrolador e memória interna em seu interior, conhecidos como *SmartCards memory e SmartCards processor*, respectivamente.

Os cartões podem ser fabricados com material PVC (*Polyvinyl Choryde*) ou em ABS (*Acrylonitrile Butadine Styrene*). A diferença entre os dois tipos de material é que o PVC pode ser moldado, com formas em alto relevo, no entanto, não é um material que pode ser reciclado, e o ABS não permite modelações em sua forma, mas é reciclável. Os cartões por contato tem uma vida útil de 10.000 ciclos de leitura e escrita, e devem passar por testes de torção, flexibilidade, desgaste, eletricidade estática e exposição a campos magnéticos antes de serem comercializados.

A área de conexão do cartão inteligente por contato físico por de oval ou quadrada, e é definida pela norma ISO/IEC 7816. Abaixo, pode-se visualizar o esquema de ligação da área de conexão. (TAVERNIER, 2007)

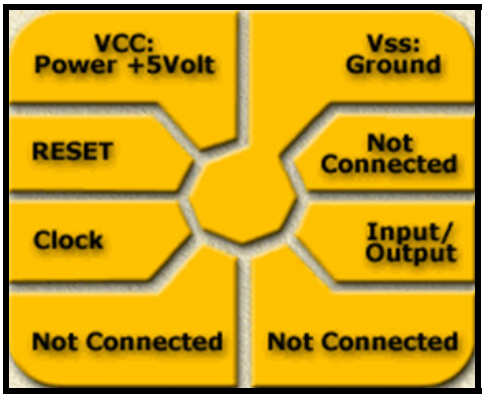


Figura 3.19 – Contato elétrico de um *Smart Card*

Os cartões *Smart Cards* tem basicamente três tipos de construção:

HMD (*Hole Mounted Device*)

Esta é uma técnica usada quando se utiliza a combinação de microcontrolador PIC e memória EEPROM que ainda não estão disponíveis para versões em cartões, tem baixo custo e baixa utilização no mercado. Os componentes relativamente grandes são montados e soldados através dos furos do cartão.

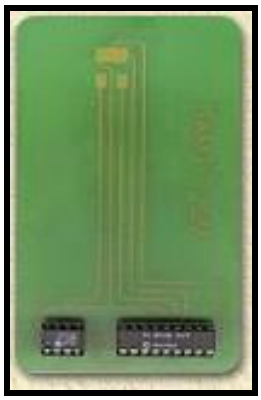


Figura 3.20 – Cartão HMD

SMD (*Surface Mounted Device*)

Este tipo de cartão é similar ao cartão HMD, mas utiliza componentes de menor dimensão, portanto são soldados na placa interna do cartão sem a necessidade de furos no mesmo.

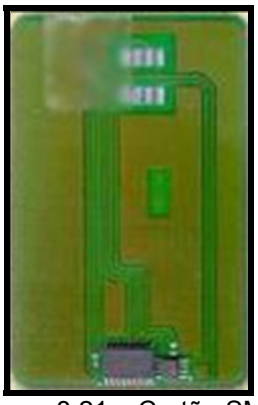


Figura 3.21 – Cartão SMD

***Integrated cards* (cartões integrados)**

Este é o tipo de cartão mais comum, utilizado atualmente. O microcontrolador e a memória EEPROM são extremamente pequenos, e ficam instalados no interior do PVC, portanto, os componentes do cartão não são visíveis. Estes cartões são produzidos em larga escala, e com isso seu custo é reduzido.

Figura 3.22 – Cartão integrado

Os cartões construídos a partir da tecnologia HMD e SMD não são mais utilizados. Atualmente, praticamente todos os cartões são do tipo integrado. Os cartões que contém em seu interior apenas memória, são reconhecidos por alguns fabricantes como cartões de memória ou *memory cards*, pois apenas armazenam informações, e a responsabilidade do processamento fica por conta do equipamento leitor, ou de um microcomputador incorporado ao sistema.

Com esta caracterização, muitos não consideram estes cartões como inteligentes, portanto, neste capítulo não será dada ênfase ao estudo deste modelo, pois o foco é justamente a aplicação dos cartões inteligentes para a aplicação no controle de acesso de pessoas em instalações elétricas automatizadas. Voltando ao estudo dos tipos de construção física de cartões, os modelos mais comuns encontrados comercialmente com a tecnologia de cartões integrados são:

Cartão GOLD

São conhecidos também como PICCard, GoldCard, SlimCard, SlimCard II ou SMD Wafer. Ainda estão disponíveis no mercado pois existem muitas aplicações implementadas com este modelo. É consequentemente o modelo de cartão mais simples de ser criado, do ponto de vista técnico, pois utiliza baixa tecnologia, proveniente dos componentes que estavam disponíveis na época de sua concepção. Todos os modelos trabalham com um microprocessador da família PIC, do fabricante Microchip, e o modelo tipicamente utilizado é o Microchip 16F84. Estes modelos de cartão tem, normalmente, um chip de memória de 2kB, modelo 24LC16.

O microcontrolador PIC 16F84 utilizado neste cartão contém em seu interior uma memória do tipo EEPROM, no entanto, sua capacidade é muito reduzida, sendo de apenas 64 *bytes*. A adição da memória externa 24LC16 permite elevar esta capacidade de armazenamento de dados à 2 kB.

As ligações elétricas do circuito seguem a norma ISO/IEC 7816, pode ser vista na figura a seguir, assim como um modelo de cartão:

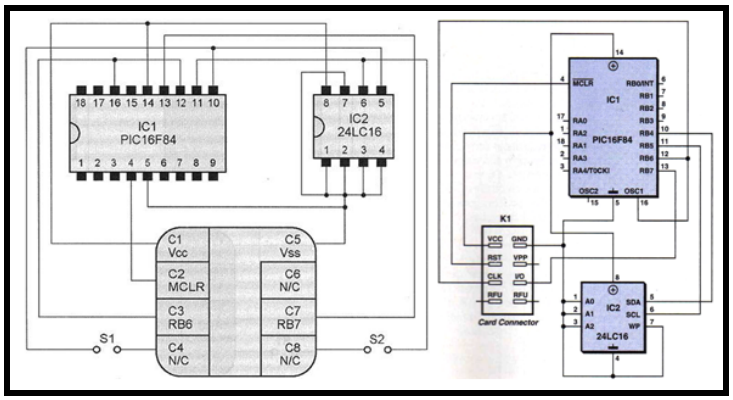


Figura 3.23 – Cartão GOLD

Existe aninda um cartão com o nome Wafer 2 ou ainda Gold 64. O seu esquema é idêntico ao do Wafer 1, como mostrado a figura abaixo, com a ampliação da memória EEPROM, para o modelo 24LC64 com 8 kB de capacidade total.

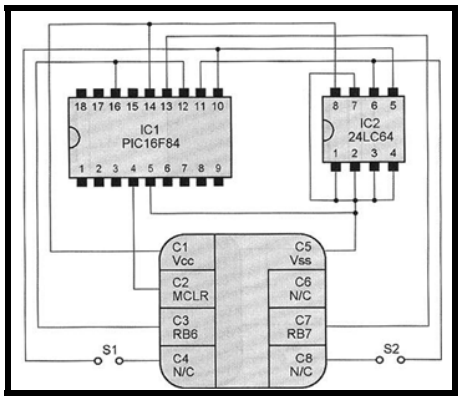


Figura 3.24 – Cartão GOLD 64

Cartão SILVER

São conhecidos também como Wafer3, Galaxy2, GreenCardII, SilverWafer, SilverCard e PICCard II. Este modelo de cartão sucede o modelo GOLD, e utiliza um microcontrolador mais rápido que o modelo anterior, o Microchip 16F876. Sua memória interna também é superior, com valores típicos de 8kB, modelo 24C62.

O esquema elétrico de seus componentes é idêntico ao modelo GOLD, conforme figura abaixo. As diferenças fundamentais estão nas características de construção do modelo de microprocessador utilizado nesta versão, que tem uma memória interna de 368 *bytes* contra os 68 *bytes* do modelo 16F84, e uma memória EEPROM interna de 256 *bytes* contra os 64 *bytes* do modelo 16F84.

Como a capacidade de armazenamento de dados neste modelo de cartão é maior, sua utilização se dá para aplicações que requerem maiores tamanhos de arquivos, utilizando assim maiores recursos de memória. Uma das vantagens deste modelo de cartão é a possibilidade de migrar aplicações do modelo GOLD para esta versão sem necessitar modificar o programa.

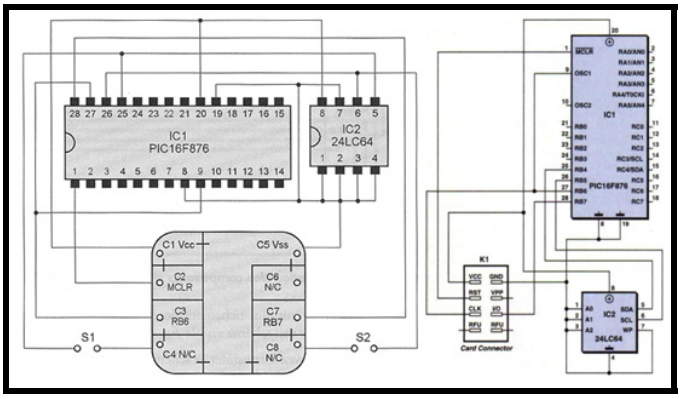


Figura 3.25 – Cartão SILVER

Cartão FUN

São conhecidos também como ATMELCard, FunCard, FunCard 2, Funcard 3, FunCard 4, FunCard 5, Funcard 6, Purple Galaxy, Prussian, Prussian2 e Prussian3.
Estes cartões possuem em seu interior o microcontrolador da família AVR, fabricante ATMEL, e trata-se de um componente com tecnologia RISC, a mesma dos microcontroladores PIC utilizados nos modelos de cartão GOLD e SILVER. O modelo de microcontrolador utilizado é o AT90S8515, contém 8kB de memória de programa e 512 *bytes* de RAM interna.

Como para os cartões precedentes, é associada memória EEPROM externa cuja dimensão varia de acordo com o tipo de *Fun Card* escolhido. Atualmente encontram-se no mercado as versões seguintes: Wafer 4 com a memória AT24C64 de 8kB. Wafer 4A com a memória AT24C128 com 16 kB. Wafer 4B com a memória

AT24C256 de 3kB. A ligação elétrica de seu circuito interno pode ser vista na figura abaixo:

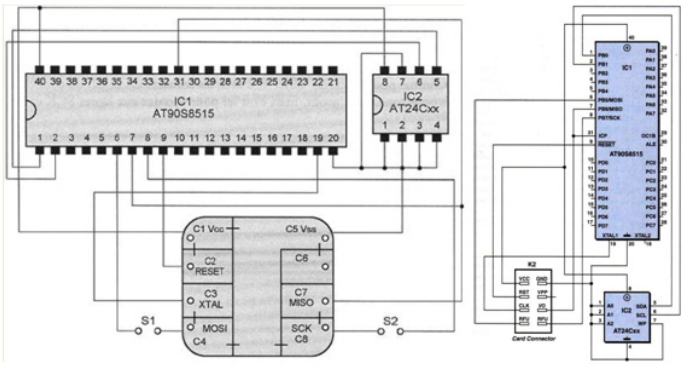


Figura 3.26 – Cartão FUN

Cartão JUPITER

São conhecidos também como BlackCard. Não são mais utilizados, pois a maioria utiliza a tecnologia SMD em sua fabricação. O microcontrolador utilizado neste modelo é o 90S2342, do fabricante Atmel. Também existem modelos de cartão Jupiter 2, que utiliza o microprocessador 90S8535, do mesmo fabricante, e com uma memória interna do tipo EEPROM, com 8kB de capacidade. Contrariamente ao FUN, que utiliza um microcontrolador AVR de alto desempenho, o cartão JUPITER utiliza um dos menores microcontroladores da família AVR, o modelo AT90S2343, associado ainda a uma memória EEPROM externa do tipo AT24C16 com apenas 2kB de capacidade. Sua utilização é apropriada em aplicações que requerem menor velocidade de processamento de informações e menor capacidade de armazenamento de dados. Sua principal vantagem em relação ao cartão de modelo FUN é ter seu custo reduzido. Abaixo, pode-se visualizar a figura do circuito elétrico interno deste modelo de cartão.

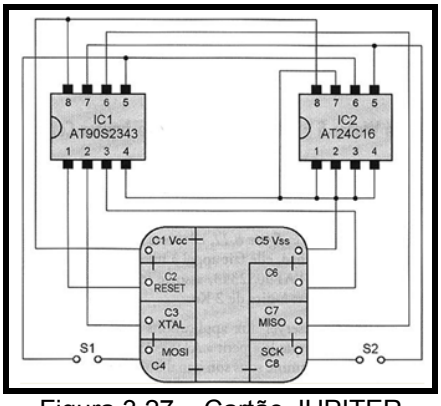


Figura 3.27 – Cartão JUPITER

Cartão BASIC

Este modelo de cartão é fabricado pela empresa alemã ZeitControl, e sua principal diferença em relação aos outros cartões já comentados neste trabalho, é que sua programação pode ser feita utilizando *software* BASIC específico do fabricante.

Esta linguagem criada pela empresa foi adaptada do BASIC comercialmente conhecido para a utilização em cartões inteligentes, e dessa forma, o *software* foi simplificado para a utilização em projetos no qual o desenvolvedor não necessite conhecer aprofundadamente a programação em *assembler* de microcontroladores, tanto da família PIC quanto da família AVR.

Outra vantagem neste modelo é que o *software* tem incorporado diversas bibliotecas de algoritmos de encriptação de dados, como por exemplo, DES e 3DES, facilitando assim a programação da segurança da informação armazenada no cartão. Existem diversos modelos de cartão comercializados atualmente, com diferentes capacidades de memória e de encriptação de dados.

O *software* desenvolvido pelo fabricante é gratuito, e pode ser carregado diretamente do sítio, e a principal vantagem é que ele conta com um simulador de leitor. Ao desenvolver aplicações, podem-se realizar testes utilizando cartão e leitor virtual, sem a necessidade de se adquirir o *hardware*.

Como o cartão contém um sistema operacional, não é necessário um programador especial, podendo ser programado por qualquer programador que seja suportado pelo *software* de desenvolvimento. (ZEIT, 2008).

Figura 3.28 – Cartão BASIC

3.2.1.2 Cartões inteligentes sem contato físico

Os cartões inteligentes sem contato físico utilizam a tecnologia RFID (*Radio Frequency Identification*) que significa Identificação por Radiofreqüência, desenvolvida pelo *Massachusetts Institute of Technology* (MIT), nos EUA, e que utiliza ondas eletromagnéticas para acessar dados armazenados em um microcontrolador. A ausência do ato inserção do cartão em um leitor eletrônico traz benefícios como economia de tempo e não desgaste dos terminais do cartão, aumentando assim sua vida útil. Os principais componentes que constituem um sistema RFID são: etiquetas, leitores de etiquetas, estações de programação de etiquetas, leitores de circulação e equipamento de ordenação.

Cada cartão tem em seu interior um *chip*, e este possui um código eletrônico único, conhecido como EPC – Electronic Product Code e que pode ser lido por meio de antenas de radiofreqüência. Existem modelos de cartões que não necessitam de alimentação, e são conhecidos como cartões passivos. Existem também os modelos ativos, que necessitam de energização em seu circuito interno. As freqüências comuns utilizadas nos sistemas RFID são em torno de 125KHz e 13,56MHz. A freqüência baixa, com variação de 9kHz a 135kHz tem como principal vantagem a alta aceitação por ser difundida mundialmente.

A distância de leitura é inferior a um metro e meio, e devido a esta característica suas principais aplicações são: identificação de animais, chaves de automóveis e identificação de livros em bibliotecas. A freqüência alta, na faixa de 13,56MHz, tem uma desvantagem de não poder ser utilizada próximo a metais, e suas principais aplicações são: movimentação de produtos, movimentação de equipamentos de linhas aéreas e acesso a edifícios. A norma que controla estes tipos de cartões é a ISO14443.

Tecnologia MIFARE®

A família MIFARE® foi desenvolvida pela empresa Philips, e atualmente é a tecnologia de cartões inteligentes sem contato mais difundida no mundo. A sua freqüência de trabalho é de 13,56MHz, e tem a capacidade de leitura e escrita. Existem diferentes modelos segundo a quantidade de informação que armazenam. Suas principais aplicações são:

- ✓ **Transportes públicos:** em substituição aos bilhetes tradicionais ou passes, utilizam-se os cartões MIFARE®, e as principais vantagens são de não requerer a impressão de dados de validação, evitar a formação de longas filas nos horários de pico no uso do transporte público e evitar fraudes como clonagem de passes ou bilhetes.

- ✓ **Controle de acesso:** são utilizados cartões MIFARE® para a identificação dos funcionários da empresa, principalmente em edifícios inteligentes. Vale salientar que a utilização desta tecnologia serve apenas para identificar a pessoa, mas não há garantia de que o usuário do cartão seja realmente o proprietário do mesmo. Para se solucionar este problema, é necessária uma autenticação do usuário, efetuada normalmente utilizando-se tecnologias biométricas, como o proposto no estudo de caso deste trabalho.

Figura 3.29 – Cartões RFID e respectivos leitores

4 APLICAÇÕES BIOMÉTRICAS

Este capítulo apresenta diversas aplicações tecnológicas da biometria, voltadas à área de segurança, no Brasil e no mundo. Algumas aplicações não tem detalhes de seus algoritmos, nem de suas limitações na aplicação, por questões de confidencialidade dos sistemas, visando dessa forma manter a segurança da instalação.

4.1 Urnas eletrônicas com leitor biométrico – impressão digital

No processo eleitoral do Brasil, o Tribunal Superior Eleitoral visa instalar urnas eletrônicas com leitores de impressão digital. As urnas eletrônicas, instaladas em 1996, agilizaram o processo de apuração dos resultados das eleições, no entanto, ainda são equipamentos susceptíveis a fraudes. O TSE tem como meta, instalar urnas com leitura biométrica para diminuir significativamente a tentativa de fraude.

Além disso, os custos envolvidos com a eleição seriam diminuídos, pois não seria necessária emissão de documentação em papel, e a função de mesário acabaria, encerrando dessa forma o trabalho de cerca de 1,5 milhão de eleitores convocados obrigatoriamente para trabalharem em dias de eleição.

A maior dificuldade está em se cadastrar cerca de 127 milhões de eleitores em todo o país, através da coleta de suas digitais e fotos. Para o processo de cadastramento, o TSE comprou um conjunto de componentes eletrônicos, tais como *laptop*, sensor de digitais tipo *scanner*, mini-estúdio fotográfico e caixa para transporte, no valor de R$13.500,00, em 2008.

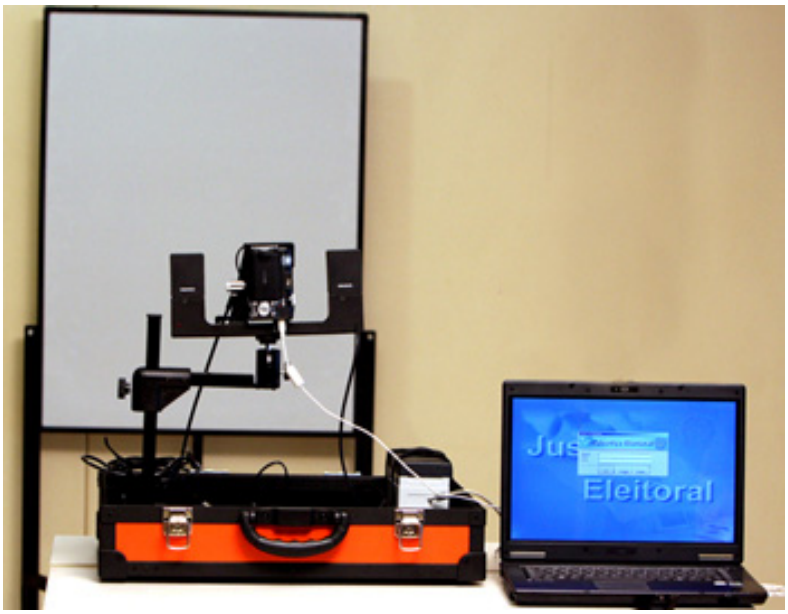


Figura 4.1 – Kit de cadastramento biométrico eleitoral

O novo modelo de urna, além de ter o leitor de impressões digitais, terá uma tela, onde deverá aparecer a foto do eleitor, no momento da confirmação de sua identificação. Uma das grandes vantagens da urna biométrica está na impossibilidade de mesários votarem pelas pessoas que não compareceram no dia da eleição, pois esta é uma fraude comum. O custo estimado para a implantação deste sistema em todo o país é de R$ 13 milhões de reais, tendo como referência o ano de 2008. (TSE, 2006).

Figura 4.2 – Urna com monitor e leitor biométrico

4.2 Utilização de biometria na venda de maconha na Holanda

Na cidade de Maastrich, Holanda, a venda de maconha é permitida nos cafés da cidade, apesar de ser considerada ilegal, no entanto o porte de pequenas quantidades é tolerado. O problema encontrado nesta venda está no fato de que menores de idade não podem comprar o produto, e maiores de idade tem um limite máximo de compra de cinco gramas por dia. No caso de venda a menores, ou de maiores quantidades que o permitido, são os cafés que respondem legalmente à justiça, e não os usuários. Para eliminar estes problemas, a Holanda irá implantar um sistema de autenticação por biometria, que consiste em leitura de impressões digitais e escaneamento facial, armazenamento das informações e controle da quantidade vendida por dia. O investimento inicial é de cerca de 100 mil euros em equipamentos, divididos entre os quinze cafés da cidade que vendem maconha atualmente. O maior problema encontrado é a invasão de privacidade. Os nomes e endereços das pessoas não serão armazenados neste novo sistema, e os detalhes sobre a quantidade adquirida de maconha a cada dia serão apagados depois da meia-noite. Os proprietários temem que as vendas venham a diminuir devido ao alto controle, mas acreditam que este novo sistema diminuirá significativamente os problemas judiciais, principalmente de irmãos mais novos que utilizam a identificação do irmão mais velho para comprar maconha. (GLOBO, 2007).

4.3 Aeroporto de Jacarta utiliza identificação pela íris

O aeroporto internacional de Jacarta, na Indonésia, instalou um sistema de identificação pela íris, com a intenção de diminuir as filas na identificação dos postos de imigração, no entanto, este serviço não é gratuito, cada passageiro que desejar passar pelo sistema de identificação pela íris, deverá pagar cerca de duzentos dólares. O nome adotado ao sistema é “Programa Safira”, e funciona da seguinte forma: passageiros se registram junto às autoridades migratórias, pagam uma taxa anual e se submetem a uma identificação eletrônica de ambos os olhos.

As informações são armazenadas em um banco de dados, para a futura comparação de dados no aeroporto. Segundo as autoridades locais, é possível identificar uma pessoa pela íris da mesma forma que a identificação ocorreria pelas impressões digitais, mas neste trabalho, verifica-se que a impressão digital só apresenta boa qualidade quando utilizada para autenticação da pessoa, a identificação desse ser feita de outra maneira.

Nos terminais do aeroporto, existem leitores de íris, e o passageiro perde cerca de dez segundos na sua identificação. O aparelho tem as instruções para o correto posicionamento do rosto em frente às câmeras, e a identificação não incomoda os usuários, pois não é emitido nenhum tipo de luz que possa ofuscar o olho, e a leitura ainda pode ser realizada sem a necessidade de se retirar óculos de sol. A empresa indonésio-holandesa, responsável pelo projeto, alega que o principal atrativo do programa é sua conveniência, embora também seja possível que a facilidade dos usuários cadastrados deixe as autoridades com mais tempo para identificarem, pelos meios habituais, outros passageiros que possam representar ameaças à segurança. Até o ano de 2006, quinhentos e cinqüenta passageiros já haviam se cadastrado no serviço. Um sistema semelhante na Holanda já conta com cerca de trinta e três mil usuários cadastrados. (REUTERS, 2006).

4.4 Unifenas usa biometria para controlar frequência dos alunos

A Universidade José do Rosário Vellano, em Minas Gerais, vai inaugurar um sistema de leitura biométrica de impressões digitais para controlar a frequência de seus alunos. O maior problema encontrado em praticamente todas as universidades é a lista de presença dos alunos, pois qualquer colega de sala de aula pode assinar pelo aluno que está ausente. O sistema implantado já está em uso desde 2007, e conta com um dispositivo de leitura biométrica dentro de cada sala de aula. A implantação do uso da biometria ainda permitiu o controle mais efetivo do acesso dos professores e o controle de ponto dos funcionários da segurança, que necessitam registrar sua presença em intervalos de quinze minutos, pelas áreas de monitoramento da instituição.

Grande parte do sistema foi desenvolvido e implantado pela própria universidade, e os custos envolvidos são somente da compra dos leitores biométricos. Uma parte do sistema foi comprado por uma empresa especialista em sistemas biométricos, e a universidade gastou cerca de dois mil reais por cada ponto de controle. O sistema implantado autentica o usuário em cerca de dois segundos. O professor Edson Antonio Velano, reitor da Unifenas, avalia positivamente o uso do sistema, mas admite que existem grandes dificuldades em sua implantação, pois se trata de quebra de paradigmas, pois não houve boa aceitação por parte dos alunos devido ao alto controle. (UNIFENAS, 2006).

4.5 Detran utiliza biometria nos centros de formação de condutores

Em todo o Estado de São Paulo, as pessoas que desejam obter a carteira de habilitação deverão ser identificadas por biometria nas auto-escolas. A medida é uma determinação do Departamento Estadual de Trânsito (DETRAN) para fiscalizar a presença dos candidatos à carteira de habilitação nas aulas teóricas e práticas. Em todas as auto-escolas do estado, deverão ter um leitor de impressões digitais para que sejam efetuadas as leituras biométricas. A medida visa acabar com as fraudes nos processos de aquisição de carteira nacional de habilitação, pois o DETRAN não tem como fiscalizar a presença dos candidatos, que devem obrigatoriamente realizar trinta horas práticas no volante. (INFO, 2006)

Figura 4.3 – Modelo de leitor biométrico utilizado pelo DETRAN/SP

5 CONTROLE INTERNO DA SEGURANÇA

Este capítulo apresenta as tecnologias utilizadas no controle interno da segurança. Os principais dispositivos que atuam para o controle interno são os circuitos fechados de televisão, conhecidos popularmente pela sigla CFTV. Atualmente, existem *softwares* de captura de imagem de sistemas CFTV capazes de atuar como dispositivos de alarmes, pois os mesmos ativam sirenes, discam para números de telefones pré-programados e podem acionam centrais de segurança. Os sistemas antigos de CFTV tinham apenas a função de captar e armazenar imagens. Ainda neste capítulo, serão demonstrados os principais dispositivos para controle perimetral de segurança, e os alarmes de intrusão, muito utilizados atualmente no mercado nacional. (PERES, 2006)

5.1 Circuito fechado de televisão CFTV

Circuito fechado de televisão, popularmente conhecido como CFTV, é um sistema de televisionamento que distribui sinais provenientes de câmeras localizadas em locais específicos, para pontos de supervisão pré-determinados. Os sistemas de CFTV podem ser aplicados com próposito de segurança e vigilância, em laboratórios de pesquisa, na área médica, linhas de produção de fábricas para o controle de processos e em atividades espaciais.

Os sistemas de CFTV normalmente utilizam câmeras de vídeo CCD (para produzir o sinal de vídeo), cabos ou transmissores/receptores sem-fio ou redes (para transmitir o sinal), e monitores (para visualizar a imagem de vídeo captada). Os sistemas existentes atualmente no mercado podem ter três configurações distintas, quanto ao requisito de instalação física:

- ✓ Sistemas interligados a fio, no qual a principal via de comunicação é o cabo coaxial. Este sistema normalmente é utilizado em circuitos analógicos;

- ✓ Sistemas *wirelles* – as câmeras se comunicam com as centrais de controle através de rádio-frequência;
- ✓ Sistemas por endereçamento IP: as câmeras possuem comunicação *Ethernet* incorporada, permitindo assim instalar o equipamento em redes estruturadas de informática.

Nestes casos, o ambiente de rede reconhece a câmera como sendo um *host* (microcomputador) do sistema.

5.1.1 Sistemas analógicos

Um sistema de circuito fechado de televisão analógica tem a finalidade de armazenar as imagens que são capturadas por câmeras analógicas e transmitir estas informações até um gerenciador de imagens. O principal cabo utilizado para transmissão de dados neste tipo de tecnologia é o cabo coaxial.

Figura 5.1 – Conjunto de equipamentos analógicos para CFTV

As imagens podem ser gravadas e armazenadas em fitas VHS, através de gravadores de vídeos conhecidos como *Time Lapses,* que são vídeocassetes com capacidade de armazenamento de aproximadamente 1000 horas de gravação em uma única fita VHS. Simultaneamente, as imagens gravadas são exibidas em um monitor, para a devida vigilância na central de controle. O armazenamento das imagens em fitas magnéticas é a principal característica de um sistema CFTV analógico.

Existem alguns equipamentos que são auxiliares ao sistema CFTV analógico:

- ✓ ***QUAD*:** Com a utilização deste equipamento, é possível realizar a visualização simultânea de imagens provenientes de quatro câmeras, dividindo-se a tela do monitor em quatro quadrantes iguais;

- ✓ ***DUAL QUAD*:** Permite a entrada de sinais analógicos de até oito câmeras, sendo possível sequenciamento e visualização de quatro em quatro imagens;

- ✓ ***TIME LAPSE*:** Trata-se de um tipo de videocassete profissional projetado para gravação de longa duração. Os tempos de gravação típicos encontrados em diversos equipamentos são: 24, 128 e até 960 horas com uma única fita cassete, modelo VHS;

- ✓ **MULTIPLEXADOR:** Permite que se observe e grave imagens de até 16 câmeras simultaneamente, dividindo a tela do monitor em até 16 pequenas imagens. O multiplexador também tem a função de digitalizar a imagem e enviar o sinal digitalizado para um gravador, caso haja um acoplado a ele. Posteriormente, ao assistir a fita que possui as 16 câmeras gravadas juntas, o multiplexador se transforma em um demultiplexador, ou seja, é possível escolher uma câmera específica para visualizar sua imagem em tela cheia;

- ✓ **MONITOR:** são fabricados para funcionar 24 horas por dia diferenciando-se dos televisores que são fabricados para um funcionamento de até 6 horas por dia. Podem ser dispensados da aplicação direta ao sistema CFTV, e nestas condições, as imagens podem ser transmitidas aos televisores de uma residência, ou ao sistema de antena coletiva de um edifício.

5.1.2 Sistemas digitais

O sistema de gravação digital tem como característica principal monitorar e gravar simultaneamente suas imagens através de um computador. A qualidade das

imagens capturadas é superior ao sistema analógico, pois são gerados até 60 quadros por segundo, o que representa o dobro de resolução comparado a um sistema convencional.

O gerenciamento das imagens é feito através de *softwares* de gerenciamento específicos, e são gravadas em *Hard Disk (HD)*, que podem posteriormente serem armazenadas em fitas DAT.

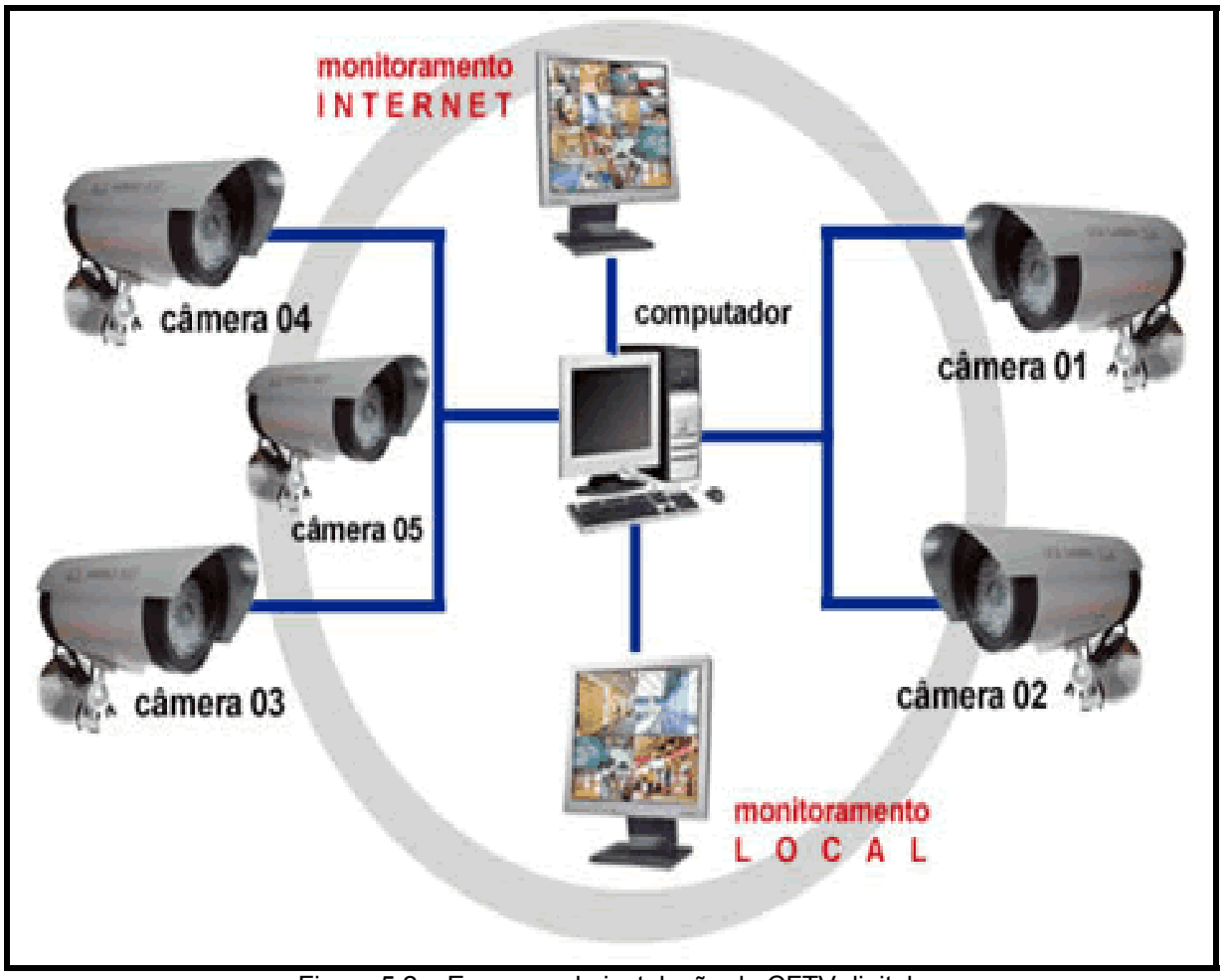


Figura 5.2 – Esquema de instalação de CFTV digital

As principais vantagens dos sistemas de CFTV digital são:

a) Alta qualidade de gravação das imagens;
b) Monitoramento ao vivo através da *Internet*;
c) Procura inteligente de evento por data, hora ou câmera específica (rápida busca da informação);
d) Relatórios de eventos;
e) Detecção de movimento;

f) Impressão de imagens;
g) Gravação por alarme e/ou agenda;
h) *Backup* em HD, *Zip Disk*, CD;
i) Acesso remoto em tempo real por *modem*, rede local ou *internet*;
j) Proteção por senha;
k) Gravação em tempo real;
l) Integração de alarmes e sensores de presença.

5.1.3 Tipos de câmeras

Para os sistemas de circuito fechado de televisão, existem diversos tipos de câmeras, como por exemplo, as micro-câmeras, câmeras *pin hole*, as mini-câmeras, câmeras profissionais, câmeras *speed dome* e câmeras IP. Abaixo, tem-se o detalhamento de cada modelo.

5.1.3.1 Micro-câmeras

Caracterizam-se por ter baixo custo, facilidade de instalação, porém qualidade limitada. Podem ser encontradas em versões preto e branco e coloridas. A qualidade das imagens geradas e o desempenho em áreas muito grandes são as principais desvantagens. Alguns modelos possuem emissores de luz infravermelhos acoplados à câmera para a captação de imagens no escuro, a pequenas distâncias.

Figura 5.3 – Micro câmera

5.1.3.2 Câmeras *Pin Hole*

São micro câmeras com a característica de possuírem uma lente com tamanho extremamente reduzido, sem prejuízo à captação da imagem. São geralmente utilizadas em aplicações o qual o tamanho deva ser reduzido, como em locais ocultos. Sua aplicação se concentra em residências, consultórios, escritórios e qualquer outro local onde a câmera deva estar escondida, sem que as pessoas percebam sua presença.

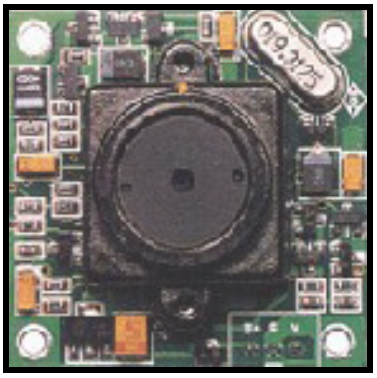


Figura 5.4 – Câmera *Pin Hole*

5.1.3.3 Mini câmeras

Seu processo de captura de imagens se assemelha aos das micro-câmeras, com a diferença de que estas possuem a conexão para diversos tipos de lentes convencionais de CFTV, podendo assim ter o controle de foco e captura de imagens ajustada ao ambiente.

Figura 5.5 – Mini câmeras

5.1.3.4 Câmeras profissionais

Caracterizam-se por serem mais robustas e com mais recursos tecnológicos, como por exemplo, a possibilidade de troca de lentes, ajustes automáticos de íris, e outros ajustes que permitem melhorar a qualidade das imagens capturadas. Possuem melhor resolução e qualidade de imagem, quando comparadas às micro-câmeras.

Figura 5.6 – Câmera profissional

5.1.3.5 Câmeras *Speed Dome*

Tem sua movimentação motorizada, e conseguem analisar imagens em giros de até 360 graus no eixo horizontal, com movimentações de até 90 graus no eixo vertical. Existem modelos que se comunicam em barramento de campo RS485, permitindo assim o envio das imagens a uma central de controle.

A movimentação de seu posicionamento é feita através de mesas de controle, e é realizada pelo responsável da central, que pode inclusive ampliar a imagem, aproximando a um ponto específico.

Figura 5.7 – Câmera *Speed Dome* e mesa de controle

5.1.3.6 Câmeras IP

As câmeras IP, conhecidas também como *network cameras*, possuem um servidor *Web* interno que possibilitam o envio de imagens em tempo real diretamente por uma rede interna ou *internet*. Podem ser fixas ou móveis, com *zoom* e movimentos horizontais e verticais, controladas à distância pela rede. Existem modelos que podem se comunicar via *wirelles*, sem a necessidade de conexão física, com exceção de sua alimentação, que é tipicamente de 12Vcc. Os protocolos e as interfaces mais utilizados e implementados nestes tipos de câmeras são TCP/UDP/IP, RTSP, SMTP, NAT, ARP, *Telnet*, DHCP, IEEE 802.11g, IEEE 802.11b, IEEE802. 3.

Figura 5.8 – Câmera IP com tecnologia *wirelles*

5.1.4 Servidores de gravação digital de imagens

São equipamentos utilizados em sistemas CFTV digitais, que armazenam informações sem a necessidade de intervenção humana. Normalmente são dotados de *softwares* que trabalham com altas taxas de compressão para a diminuição do tamanho dos arquivos gerados pela captura da imagem e alta capacidade de armazenamento. O custo destes equipamentos está diretamente vinculado à capacidade de armazenamento e número de canais de entrada no dispositivo, pois os mesmos têm a capacidade de entrada direta do sinal de uma câmera.

Os modelos típicos trabalham com até 16 câmeras em sua entrada, e o equipamento grava em disco rígido as informações provenientes de todas as câmeras

simultaneamente. Ainda existe a possibilidade de se visualizar as imagens através de um monitor de vídeo convencional, mesmo durante a gravação dos dados.

A resolução de captura das imagens pode ser previamente programada de modo independente por canal, ou seja, cada imagem proveniente de uma câmera pode ter a imagem capturada com resolução maior ou menor que outra câmera, desde que a resolução máxima total do dispositivo não seja ultrapassada.

Na visualização das imagens em tempo real, o equipamento permite configurar a apresentação no monitor de apenas uma imagem, ou de todas as imagens provenientes de todas as câmeras instaladas no dispositivo, através de *software* específico. A grande vantagem nos sistemas digitais de CFTV é a busca rápida das informações, pois nestes tipos de gravadores de imagens, o usuário do sistema de segurança tem acesso a ferramentas de *software* capazes de procurar imagens de forma indexada por data, hora e canal.

Figura 5.9 – Servidor digital de CFTV

5.1.5 Placas de captura para sistemas CFTV

São circuitos eletrônicos dedicados à conexão direta com câmeras de vigilância, e podem ter até 16 entradas de vídeo e 16 entradas de áudio. Tem as mesmas funções do servidor de imagens citado no item anterior deste trabalho, no entanto, precisam ser instaladas em um microcomputador convencional.

Seu desempenho está vinculado ao modelo de microcomputador utilizado. Pode efetuar gravações de até 480 *frames* por segundo, o que a torna um equipamento de atuação para visualização de imagens em tempo real. A compressão das imagens

para o armazenamento é feita através de *hardware*, e baseia-se nas tecnologias MPEG2 e MPEG4, liberando dessa forma os processos executados na CPU do microcomputador.

Figura 5.10 – Placa de captura para sistema CFTV

5.1.6 *Softwares* para sistemas CFTV

Os *softwares* para sistemas CFTV são chamados de sistemas de vigilância digitais, baseados em microcomputador, pois tem as funcionalidades de um sistema de segurança, podendo até gerar alarmes. Funcionam normalmente com técnicas de comparação de imagens em duas dimensões.

Dessa forma, o usuário pode gravar uma imagem padrão, chamada de *template*, e armazenar no *software* como sendo uma imagem sem geração de alarmes. A partir desta informação, qualquer objeto, animal ou pessoa que entrar no ambiente, mudará a imagem padrão, que será a fonte de comparação do *software*, fazendo com que o mesmo ative um alarme.

Como todo o sistema de segurança se encontra instalado em um microcomputador, a geração do alarme se dá de diversas formas, como por exemplo, envio de *e-mail* para um endereço pré-programado, ou ativação de uma sirene.

Os *softwares* possuem recursos de compressão de imagens, caso isto não seja realizado pelo *hardware* responsável pela captura da imagem, e ainda podem gerenciar imagens provenientes de diversos servidores de vídeo, simultaneamente.

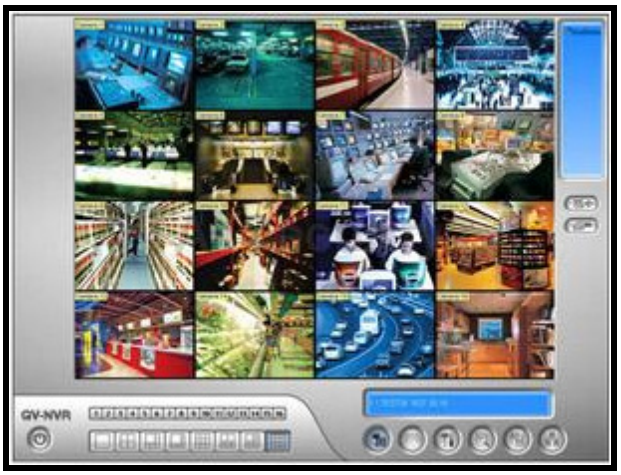


Figura 5.11 – Tela de um *software* para sistemas CFTV

5.2 Sistemas de alarmes de intrusão e segurança perimetral

A proteção das áreas externas de residências e empresas precisa ser realizada por equipamentos de alta tecnologia, que façam uma detecção de invasão efetiva, pois diversos fatores como condições ambientais, animais, árvores e outros objetos em movimento podem causar uma falsa detecção de invasão. Outro fator importante nos sistemas de segurança perimetral é a possibilidade de se ocultar os equipamentos para que o invasor não tenha acesso aos dispositivos e em consequência não possa vir a desativá-los.

Os sistemas de segurança perimetral são compostos basicamente de sensores externos, projetados para funcionar em diversas circunstâncias ambientais, como temperatura elevada, chuva, vento, ruído, etc. (TSS, 2005).
Os sensores externos podem ser classificados em alguns grupos:

a) **Sensores volumétricos:** geram um campo invisível de atuação, e detectam qualquer movimento realizado na área deste campo. São praticamente imunes à maioria das condições ambientais.
b) **Sensores para cerca/muro:** detectam a invasão através da vibração do sistema elétrico instalado ou da tentativa de corte do enlace do sensor.

c) **Sensores de movimento em vídeo:** detectam a invasão através da comparação de imagens pré-programadas ou por detecção de calor (infravermelho).
d) **Sensores de barreira:** tem a finalidade de fornecer uma barreira física ao intruso e um sistema de sensoriamento para a detecção. Podem ser utilizados como uma maneira de intimidação à invasão do sistema.

5.2.1 Detectores magnéticos

Os detectores magnéticos são compostos de duas lâminas metálicas que formam um contato normalmente aberto (*reed switch*), e se fecham na presença de um campo magnético. São muito utilizados em alarmes residenciais, sendo instalados em portas e janelas. O contato elétrico é instalado na parte fixa da porta ou janela, e um ímã permanente é instalado na parte móvel.

Ao se abrir a janela ou porta, o ímã permanente se afasta do detector, fazendo com que seu contato elétrico se abra, retirando assim a energização de um ponto específico do controlador de alarme (canal ou laço), que interpretará este evento como invasão do local.

Os detectores magnéticos podem ser instalados com fios, interligando o sensor até uma central de controle, ou através de radiofrequência, sem a necessidade de fios para a comunicação com a central. Neste segundo caso, é necessário o uso de baterias para a alimentação do dispositivo. (ECP, 2007)

Figura 5.12 – Conjunto detector magnético sem fio

5.2.2 Detectores piroelétricos

Também conhecidos como detectores de infravermelho passivos, os detectores piroelétricos detectam a presença de pessoas através da leitura dos raios infravermelhos emitidos pelo corpo humano (calor).

São muito utilizados para a automação de sistemas de iluminação, tendo a função de acionar as lâmpadas de um local específico quando da presença de uma pessoa. Seu custo é baixo, e o mesmo pode ser instalado no escuro, pois sua funcionalidade não depende da captura de imagens. A principal desvantagem é a baixa precisão e vulnerabilidade a fraudes. (NAPCO, 2007)

Figura 5.13 – Sensor infravermelho passivo

5.2.3 Detectores por quebra de vidro

Detectores por quebra de vidro incorporam um microfone ligado a um circuito composto por um analisador de áudio, e detectam o som típico da quebra de um vidro (análise frequencial), ignorando distúrbios ambientais e ruídos externos aleatórios.

Os equipamentos mais recentes não necessitam estarem presos a uma janela, podendo dessa forma proteger diversas janelas simultaneamente, a até 6 metros de distância do equipamento. Estes sistemas de segurança podem incluir ajuste de sensibilidade, reduzindo o número de alarmes falsos. (EURO, 2007).

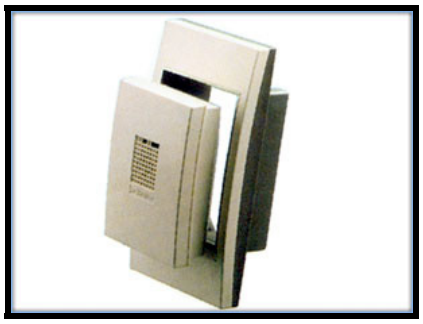


Figura 5.14 – Detector por quebra de vidro

5.2.4 Unidades de controle

Consiste em um equipamento microprocessado, responsável por captar todas as informações de campo, enviadas pelos sensores, e processar estas informações, avisando ao proprietário do ambiente sobre qualquer tentativa de invasão.
As principais atividades de uma central de alarmes são:

a) Enviar sinal elétrico a um local remoto, previamente escolhido, de forma silenciosa, avisando sobre a intrusão;
b) Realizar discagem telefônica para um número previamente programado;
c) Disparar sirene no local da intrusão;
d) Avisar central de monitoramento remoto.

As comunicações podem ser realizadas com fio ou sem fio (*wirelles*), e alguns equipamentos possuem bateria e telefonia celular incorporadas, para que possam enviar aviso de alarme ao proprietário mesmo com o corte dos fios da instalação elétrica, ou desmontagem do sistema. (BOLZANI, 2004)

Figura 5.15 – Central de controle de segurança

5.2.5 Sensor infravermelho ativo

É composto por um transmissor que emite um feixe Infravermelho para um receptor. Caso haja interrupção do feixe transmitido, o alarme é disparado. Existem modelos de feixe único ou de feixe duplo. Para evitar disparos falsos por vegetações e aves, é recomendado o uso do sensor de feixe duplo para ambientes externos.

O alcance dos feixes pode variar de 20 metros até 1500 metros, dependendo do dispositivo utilizado, no entanto, recomenda-se limitar a distância do receptor ao emissor em no máximo 150 metros, pois uma alta intensidade de chuva pode afetar o desempenho do dispositivo, e longas distâncias dificultam o alinhamento dos feixes. (THOMAZINI; ALBUQUERQUE, 2007)

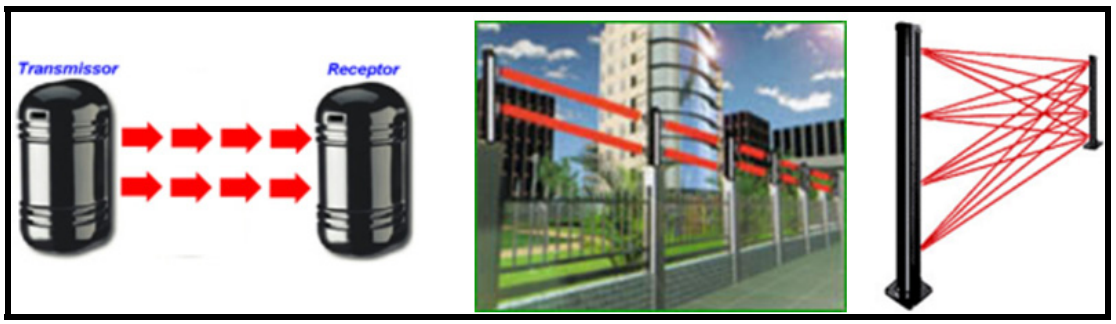


Figura 5.16 – Sensor infravermelho ativo e aplicações

5.2.6 Sensor microondas

Consistem em detectores de intrusão baseados em emissão de microondas. Dois dispositivos eletrônicos são instalados um em frente ao outro, sendo que um dos equipamentos emite microondas em torno de 10GHz com baixa potência, e o outro é responsável pela recepção do sinal, (conjunto emissor/receptor), criando assim uma zona de proteção em formato elipsóide, com dimensões que variam de acordo com o tipo de antena, a distância entre o dispositivo emissor e o dispositivo receptor, e a regulagem da sensibilidade, existente no controlador eletrônico do receptor.

O alcance deste tipo de sensor varia de 50 metros até 200 metros. O dispositivo receptor possui um processador interno, responsável por analisar o sinal recebido, e possui alto desempenho na detecção, com baixos índices de falsos alarmes. (REFORCE, 2007)

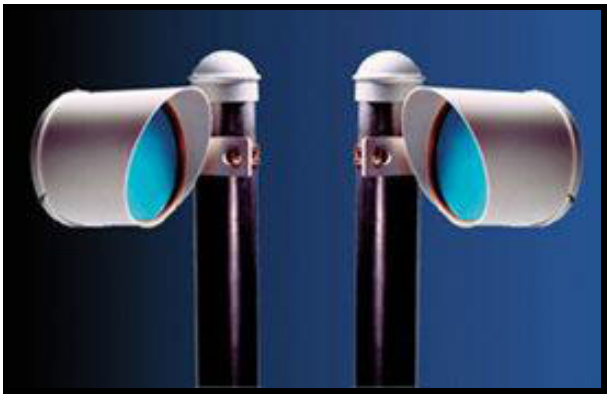


Figura 5.17 – Conjunto sensor de microondas

5.2.7 Sensor por campo eletromagnético

Consistem em cabos sensoriais e de alimentação, instalados dentro da terra, normalmente cobertos por grama ou concreto. Através da alimentação elétrica dos mesmos, é gerado um campo eletromagnético em torno de cabos sensoriais. No caso de intrusão, o corpo humano modifica o campo eletromagnético recebido pelo cabo sensorial, e esta variação é detectada, gerando o alarme. Assim como outros tipos de sensores, a sensibilidade deste equipamento pode ser regulada de forma a diminuir falsos alarmes gerados pela detecção de pequenos animais. Normalmente são instalados em áreas externas, e em locais onde a construção de muros prejudique a arquitetura do empreendimento. (ORMAX, 2007).

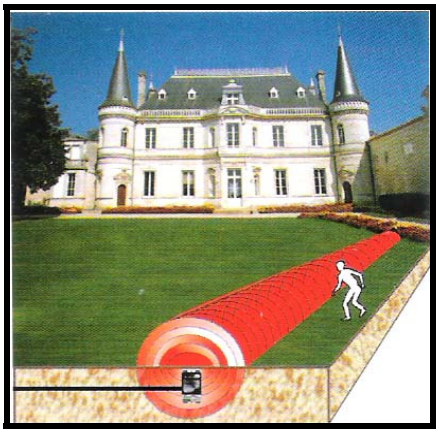


Figura 5.18 – Ilustração de um sistema de sensoriamento eletromagnético

5.2.8 Sensor por cabo piezo elétrico (microfônico)

Estes sensores são compostos de cabos coaxiais fixados nas cercas, com distância aproximada de 30 centímetros de um cabo a outro, e visam detectar o corte, ruptura ou vibração de cercas e alambrados.

As perturbações mecânicas são transformadas em sinais eletrônicos e são analisados por um processador digital, que irá determinar a condição de alarme em função de parâmetros pré-estabelecidos.

Os alarmes falsos, gerados por contato de animais, aves e ventos fortes que possam vibrar as cercas, são evitados devido à prévia programação de sensibilidade na central de alarmes. (REFORCE, 2007).

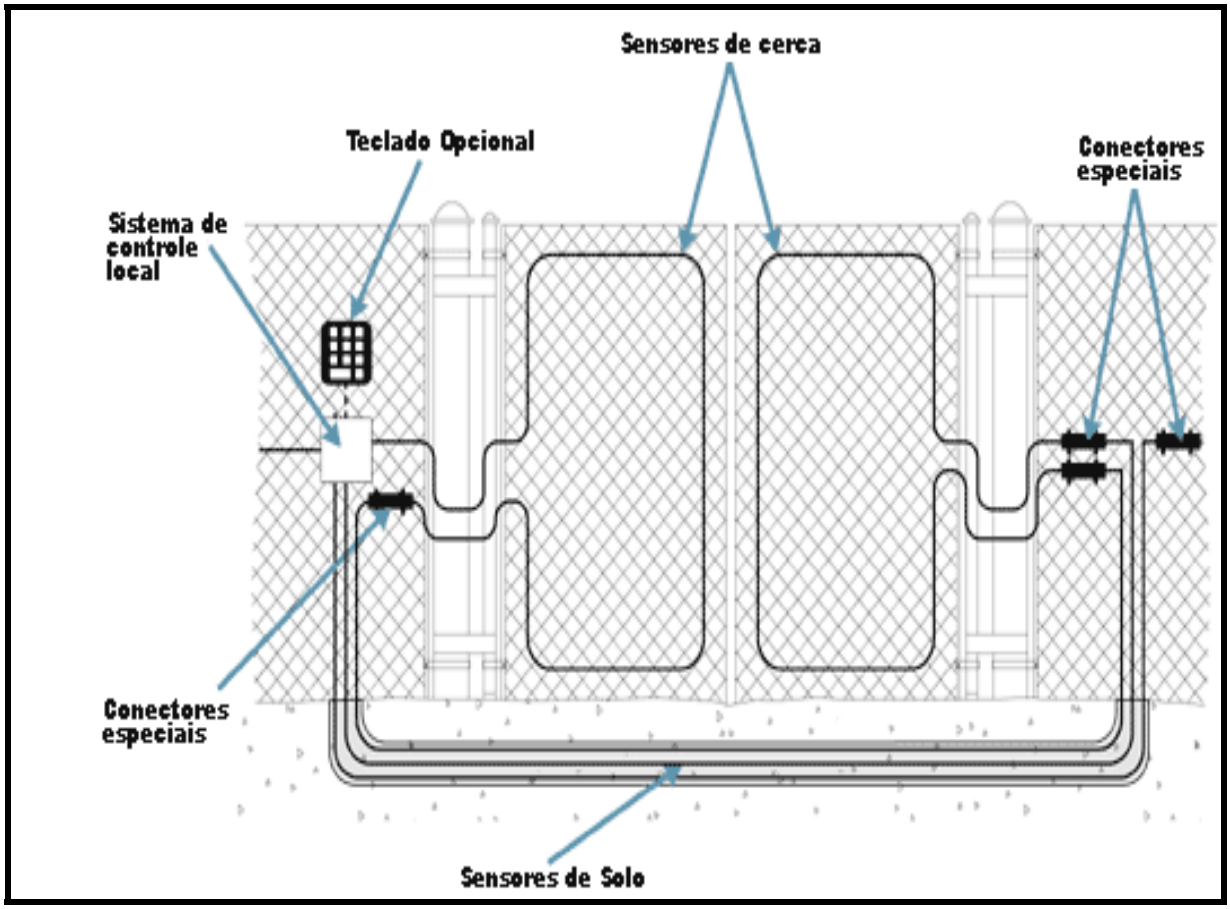


Figura 5.19 – Exemplo de funcionamento de cabo microfônico

5.2.9 Sensor por fibra ótica

A fibra ótica transmite luz, e por este motivo é segura quando instalada próximo a campos eletromagnéticos. Sua utilização na detecção de intrusão consiste em instalar cabos óticos em cercas, paredes, túneis, ou ainda enterrados diretamente na terra ou sob pisos.

O princípio de funcionamento do sistema consiste na transmissão de luz através do elemento ótico, gerando assim um padrão pré-definido de comunicação, no qual um receptor microprocessado verifica constantemente esse padrão.

No caso de tentativas de intrusão, serão geradas vibrações, e movimentações do cabo ou pressões provocarão um deslocamento do feixe de luz transmitido. Uma central de processamento digitaliza os sinais e analisa o nível e a frequência deste deslocamento, e verifica se os padrões do sinal estão dentro do padrão; caso não estejam, um alarme será ativado.

O equipamento permite ajustes de sensibilidade para se evitar falsos alarmes gerados por animais ou condições ambientais. (TSS, 2007).

5.2.10 Cercas eletrificadas

As cercas eletrificadas consistem em um sistema composto por hastes de alumínio instaladas sobre muros, e isoladores com quatro ou seis cabos finos de aço inoxidável, ligados a uma central de processamento e geração de alta tensão pulsante. No caso de rompimento dos cabos ou fuga de corrente elétrica para o terra, ocorrerá geração de alarme pela central de processamento.

A intensidade do choque elétrico gerado pela central é de aproximadamente 8000 Volts, e a intensidade de corrente elétrica é de aproximadamente 1mA, e sua

geração é pulsante, o que provoca forte susto no invasor mas não oferece riscos à vida do mesmo.

As principais vantagens de se utilizar a cerca eletrificada como equipamento de segurança perimetral consistem basicamente em baixo consumo de energia, maior resistência ao tempo, alta segurança, alta confiabilidade e baixo custo.

Apesar de não existir uma legislação específica sobre a utilização da cerca eletrificada no Brasil, alguns aspectos jurídicos podem ser levados em consideração:

a) A instalação de cerca eletrificada não é proibida, pois se trata de um exercício regular de direito, O artigo 5º, inciso II, da Constituição Federal dispõe que “ninguém será obrigado a fazer ou deixar de fazer alguma coisa senão em virtude da lei”;
b) A cerca eletrificada é chamada de ofendículo, meio pelo qual o proprietário de um bem coloca aparelhos para impedir e prevenir a invasão de sua propriedade. Não há regulamentação legal no âmbito federal para altura mínima, potência máxima, tipo de choque;
c) Os artigos 572 e 588 do Código Civil prevêem que “o proprietário pode levantar em seu terreno as construções que lhe aprouver, salvo o direito dos vizinhos e os regulamentos administrativos, e ainda tem direito de cercar, murar, valar, ou tapar de qualquer modo seu prédio.”

Algumas recomendações sobre a instalação e uso das cercas eletrificadas devem ser seguidas: (ABESE, 2007).

a) O equipamento não pode oferecer risco à integridade física dos usuários ou de quem venha a “tocar” nele por estar eletrificado;
b) O choque provocado pela cerca é conhecido como choque moral, possui alta voltagem e baixa amperagem. Deve ser pulsativa e não deve queimar, deixar marcas ou fazer com que os animais e as pessoas que nela encostem ou segurem fiquem presas;
c) Sinalizar devidamente o local (perímetro) a respeito da cerca e suas consequências;

d) Informar todos os moradores, funcionários e a quem se faça necessário, que ocupem a área interna da cerca, de sua finalidade e periculosidade, principalmente as crianças, certificando-se de sua compreensão;

e) Informar vizinhos sobre a finalidade e a periculosidade da cerca;

f) Desligar o equipamento antes de regar plantas próximas à cerca, fazer podas de árvores ou plantas (caso exista) e fazer manutenção do equipamento ou do muro;

g) Utilizar sempre assistência técnica autorizada/credenciada;

h) Não deixar que a vegetação, caso exista, venha a tocar a cerca.

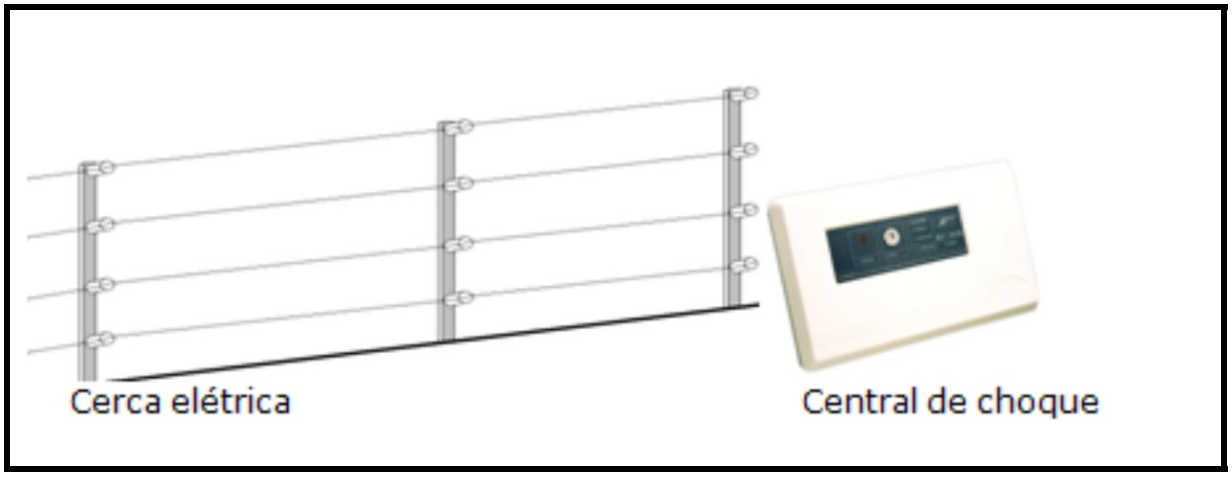


Figura 5.20 – Exemplo de aplicação de cerca eletrificada

6 ESTUDO DE CASO – IMPLANTAÇÃO DE SISTEMA BIOMÉTRICO

A proposta de implantação de um sistema de segurança utilizando biometria foi definida a partir da necessidade de uma instituição de ensino. Inicialmente, pensou-se em implantar biometria no controle de acesso dos alunos e funcionários, no entanto, a escola ocupa uma área interna a uma fábrica, e esta não permitiu o acesso às catracas existentes para que fossem efetuadas as devidas modificações no sistema. Esta modificação aumentaria significativamente o nível de segurança.

Definiu-se então o controle do acesso à sala do servidor de informática, pois a escola tem uma diretriz específica sobre a segurança e controle no acesso a este ambiente. Mensalmente, um funcionário deve acessar a sala para efetuar *backup* físico dos arquivos do servidor em fitas DAT, e armazenar em setor responsável.

A sala do servidor é um ambiente com três metros de comprimento por dois metros de largura, com um servidor de informática em seu interior, e um cofre com abertura mecânica, onde são armazenados os *softwares* originais utilizados pela escola.
Para acesso a este ambiente, tem-se uma porta de 80 centímetros de largura e 2,10 metros de altura, com uma fechadura convencional, abertura por chave simples.

A proposta é retirar a fechadura convencional, e instalar uma fechadura elétrica, com acionamento realizado pelo servidor. Além da troca da fechadura, será instalado um leitor biométrico de impressão digital, próximo à porta, para que o usuário possa colocar seu dedo indicador e ter validado sua entrada na sala do servidor.

A impressão digital normalmente é utilizada apenas para autenticar a identificação previamente realizada por outros dispositivos, como por exemplo, a utilização de crachás com códigos de barra, ou teclados numéricos para que possa ser digitada uma senha, no entanto, nesta aplicação, existe somente uma pessoa habilitada a acessar a sala do servidor em todo o ambiente educacional, portanto, não se faz necessária a identificação prévia da mesma.

6.1 Implantação do *hardware*

O *hardware* básico para a implantação deste sistema será a instalação do leitor biométrico, da fechadura elétrica e de um sistema de interface entre o servidor de informática e a fechadura, proposta neste trabalho. O diagrama em blocos abaixo define o *hardware* que será utilizado neste estudo de caso:

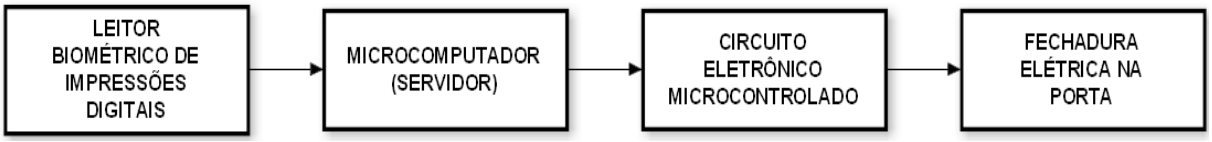


Figura 6.1 – Diagrama em blocos do *hardware*

6.1.1 Leitor biométrico utilizado

O leitor biométrico utilizado para efetuar a captura da imagem de uma impressão digital já tem incorporado o *scanner*, e o circuito de processamento necessário à aquisição da imagem. A comunicação entre o leitor e o servidor será feita através de um cabo incorporado ao leitor, com comunicação USB (Universal Serial Bus) versão 2.0. No servidor, as informações adquiridas serão tratadas e armazenadas em um banco de dados, e essas características serão tratadas na descrição do *software* utilizado. Abaixo, tem-se a foto superior do circuito eletrônico, com o *scanner* ótico incorporado do leitor de impressões digitais, que pode ser visualizado no centro do circuito, com uma janela de captura na cor vermelha, e um conjunto de *leds*, que servem para iluminar o dedo no momento da aquisição da imagem.

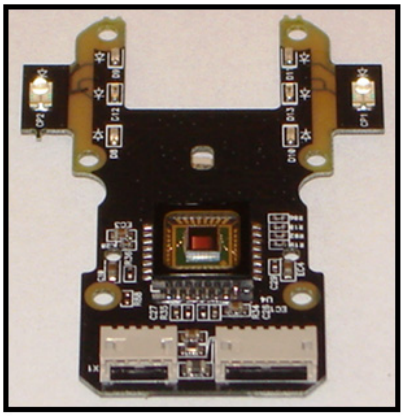


Figura 6.2 – Foto superior do circuito do leitor de impressões digitais

O conjunto de seis *leds* pisca três vezes ao iniciar o dispositivo, e então, após a checagem inicial ter sido completada, apenas quatro *leds* permanecem acesos. Ao tocar o dispositivo, um sensor interno detecta a presença do dedo, fazendo com que todos os *leds* se acendam, para melhorar a imagem detectada pelo *scanner.* Após cerca de um segundo, os *leds* se apagam, mostrando dessa forma que o processo de detecção da impressão digital terminou.

Abaixo, tem-se a foto inferior do circuito eletrônico, com a imagem do processador utilizado, DP6471, que é responsável por todo o processo de captura e processamento da imagem da impressão digital.

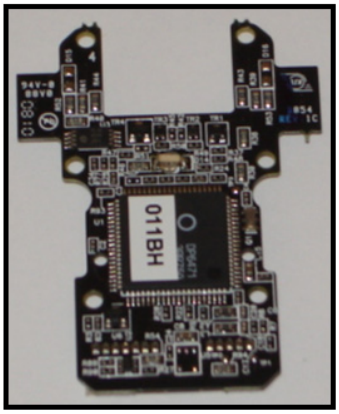


Figura 6.3 – Foto inferior do circuito do leitor de impressões digitais

O *scanner* ótico tem a dimensão aproximada de meio centímetro quadrado, sendo dessa forma muito menor que um dedo. Para que seja efetuada leitura de dedos de diversas dimensões, sem alterar o tamanho do *scanner*, utiliza-se uma lente direcional, que amplia a imagem capturada, e ainda serve como dispositivo de proteção ao *scanner*, uma vez que impede o contato físico direto com o dispositivo eletrônico sensível. Abaixo, tem-se a foto do conjunto de lente, que fica sobreposto ao *scanner* ótico.

Figura 6.4 – Conjunto de lentes e acoplamentos do leitor

Todo o *hardware* se comunica com um microcomputador através de comunicação padrão USB versão 2.0. A sigla USB vem de Universal Serial Bus, e trata-se de uma tecnologia de comunicação implementada por um consórcio de empresas de tecnologia da informação, em 1995. A velocidade de comunicação na versão utilizada neste trabalho varia de 1,5 a 400Mbps, e o número máximo de conexões de dispositivos no mesmo canal é de 127. O cabo de comunicação padrão é composto por quatro fios, sendo dois para dados, e dois para a fonte de alimentação de 5Vcc, e o comprimento máximo do cabo é de 5 metros. Nesta aplicação, o comprimento do cabo é de três metros, esta distância foi definida pensando-se nas posições entre o leitor de impressões digitais e a porta (conector) USB do servidor da sala. (USB, 2008)

Abaixo, tem-se a figura do cabo utilizado nesta aplicação.

Figura 6.5 – Cabo de comunicação entre o leitor e o microcomputador

Todo o conjunto leitor de impressões digitais pode ser visto na figura abaixo:

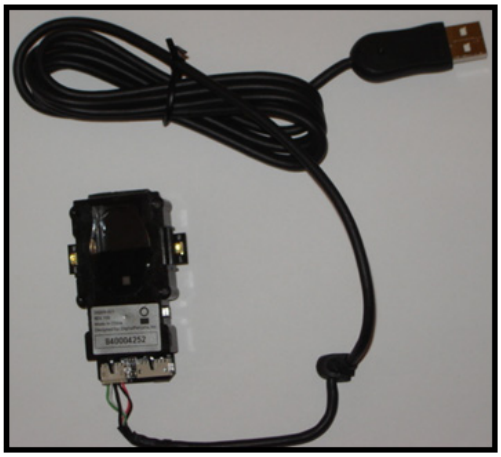


Figura 6.6 – Dispositivo de leitura biométrica

6.1.2 Microcomputador servidor

O servidor utilizado é o modelo MX221, fabricante Itautec, e suas principais características técnicas são:

- ✓ Gabinete em *rack* modelo 2U;
- ✓ Dois processadores modelo Intel® Xeon™ dual core;
- ✓ Memória RAM modelo FB-DIMM DDR2 PC5300 com ECC, de 16GB de;
- ✓ Rede Ethernet 2 x 10/100/1000 Mbps com I/OAT;
- ✓ Placa de vídeo Padrão VGA com 16MB de memória;
- ✓ Controladora IDE com um canal ATA100;
- ✓ Controladora SATA com seis canais de 3.0GB/s cada;
- ✓ Controladora SAS com quatro canais SAS de 3.0GB/s cada;
- ✓ Controladora RAID de oito canais SAS de 3.0GB/s cada;
- ✓ Dois discos SATA fixos;
- ✓ Unidade ótica CDROM;
- ✓ Dois *slots* PCI-X 64 bits/133MHz;
- ✓ Um *slot* PCI-X 64 bits/100MHz;
- ✓ Dois *slots* PCI-Express no formato x8;
- ✓ Um *slot* PCI-Express x4 no formato x8;
- ✓ Quatro interfaces de comunicação USB;
- ✓ Uma interface de comunicação serial padrão IEC-RS232C
- ✓ Uma interface de comunicação paralela;
- ✓ Uma interface de comunicação de rede com conector RJ45;
- ✓ Uma interface de vídeo padrão VGA;
- ✓ Uma interface para teclado e uma para mouse padrão OS/2;
- ✓ Fonte integrada fixa de 650W;
- ✓ *Software* de gerenciamento Windows 2003 Standard.

Nenhuma interface de comunicação USB é utilizada pela instituição, portanto, a instalação do leitor biométrico no servidor não teve grandes problemas, bastando apenas conectar o cabo ao conector do servidor.

6.1.3 Circuito de interface

O leitor biométrico está fisicamente ligado ao servidor (microcomputador) através da conexão USB. Com esta conexão, é possível efetuar a leitura da impressão digital e a autenticação do usuário em questão. No entanto, não existe um meio físico para a comunicação entre a fechadura elétrica e o servidor.

Para que seja efetuada esta comunicação, foi implementado um circuito eletrônico, que efetua a comunicação da fechadura com a porta paralela do microcomputador. Abaixo, pode-se visualizar o esquema eletrônico do circuito:

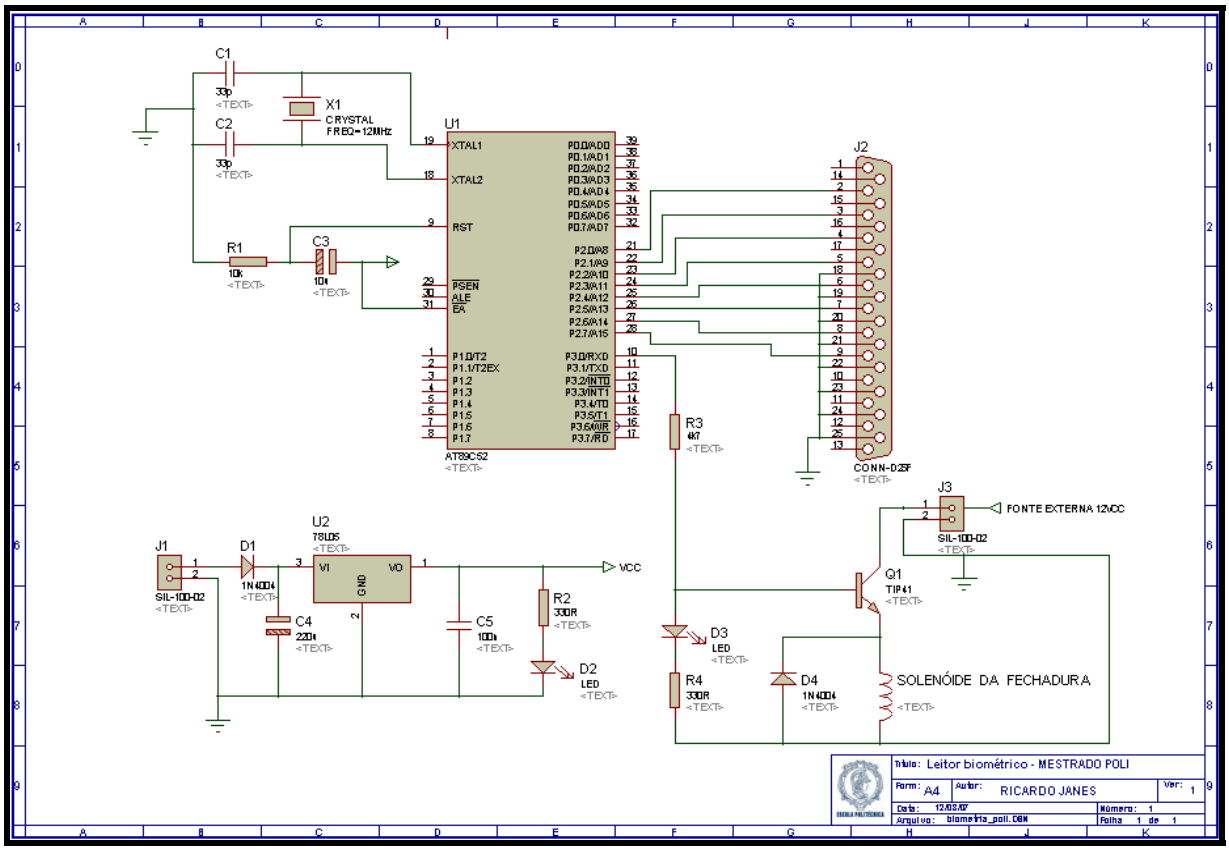


Figura 6.7 – Circuito eletrônico microcontrolado

Abaixo, pode-se visualizar uma foto do circuito implementado para o interfaceamento entre os dispositivos envolvidos, com o cabo de comunicação paralela conectado ao circuito e ao servidor.

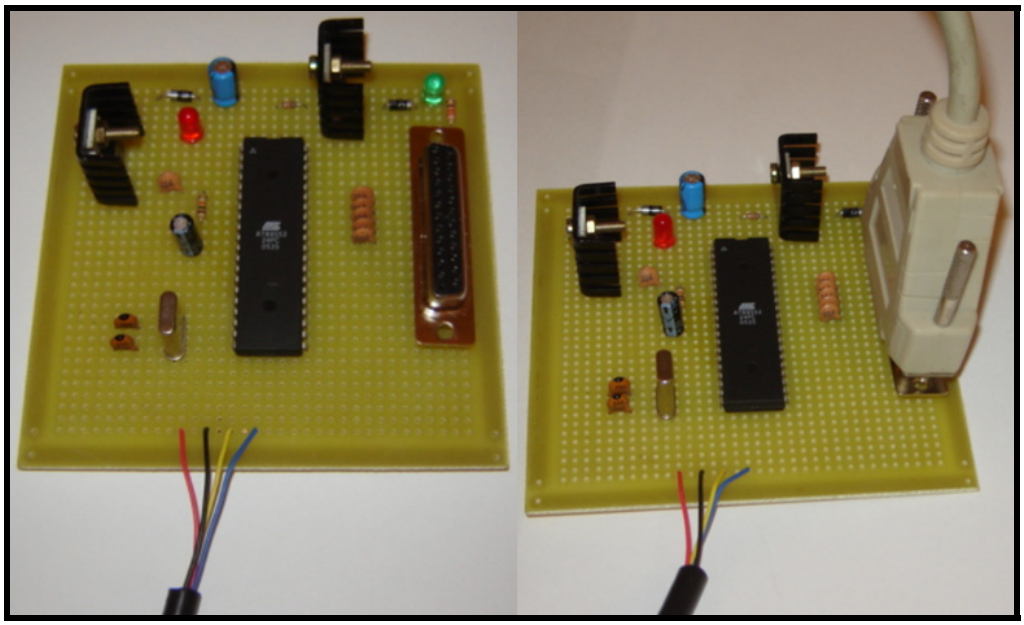


Figura 6.8 – Circuito de interface entre o servidor e a fechadura elétrica

A porta paralela do computador utiliza um conector padrão DB25, e o padrão de comunicação é conhecido como EPP (Enhanced Parallel Port), que pode atingir uma taxa de transferência de 2MB/s, através de um barramento de dados de 32 bits, ou ECP (Enhanced Capabilities Port), que tem as mesmas características que a EPP, no entanto utiliza o acesso direto à memória sem a necessidade do uso do processador para a transferência dos dados.

Os principais registradores vinculados à porta paralela do microcomputador são:

- ✓ Registrador de dados: é composto por oito bits, seu endereço físico pode ser 0378H ou 0278H (LPT1 ou LPT2) e sua principal característica na comunicação é de escrita no canal;
- ✓ Registrador de status: é composto por cinco bits, seu endereço físico pode ser 0379H ou 0279H (LPT1 ou LPT2) e sua principal característica na comunicação é de leitura no canal;
- ✓ Registrador de controle: é composto por quatro bits, seu endereço físico pode ser 037AH ou 027AH (LPT1 ou LPT2) e sua principal característica na comunicação é de escrita no canal.

A função deste circuito eletrônico é de receber através da porta paralela, comando específico para liberar a abertura da porta. Através do software, foi

definido que a abertura da porta se realiza quando da autenticação verdadeira da impressão digital do usuário.

Quando o *software* (específico do fabricante do dispositivo) autentica positivamente o usuário, a porta paralela do servidor envia *bits* lógicos de nível “1”, que correspondem à tensão de 5Vcc, no registrador de dados da porta paralela.

O microcontrolador utilizado neste circuito foi o AT89S52, fabricante ATMEL, da família 8051, e sua função é de receber os *bits* da porta paralela. O microcontrolador utilizado tem as seguintes características:

- ✓ Memória Flash com 8kB de capacidade, regravável até 1000 ciclos;
- ✓ Range de alimentação de 4 a 5,5Vcc;
- ✓ Memória RAM interna de 256X8*bits*;
- ✓ 32 pinos de interface I/O programáveis;
- ✓ Três timers/counters de 16 *bits;*
- ✓ Oito fonts de interrupção;
- ✓ Canal serial UART full duplex;

Quando os *bits* do registrador de dados estão em nível lógico zero, o microcontrolador não realiza nenhuma tarefa, mas quando os *bits* do registrador de dados estão em nível lógico “1”, o microcontrolador ativa um transistor bipolar de junção, que por sua vez entra em saturação, alimentando a bobina solenóide da fechadura por um segundo, sendo este tempo o suficiente para liberar a entrada do usuário.

Abaixo, tem-se o fluxograma de todo o funcionamento do sistema.

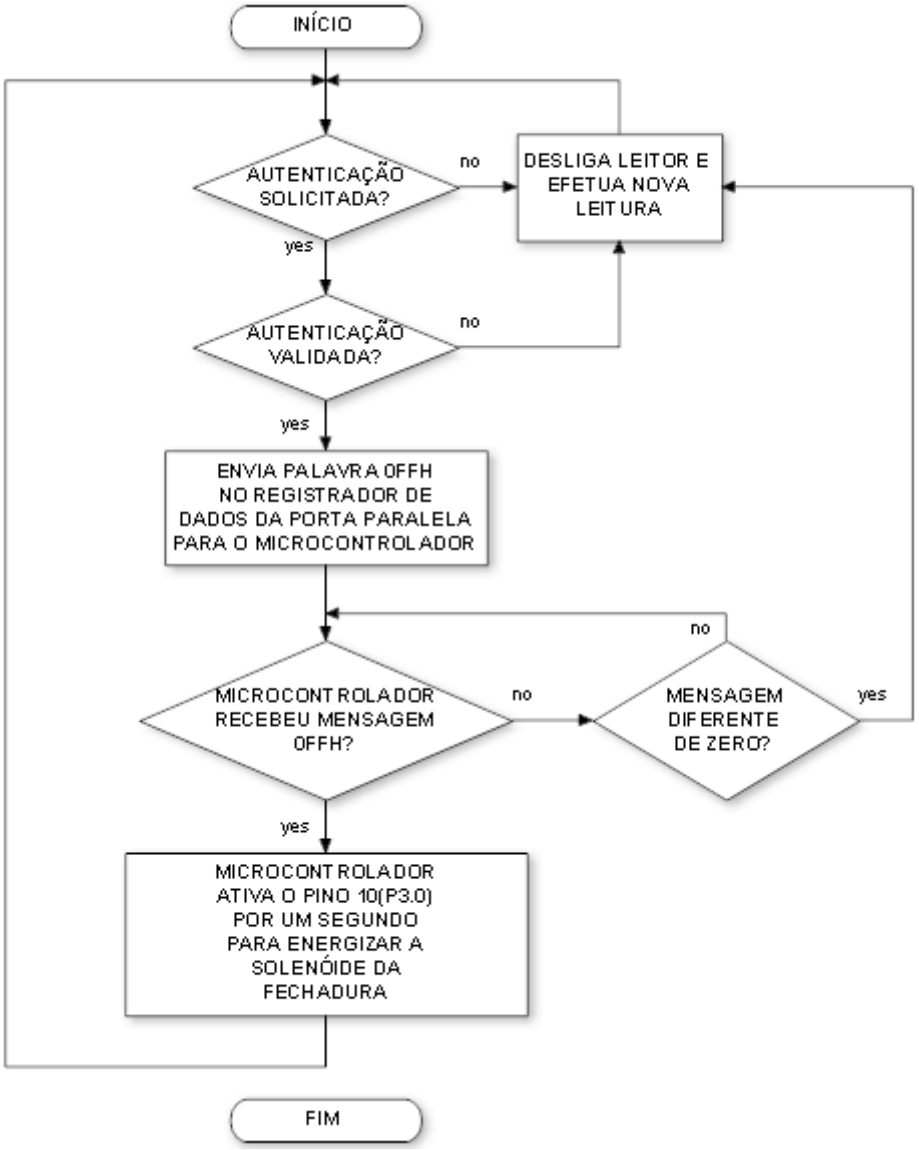


Figura 6.9 – Fluxograma do projeto

6.1.4 Fechadura elétrica

A fechadura elétrica utilizada para o controle de abertura da sala do servidor foi escolhida priorizando o custo das modificações na porta. Vários modelos estão disponíveis, e foi escolhido o modelo de fecho elétrico, pois com este modelo pode-se manter a fechadura original. Com esta implementação, ainda se tem a possibilidade de abertura da porta utilizando chave, pois a critério da direção da instituição, o sistema poderia entrar em falha impossibilitando assim o acesso.

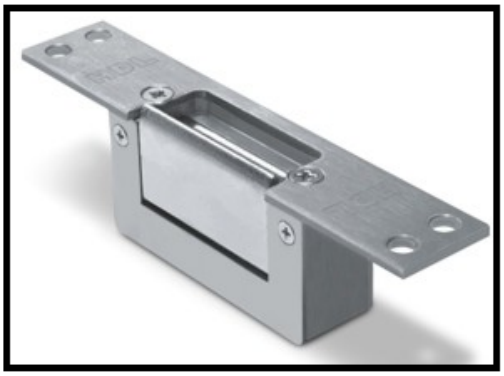


Figura 6.10 – Fecho elétrico para abertura da porta

Este fecho é eletromagnético, tendo em seu interior uma bobina do tipo solenóide, que ao ser energizada, cria um ímã temporário, destravando o mecanismo. Ainda possui uma memória mecânica interna, permitindo assim o destravamento da porta no primeiro impulso elétrico. Sua alimentação é de 12Vcc, e a potência é de 15W. O modelo necessita de uma fonte de energia externa, que forneça a alimentação citada anteriormente, e foi utilizada uma fonte do mesmo fabricante do fecho elétrico, por ter o menor preço, quando comprada em conjunto.

Figura 6.11 – Fonte de alimentação do fecho elétrico

6.2 Implantação do *software*

O *software* responsável pela identificação do usuário é proprietário, e o acesso ao seu algoritmo e os arquivos gerados pela captação da imagem da impressão digital não estão disponíveis. Para maiores informações sobre o equipamento e seu respectivo software, o fabricante disponibiliza o endereço http://www.digitalpersona.com.

O *software* de identificação biométrica valida campos de senha, de qualquer outro software OPC. Ao instalar o programa, o servidor ficou em estado de aguardo de senha. Ao ligar o servidor, após instalar o *software* biométrico, abriu-se a tela inicial, com os campos de *login* e senha, e automaticamente o *software* biométrico gerou a seguinte tela:

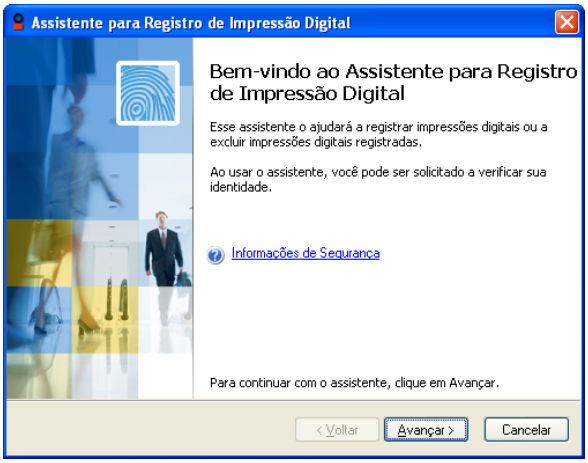
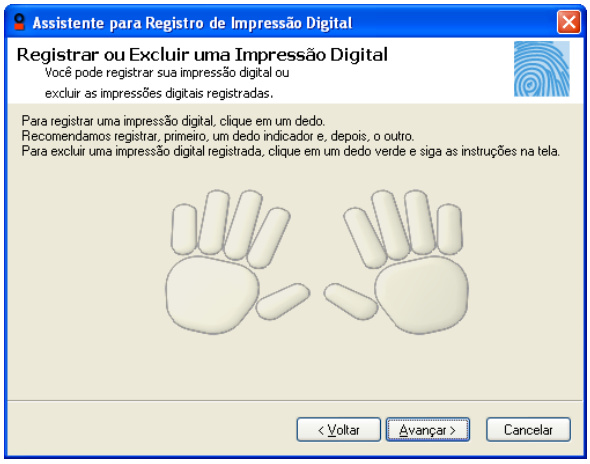


Figura 6.12 – Software para identificação biométrica

A seguir, vários passos foram seguidos, até a finalização de cadastro biométrico. Todas as telas foram salvas, durante o processo de cadastramento, e podem ser visualizadas abaixo:



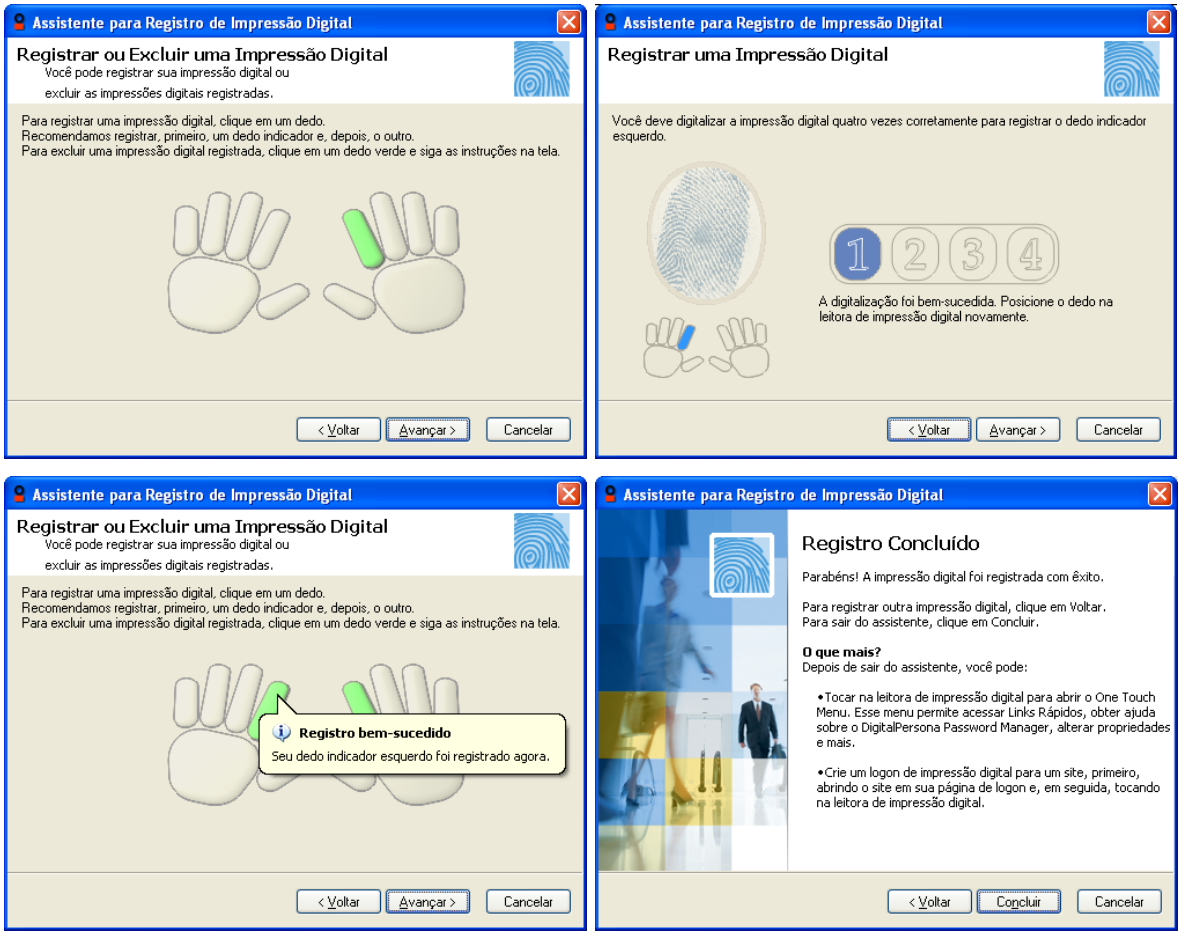


Figura 6.13 – Telas para cadastramento de impressão digital

Propositadamente, a posição do dedo foi invertida no momento do cadastramento, dificultando assim a leitura biométrica. O resultado no *software* foi o seguinte:

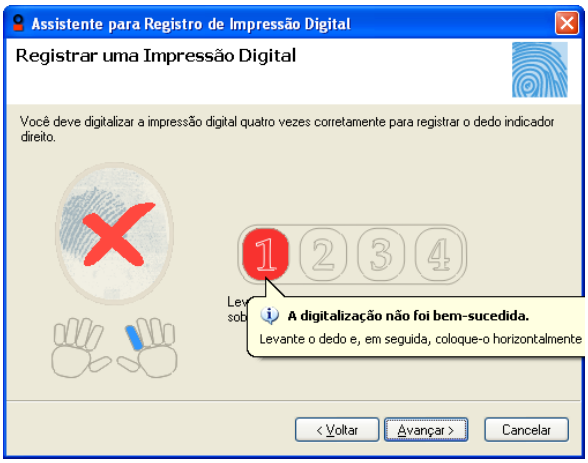


Figura 6.14 – Tela para falsa identificação biométrica

Após o cadastro, ao tocar o leitor, se a identificação for positiva, abre-se uma tela com as opções disponíveis:

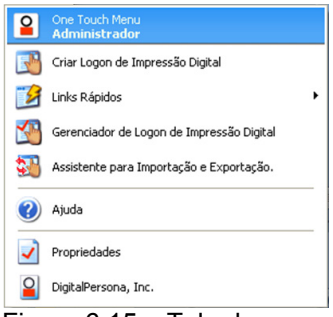


Figura 6.15 – Tela de menu

A partir desta etapa, a leitura biométrica foi cadastrada. O próximo passo foi desenvolver um *software* responsável por enviar a palavra 0FFH através da porta paralela, para que o circuito microcontrolado possa acionar a fechadura elétrica, e conseqüentemente, abrir a porta. Para isso, foi utilizado o *software* Borland C++ Builder Enterprise Suite versão 5.0. Com este *software*, uma tela inicial foi gerada, solicitando a senha do usuário. Como o *software* biométrico já estava instalado no servidor, ao abrir a tela inicial com pedido de senha, o cadastro da senha foi feito colocando-se o dedo indicador direito no leitor, e automaticamente o *software* desenvolvido liberou o pedido de senha. Neste momento, com a autenticação do usuário, um bloco de programação desenvolvido foi executado, enviando a palavra necessária para que o microcontrolador abra a porta.

Abaixo, pode-se visualizar a tela inicial gerada no servidor:

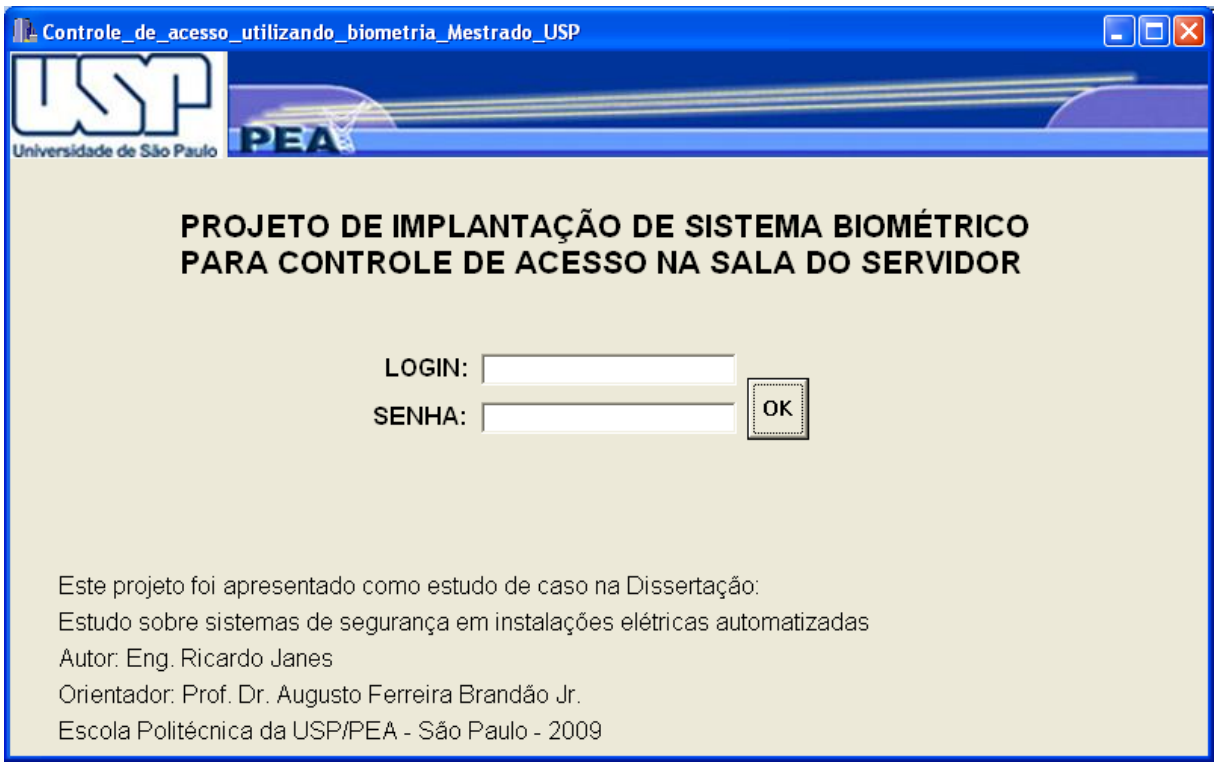


Figura 6.16 – Tela do *software* de controle de acesso

Como comentado anteriormente, ao aparecer esta tela no sistema, bastou-se colocar o dedo indicador no leitor, e a próxima tela cadastrou o acesso biométrico, substituindo os campos de login e senha. Esta tela de cadastro biométrico pode ser visualizada abaixo:

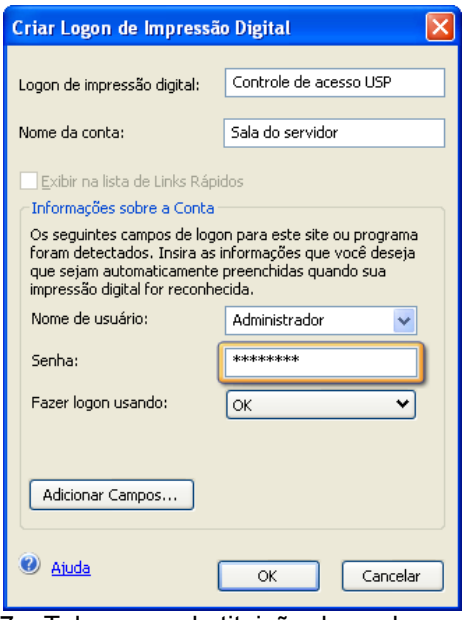


Figura 6.17 – Tela para substituição de senha por biometria

Com a autenticação do usuário, o *software* biométrico libera a tela de acesso, e neste momento é processado um programa no servidor, para que o envio da palavra 0FFH possa ser feito, utilizando a porta paralela. Abaixo, pode-se visualizar o bloco específico de programação desenvolvido:

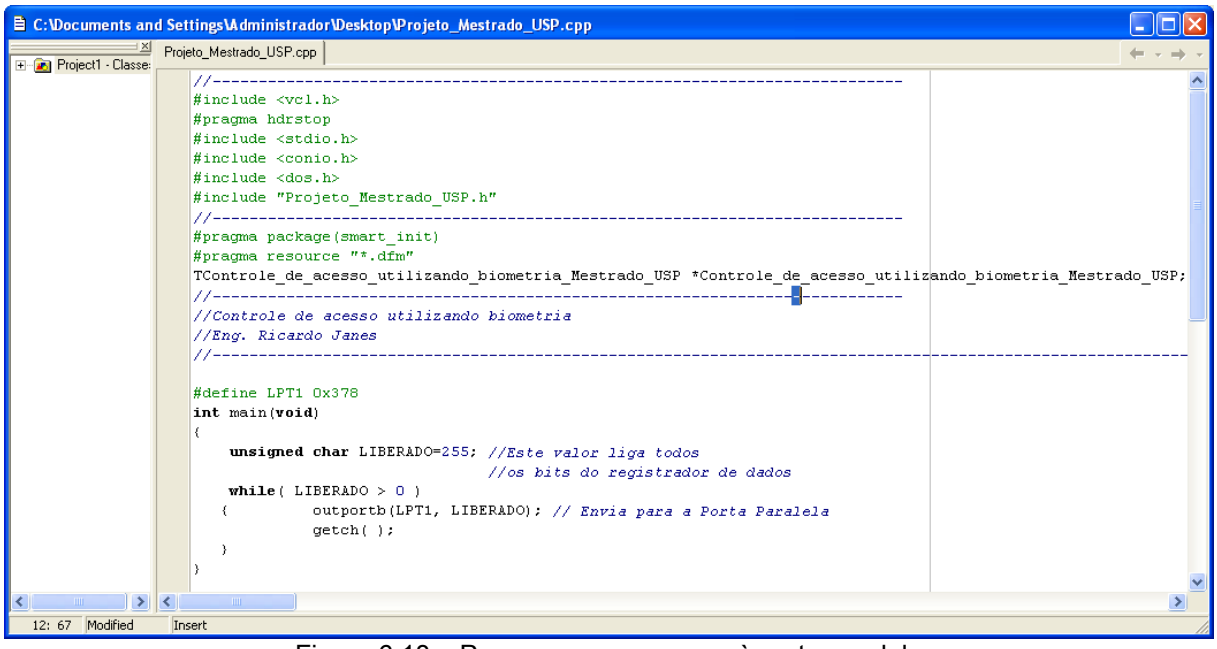


Figura 6.18 – Programa para acesso à porta paralela

7 CONCLUSÕES

Este trabalho apresentou uma inspeção prévia sobre as principais tecnologias biométricas utilizadas no controle de acesso em uma instalação automatizada. Os custos e o nível de segurança são as características principais que podem ser consideradas para fazer a escolha da melhor tecnologia a ser aplicada.

Em alguns casos, os perfis de usuário e o nível de segurança são os critérios mais importantes na escolha da tecnologia.

Durante o estudo, percebe-se claramente que a melhor tecnologia biométrica existente atualmente é a identificação da íris, no entanto, também é a que apresenta o maior custo para implementação.

Com os dados apresentados sobre as tecnologias biométricas neste texto, é possível realizar estratégias de controle multimodais, de acordo com a característica da instalação automatizada, criando novas tecnologias que podem ser adotadas para melhorar a exatidão e segurança de um sistema, baseando-se na precisão, custo, aplicabilidade ou disponibilidade.

O protótipo implementado neste trabalho gerou um custo aproximado de R$ 500,00, e se comparado às tecnologias estudadas, representa um custo muito baixo. Praticamente todas as tecnologias biométricas apresentam desvantagens que as fazem necessitar de aperfeiçoamento, ou em alguns casos, da aplicação de outra solução.

No processo de reconhecimento da retina, a principal dificuldade se encontra no fato de que a pessoa a ser identificada não pode estar usando óculos; no reconhecimento por face, um ferimento ou inchaço no rosto podem prejudicar o processo de identificação, gerando falsos negativos; no reconhecimento da geometria da mão, anéis podem causar falsos negativos; no reconhecimento por voz, ruídos externos, rouquidão e até mesmo a imitação da voz de outra pessoa pode causar problemas na identificação; no reconhecimento dinâmico de assinaturas, o estado emocional da pessoa e o passar do tempo podem modificar o padrão da escrita.

Pode-se afirmar que a utilização de biometria é uma tendência mundial, no entanto, nos últimos dois anos, os projetos que envolvem este tipo de tecnologia não foram

implantados. Apesar de ser uma tendência, existe atualmente uma questão polêmica levantada por diversos grupos de pesquisadores, sobre a segurança dos dados biométricos de cada indivíduo.

Alega-se que ao se implantar um sistema de segurança, como por exemplo, o uso de cartão com código de barras para controle de acesso, se o mesmo for copiado, basta anulá-lo e construir um novo cartão, com novo código.

Com a biometria, o grande risco de se perder uma informação no caso de uma invasão do sistema e conseqüente roubo das informações, é que a característica da pessoa não pode ser mudada, nem mesmo com cirurgia plástica, o que tornaria todo o sistema sem utilidade.

Praticamente todos os algoritmos utilizados em biometria se baseiam no estudo de imagem, que pode ser bidimensional ou tridimensional.

Os índices FRR e FAR de cada tecnologia não puderam ser identificados, pois necessitaria ter um modelo de cada equipamento para efetuar testes, uma vez que cada fabricante divulga um número diferente para estes índices, e estes números não são próximos uns dos outros.

Como visto no trabalho, a biometria na maioria dos casos é usada para se autenticar uma pessoa, e a identificação é realizada através de outras tecnologias, no entanto, a identificação da íris é uma tecnologia que identifica a pessoa, e em tempo extremamente rápido, devido ao seu algoritmo. Por estes motivos, se salientou acima neste mesmo texto, que esta é a melhor tecnologia biométrica até o momento.

A identificação por voz se mostra como sendo a mais vulnerável a fraudes, e mais susceptível a falsas identificações negativas. Os algoritmos apresentados em cada tecnologia são comercialmente difundidos, mas o detalhamento da geração dos arquivos digitais em cada algoritmo não é divulgado por nenhum fabricante, pois se trata de seu segredo industrial. Se houvesse divulgação destes detalhes, a tecnologia seria facilmente copiada, pois o *hardware* utilizado em geral é de simples implementação.

O estudo sobre os sistemas de detecção e combate de incêndios servem como base para futuros projetos sobre este tema, pois detalha os diversos equipamentos que podem ser utilizados, assim como o estudo sobre o controle interno da segurança e os sistemas de alarmes de intrusão e segurança patrimonial.

REFERÊNCIAS

ABESE, Associação Brasileira das Empresas de Sistemas Eletrônicos de Segurança. Disponível em <http://www.abese.com.br>. Acesso em: 23 mar. 2007.

ACHERMANN, B., JIANG, X., and BUNKE, H., **"Face recognition using range images"**, in Proc. of International Conference on Virtual Systems and MultiMedia (VSMM97), Geneva, Switzerland, Sep. 1997, pp. 129-136.

BLEUMER, G., **“Biometric Authentication and Multilateral Security”**, AT&T Labs-Research, 2000.

BOLZANI, Caio Augustus M. **Residências Inteligentes: um curso de domótica** – 1ª Ed. São Paulo: Editora Livraria da Física, 2004.

DAUGMAN, J. G., **“Biometric personal identification system based on iris analysis,”** U.S. Patent 5,291,560, Mar. 1, 1994. U.S. Pat. Off., Washington, DC.

DGV. Disponível em <http://www.dgv.com.br>. Acesso em 21 fev. 2007.

ECP. Disponível em <http://www.ecp.com.br>. Acesso em: 08 set. 2007.

EQUIPEX. Disponível em <http://www.equipex.com.br>. Acesso em: 23 mar. 2007.

EURO. Disponível em <http://www.eurox10.com.br>. Acesso em: 10 fev. 2007.

FAUNDES-ZANUY, E., **“State-of-the-art in Speaker Recognition,”** IEEE Aerospace and Electronic Systems Magazine, 20 (5) (2005) pp. 7-12.

GLOBO. Disponível em <http://g1.globo.com/Noticias/Tecnologia/0,,MUL56206-6174,00.html>. Acesso em 12 nov. 2008.

IBI, Intelligent Buildings Institute. **Intelligent Buildings Definition – guideline.** Intelligent Buildings Institute Foundation, 1st edition, Washington, USA, 1987.

INFO. Disponível em <http://info.abril.com.br/aberto/infonews/072005/11072005-8.shl>. Acesso em 12 dez. 2008.

JAIN, A. K., BOLLE, R., PANKANTI, S., **Biometrics: Personal Identification in Networked Society.** Norwell, MA: Kluwer, 1999.

JAIN, L.C., HALICI, U., HAYASHI, I., LEE, S.B., TSUTSUI, S.: **Intelligent Biometric Techniques in Fingerprint and Face Recognition**, CRC Press LLC, (1999).

LAMONDON, R., PARIZEAU, M., **"Signature verification from position, velocity and acceleration signals: A comparative Study,**" Proceedings of the 9th Int. Conf. on Pattern Recognition (ICPR'88), Vol. 1, 1988, Rome, Italy, pp. 260-265.

LIU, Simon and Silverman, Mark, " **A Practical Guide to Biometric Security Technology"**, IEEE IT Pro, vol. 1, pp 27-32,Jan-Feb. 2001.

MALTONI, D., MAIO, D., JAIN, A.K., PRABHAKAR, S., **"Handbook of Fingerprint Recognition",** Springer, 2003.

MARTE, Claudio Luiz. **Automação predial: a inteligência distribuída nas edificações.** São Paulo: Carthago & Forte, 1995.

NAPCO. Disponível em <http://www.napco.com.br>. Acesso em: 28 ago. 2007.

NBR 9441: Execução de sistemas de detecção e alarme de incêndio. Rio de Janeiro, 1998.

ORMAX. Disponível em <http://www.ormax.com.br>. Acesso em 16 out. 2007.

PERES, Marcelo Pereira. **Guia do CFTV – Treinamento Básico**, 2006. Disponível em <http://www.guiadocftv.com.br>. Acesso em 15 out. 2007.

REFORCE. Disponível em <http://www.reforcemonitoramento.com.br>. Acesso em 02 set. 2007.

RABINER, L.R., SCHAFER, R.W., **Digital Processing of Speech Signals,** Prentice-Hall, Englewood Cliffs, NJ, 1978.

REUTERS. Disponível em <http://www.reuters.com>. Acesso em 12 jan. 2009.

RIHA, Z., MATYAS, V., **"Biometric Authentication Systems",** FI MU Report series, 2000.

SANCHEZ-REILLO, R., GONZÁLES-MARCOS, A., **"Access Control System with Hand Geometry Verification and Smart Cards".** IEEE Aerospace and Eletronic Systems Magazine, Vol. 15, Nº. 2, Feb. 2000. pp. 4.

SECURITON. Disponível em <http://www.securiton.eu>. Acesso em 12 dez. 2007.

SERPRO. Disponível em <http://www.serpro.gov.br>. Acesso em 16 jan. 2007.

THOMAZINI, Daniel. ALBUQUERQUE, Pedro U. Braga De. **Sensores industriais: Fundamentos e aplicações. São Paulo. Érica. 2007.**

TSE. Disponível em <http://www.tse.gov.br/internet/index.html>. Acesso em 13 set. 2008.

TSS. Disponível em <http://www.tss.com.br>. Acesso em: 17 jan. 2007.

UNIFENAS. Disponível em <http://www.unifenas.br>. Acesso em 12 nov. 2008.

VARCHOL, P., LEVICKY, D. **Implementation of Gaussian mixture models for biometric security system.** In Proceedings Komunikacne a informacne technologie, Tatranske Zruby(Slovak Republic), 2007.

VICTOR, B., BOWYER, K., SARKAR, S., **"An Evaluation of Face and Ear Biometrics".** In: Proc. Of International Conference on Pattern Recognition. 2002, pp. 429–432.

WILDES, R., **"Iris Recognition: an emerging Biometric technology"** Proc. IEEE, Vol. 85, Sept.1997, pp 1348-1363.