UNIVERSIDADE ALTO VALE DO RIO DO PEIXE- UNIARP
CURSO DE ENGENHARIA DE CONTROLE E AUTOMAÇÃO

MARCELO HAHN AITA

CONTROLE DE ACESSO DE PESSOAS NO AMBIENTE DA UNIARP

CAÇADOR – SC
2011

MARCELO HAHN AITA

CONTROLE DE ACESSO DE PESSOAS NO AMBIENTE DA UNIARP

Trabalho de conclusão de curso apresentado como exigência para obtenção do título de Engenheiro de Controle e Automação, ministrado pela Universidade Alto Vale do Rio do Peixe – Uniarp, sob orientação do professor Edson Donizetti Dalla Santa.

CAÇADOR - SC

2011

CONTROLE DE ACESSO DE PESSOAS
NO AMBIENTE DA UNIARP

MARCELO HAHN AITA

Este Trabalho de Conclusão de Curso foi submetido ao processo de avaliação pela Banca Examinadora para a obtenção do Título de:

Engenheiro de Controle e Automação

E aprovada na sua versão final em __/__/____, atendendo às normas de legislação vigente da Universidade do Alto Vale do Rio do Peixe e Coordenação do Curso de Engenharia de Controle e Automação.

_____
Everaldo Cesar de Castro

BANCA EXAMINADORA

_____
Edson Donizetti Dalla Santa

_____
Herculano De Biasi

_____
Humberto Brezolin

AGRADECIMENTOS

Agradeço aos meus pais, Tarcila e Paulo, pela dedicação à minha formação durante todos esses anos.

A minha tia Ana, por me mostrar o quanto é importante cursar um ensino superior.

Ao meu tio Roberto, por me ajudar e mostrar na prática o que aprendi na teoria.

A minha esposa Miriane, por ter me apoiado e me motivado durante todos esses anos.

Ao meu orientador, Edson.

RESUMO

O presente trabalho tem o objetivo de aprofundar alguns conhecimentos sobre tecnologias mais comumente utilizadas em sistemas de controle de acesso e seleção da tecnologia com maior custo-benefício para a universidade. Será apresentado um projeto de uma catraca e seu custo e uma explicação do software que controlará esse sistema comparando com a aquisição de um produto pronto.

.

Palavras – chave: controle de acesso; catraca eletrônica; código de barras; *RFID*; biometria;

ABSTRACT

This paper aims to deepen knowledge about some technologies commonly used in access control systems and selection of technology more cost-effective way to university. This paper presents a project of a turnstile and its cost and an explanation of the software that will control this system compared to the purchase of a finished product.

Keywords: access control; electronic turnstile; barcode; *RFID*; biometrics;

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE SIGLAS

UPC – *Universal Product Code*, símbolo padrão de código de barras dos Estados Unidos e do Canadá, que é administrado pelo UCC (*Uniform Code Council, Inc*).

EAN – *European Article Number*, depois renomeado para *International Article Number* e posteriormente mudando a sigla para GS1.

ASCII – *American Standard Code for Information Interchange* é uma codificação de caracteres usado em computadores para representar símbolos, pontuação, letras e números.

CCD - *Charge Coupled Device* – Descarga por Acoplamento Capacitante.

RFID – *Radio Frequency Identification* – Identificação por Radiofrequência.

USB – *Universal Serial Bus*.

UNIARP – Universidade Alto Vale do Rio do Peixe.

GS1 – *Global Standards*, aqui no Brasil, Associação Brasileira de Automação.

SUMÁRIO

1 INTRODUÇÃO

Este trabalho fala sobre controle de acesso de pessoas no ambiente da UNIARP. O livre acesso de qualquer pessoa na Universidade pode prejudicar os acadêmicos, funcionários e professores, como vem ocorrendo em outras universidades e escolas do país, nos deixando preocupados com a total falta de segurança. A questão é como automatizar o controle de acesso de alunos, professores e funcionários da UNIARP?

Com a crescente violência no país e dentro das escolas e universidades deve-se dar importância para a segurança dos alunos e isto motivou a fazer este estudo de viabilidade para implantação de catracas de acesso na UNIARP.

O Objetivo geral deste trabalho é comparar as diversas tecnologias para controle de acesso que se adapte melhor às necessidades da UNIARP e fazer um levantamento do custo de implantação das catracas e do sistema.

Os objetivos específicos são:

Compreender mais sobre tecnologia de código de barras, biometria, *RFID* e reconhecimento facial.

Fazer um controle de acesso automatizado, registrando os acessos e criando dados estatísticos.

Comparar os custos de implementação baseando-se em três possibilidades: projetando e construindo hardware e software; adquirindo hardware e projetando software; e adquirindo hardware e software.

Este trabalho utilizará pesquisa bibliográfica para aprofundar sobre as tecnologias utilizadas em controle de acesso e pesquisa de campo para levantar dados sobre o ambiente em questão como os custos do projeto.

Este trabalho está organizado em 3 capítulos.

O Capítulo 1 trata do problema de pesquisa deste trabalho e quais os objetivos do mesmo.

No Capítulo 2, a primeira parte apresenta uma revisão bibliográfica sobre aspectos das tecnologias normalmente utilizadas em controle de acesso. A segunda parte apresenta todos os passos metodológicos empregados no desenvolvimento do Trabalho de Conclusão de Curso.

Seguido das conclusões no Capítulo 3 com a apresentação dos resultados obtidos com o estudo.

2 DESENVOLVIMENTO

2.1 REFERENCIAL TEÓRICO

Neste capítulo serão descritas as tecnologias usadas em controle de acesso com catracas eletrônicas que foram estudadas a fim de se ter um embasamento para o projeto deste trabalho. Na primeira parte será apresentada uma explanação sobre código de barras, na segunda, sobre biometria e na terceira, sobre RFID (*Radio Frequency Identification*).

2.1.1 Código de Barras

O código de barras foi criado para automatizar a entrada de dados em computadores substituindo operadores que precisavam digitar preços de um produto manualmente. Para um computador processar as informações e diferenciar um produto de outro surgiu a necessidade de criar um código único. Em 1973 começou a ser adotado o código UPC nas indústrias americanas e mais tarde em 1977 foi criada a EAN (*European Article Numbering Association*) que "se encarregou de estabelecer as diretrizes referentes à implantação do sistema de código de barras no mercado europeu" (GROSSMANN, ZYNGIER, 1991, p. 31). A EAN concluiu que o símbolo precisaria de treze dígitos para codificar todos os produtos existentes e para não gerar um trabalho manual ainda maior, a entrada automática de dados passou a ser utilizada.

Código de barras "é um símbolo composto de barras paralelas de larguras e espaçamentos variados" (GROSSMANN; ZYNGIER, 1991, p. 11). Essas barras pretas e brancas representam números e/ou letras. Existem vários padrões de código de barras, cada qual com aplicações específicas. Segue abaixo alguns exemplos.

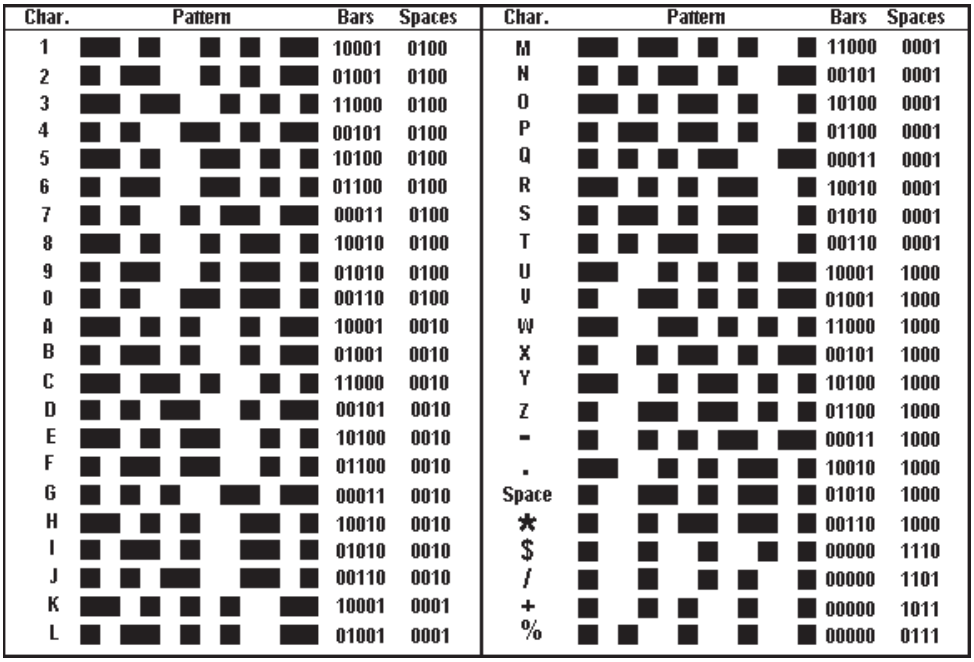
2.1.1.1 Código 39

Código 39 ou três de nove, foi a primeira simbologia de código de barras desenvolvida, é alfanumérico, de baixa qualidade, normalmente não tem dígito verificador e é simples de ser gerado. É usado em codificações internas de empresas, indústrias mecânicas, empresas aéreas, de saúde e em algumas aplicações comerciais.

Segundo Grossman e Zyngier (1991, p. 54):

> O código 39 é constituído por nove elementos, dos quais três são largos. Nesse caso, porém, cada caracter é representado por cinco barras e quatro espaços, sendo que tanto as barras quanto os espaços podem ser largos (no máximo de três).

O símbolo possui margens de silêncio antes e após o código e usa o asterisco como caractere de início e de fim.



Char.	Pattern	Bars	Spaces	Char.	Pattern	Bars	Spaces
1		10001	0100	M		11000	0001
2		01001	0100	N		00101	0001
3		11000	0100	O		10100	0001
4		00101	0100	P		01100	0001
5		10100	0100	Q		00011	0001
6		01100	0100	R		10010	0001
7		00011	0100	S		01010	0001
8		10010	0100	T		00110	0001
9		01010	0100	U		10001	1000
0		00110	0100	V		01001	1000
A		10001	0010	W		11000	1000
B		01001	0010	X		00101	1000
C		11000	0010	Y		10100	1000
D		00101	0010	Z		01100	1000
E		10100	0010	-		00011	1000
F		01100	0010	.		10010	1000
G		00011	0010	Space		01010	1000
H		10010	0010	*		00110	1000
I		01010	0010	$		00000	1110
J		00110	0010	/		00000	1101
K		10001	0001	+		00000	1011
L		01001	0001	%		00000	0111

Figura 1: Codificação de caracteres no código 39
Fonte: (ALLEN, 2011)

Figura 2: Exemplo de código 39
Fonte: (LINHABASE, 2011)

2.1.1.2 Código 2 de 5 entrelaçado

Código de alta densidade. Segundo Erdei (1994, p.77) “no símbolo, dois caracteres são agrupados juntos, utilizando barras para representar o primeiro caractere e espaços para o segundo”. Nesta simbologia cinco barras (ou espaços) definem um caractere e duas delas são largas. Somente podem ser codificados dados numéricos em quantidades pares, se for necessário deverá ser acrescentado um zero a esquerda da sequência numérica. Este código é usado em boletos bancários e faturas de consumo, possuindo tamanho variável e podendo conter um dígito verificador. O caractere de inicio é composto por duas barras estreitas e o de fim por uma barra larga e uma barra estreita.

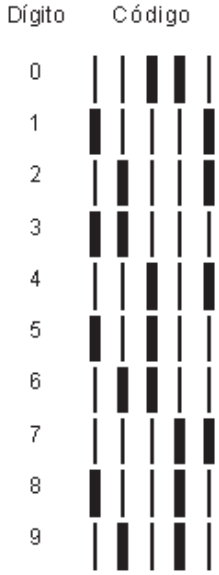


Figura 3: Codificação de caracteres no código 2 de 5 entrelaçado
Fonte: (PSITECNOLOGIA, 2011)

Figura 4: Exemplo de código 2 de 5 entrelaçado
Fonte: (LINHABASE, 2011)

2.1.1.3 Código 128

Este código permite utilizar todos os 128 caracteres ASCII, sua verificação pode ser através de um digito verificador ou por meio de paridades, é um código compacto e tem 3 classificações:

- 128 A: inclui letras maiúsculas, caracteres especiais e pontuação.
- 128 B: podem ser codificadas letras maiúsculas ou minúsculas.
- 128 C: código otimizado para utilização de números.

2.1.1.4 Código UPC

Código *Universal Product Code* - UPC é o formato padrão dos Estados Unidos e Canadá, utilizado para produtos de varejo, e tem duas versões, UPC-A com 12 dígitos, de uso geral e UPC-E com 8 dígitos que é mais restrito. Os dígitos do UPC-A são divididos em 4 partes a partir da esquerda:

- 1° dígito: categoria do produto (alimentos, medicamentos, cupons, etc...)
- 2° ao 6°: código do fabricante.
- 7° ao 11°: código do produto.
- 12°: dígito verificador.

E o código apresenta o separador esquerdo e direito, ambos com duas barras intercaladas por um espaço e o separador central com três barras intercaladas por dois espaços, esses apresentam as barras com uma altura maior do que as demais. “Cada caractere numérico é representado por 2 barras + 2 espaços, situados alternadamente, ou seja, 4 elementos para cada caractere. A largura e a localização

dos elementos é o que distingue um do outro" (ERDEI, 1994, p. 35). Cada caractere terá a largura de 7 módulos. Módulo é a menor tamanho possível de uma barra ou espaço, então cada barra ou espaço poderá ter o tamanho de um até quatro módulos.

A codificação de cada caractere pode ser denominada como A ou C dependendo da quantidade de módulos das duas barras, se for par ou ímpar, e do primeiro e do último módulo ser barra ou espaço. Os caracteres do tipo A estão situados no lado esquerdo do separador central, o primeiro módulo é um espaço, o último é uma barra e tem número ímpar de módulos (3 ou 5). Já os caracteres do tipo C estão situados no lado direito do separador central, o primeiro módulo é uma barra, o último é um espaço e tem número par de módulos (2 ou 4).

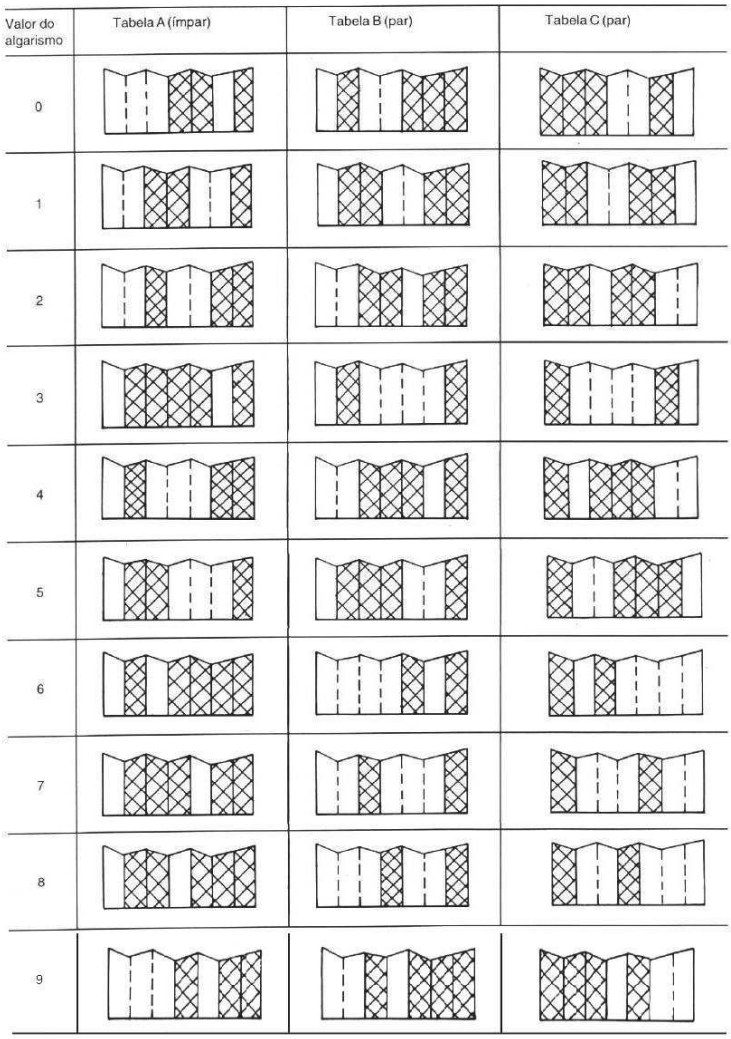


Figura 5: Codificação UPC/EAN
Fonte: (ABNT, 1987)

O código UPC usa as tabelas A e C que são oticamente inversas, ou seja, as barras na tabela A tornam-se espaços na tabela C e permite que o leitor possa ler o código nos dois sentidos. Os dígitos do lado esquerdo têm número ímpar de barras e número par de espaços, no lado direito é o contrário e com isso o software difere qual é o sentido da leitura.

Figura 6: Exemplo de código de barras UPC-A
Fonte: (BRAIN, 2011)

O dígito verificador é consistido de um cálculo sobre todos os outros dígitos do código de barras da maneira abaixo:

1. Soma-se os números das posições ímpares começando da esquerda e multiplica-se por 3;
2. Soma-se os números das posições pares;
3. Soma-se os números do item 1 e 2;
4. Divide-se o resultado obtido no item 3 por 10 e obteremos um quociente e um resto;
5. Subtrai-se o resto de 10 e obteremos o dígito de verificação.

Utilizando o código de barras da figura acima temos:

6+9+8+0+0+9=32

3+3+2+0+3=11

(32*3)+11=107

107/10=10 e sobra 7

10-7=3

O dígito de verificação é 3.

Após o cálculo do dígito verificador é feito um novo cálculo considerando o dígito verificador. Se o resto da divisão for zero, fica confirmado o valor do dígito.

6+9+8+0+0+9=32

3+3+2+0+3+3=14

(32*3)+14=110

110/10=10 e sobra 0

Então o dígito está correto.

O código UPC-E é gerado a partir de alguns códigos UPC-A reduzindo de 12 para oito números no símbolo. Esta redução é feita suprimindo 4 zeros do código. Desprezando o dígito da categoria do produto e o dígito de verificação, os outros 10 números são reduzidos para seis de acordo com a seguinte tabela:

Tabela 1: Tabela usada para transformar um código UPC-A para UPC-E

Empresa	Produto	UPC-E
ab000	0000xyz	abxyz0
ab100	0000xyz	abxyz1
ab200	0000xyz	abxyz2
abc00	00000yz	abcyz3 (c de 3 a 9)
abcd0	000000z	abcdz4
abcde	000000z	abcdez (z de 5 a 9)

Fonte: (DQSOFT, 2011).

Quando o número correspondente ao código do fabricante termina com 000, 100, 200 como nas três primeiras linhas da tabela, o fabricante pode ter até 1000 produtos. No caso da quarta linha, quando o código da empresa tem o terceiro dígito de 3 a 9 e termina em 00, poderão ser codificados 100 produtos. Quando o número do fabricante terminar com 0, a empresa pode ter até 10 produtos e quando não terminar em zero, o fabricante só poderá ter 5 produtos.

Os quatro primeiros caracteres do código UPC-E são codificados pela tabela A e os outros quatro são codificados pela tabela B da figura 5, este código não possui separador central e o separador direito é modificado para 010101 onde 0 representa o espaço e 1 representa a barra. O UPC-E é usado em produtos onde não tem espaço para imprimir um código UPC-A.

O Código UPC é compatível com o EAN pois usam a mesma codificação e para transformar um UPC-A (12 dígitos) em EAN-13 (13 dígitos) é só acrescentar um zero na frente do código.

2.1.1.5 EAN - *European Article Number*

É um código usado comercialmente no mundo inteiro exceto nos Estados Unidos e Canadá. Tem duas versões, o EAN-13 de uso geral e o EAN-8, restrito a produtos que não tenham espaço para o EAN-13. O EAN-13 é dividido em 4 partes:

- 1° ao 3° dígito: código do país.
- 4° ao 7° ou 4° ao 8°: código do fabricante.
- 8° ao 12° ou 9° ao 12°: código do produto.
- 13°: dígito verificador.

Como esse código é usado internacionalmente, o código do país é determinado pela EAN. O código do Brasil é 789. O código do fabricante pode ter 4 ou 5 dígitos conforme a quantidade de produtos. Com 4 dígitos, uma empresa pode ter 100000 produtos diferentes, com 5 dígitos pode ter 10000 produtos. O dígito verificador é calculado da mesma maneira que no código UPC, porém considerando o primeiro dígito.

O código EAN utiliza os mesmos separadores e as mesmas tabelas de codificação do UPC, mas com a diferença de codificar os caracteres a esquerda do separador central com as tabelas A e B, enquanto o UPC utiliza apenas a A. A codificação dos caracteres a esquerda é definida por outra tabela que utiliza o primeiro dígito do código do país e este dígito não estará representado por barras ou espaços e é impresso à esquerda do caractere de início.

Tabela 2: Tabela de sequência de caracteres

1° Dígito	2° Dígito	3° Dígito	4° Dígito	5° Dígito	6° Dígito	7° Dígito
0	A	A	A	A	A	A
1	A	A	B	A	B	B
2	A	A	B	B	A	B
3	A	A	B	B	B	A
4	A	B	A	A	B	B
5	A	B	B	A	A	B
6	A	B	B	B	A	A
7	A	B	A	B	A	B
8	A	B	A	B	B	A
9	A	B	B	A	B	A

Fonte: (GROSSMANN; ZYNGIER, 1991)

Analisando a tabela podemos ver que o código UPC, que tem o primeiro caractere 0, utiliza todos os caracteres codificados na tabela A, já o Brasil, que tem o primeiro caractere 7, utiliza na ordem ABABAB para codificar os caracteres antes do separador central.

Figura 7: Exemplo de código de barras EAN-13
Fonte: (LINHABASE, 2011)

Assim como o UPC-E, o EAN-8 é usado em produtos pequenos que não suportam o EAN-13, mas a diferença é que no UPC-E, o número do fabricante e do

produto é reduzido e no EAN-8 é um código designado pelo órgão responsável pelo sistema de numeração que indica o produto e o fabricante, cada país filiado à GS1 tem um número limitado de códigos para EAN-8 por isso o seu uso é muito restrito.

O EAN-8 possui 8 dígitos, dividido em três partes:

- 1° ao 3° dígito: código do país.
- 4° ao 7°: código do produto e fabricante.
- 8°: dígito verificador.

O EAN-8 possui os mesmos separadores do EAN-13 e o cálculo do dígito é igual, apenas considerando 5 zeros à esquerda. Os dígitos a esquerda do separador central são codificados pela tabela A e os dígitos da direita pela tabela C.

Figura 8: Exemplo de código de barras EAN-8
Fonte: (LINHABASE, 2011)

2.1.1.6 Leitura do código de barras

A leitura do código de barras é feita de forma ótica por dispositivos chamados *scanners*. Os *scanners* emitem e recebem um feixe de luz que percorre horizontalmente o código no qual a luz é absorvida nas barras escuras e refletidas nos espaços. O scanner transforma a reflexão em um sinal elétrico analógico e depois em um sinal digital que é interpretado por uma tabela de simbologia do código programado.

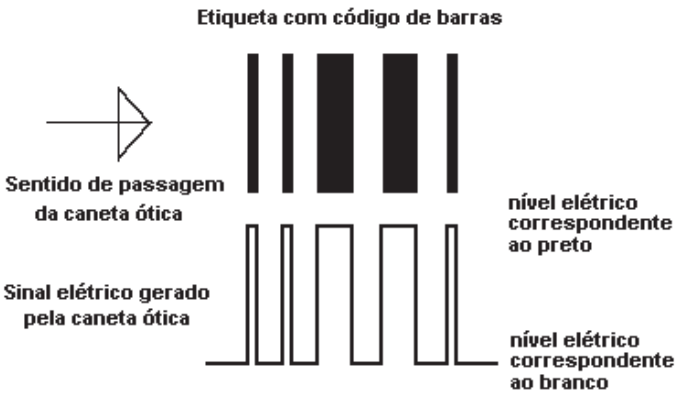


Figura 9: Leitura de código de barras
Fonte: (PSITECNOLOGIA, 2011)

Alguns tipos de scanner são:

Caneta ótica: a leitura é feita encostando a ponta da caneta e movendo-a sobre o código de barra. É barata e pouco confiável pois depende da velocidade constante para uma boa leitura. Segundo Grossmann e Zyngier (1991, p. 102) “a caneta fica ligada a um decodificador que terá a função de contabilizar o tempo que se fica em cima de cada barra ou espaço e, assim, decodificar o código”.

- Leitor laser: um diodo laser é usado como fonte de luz. Um espelho oscilante faz com que o feixe de luz se movimente. Normalmente visto em duas formas:
  - Pistola: o operador aponta o feixe de luz para o código de barra.
  - Leitor fixo: comum em supermercados, onde o operador movimenta o código na frente do feixe de luz. Normalmente se usa um dispositivo omnidirecional que pode ler o código de barra em qualquer orientação, para isso se usa mais de um diodo laser e mais de um espelho. Tem alta capacidade de processamento.

- Slot scanner: tem custo baixo, usado com cartões de identificação em controle de acesso, pode utilizar luz vermelha visível ou infravermelha.
- Leitor CCD: tem boa qualidade e baixo custo, a luz refletida é transformada em um sinal elétrico e depois convertida em bits através de um conversor analógico-digital.

2.1.2 Biometria

A palavra biometria vem do grego bio = vida e metron = medida e é o uso de características biológicas e comportamentais do ser humano para identificar um indivíduo específico (PINHEIRO,2008). A biometria é usada na identificação criminal, controle de acesso em ambientes restritos ou sistemas e redes de computadores, controle de ponto, proteger informações, entre outras aplicações. É dividido em características físicas e comportamentais.

2.1.2.1 Características físicas

2.1.2.1.1 Impressão digital

É o desenho formado pelas elevações da pele na polpa dos dedos das mãos, essas elevações possuem terminações e bifurcações que são únicas em cada indivíduo. É a característica biométrica mais estudada e utilizada para identificação e é exclusiva de cada indivíduo (PINHEIRO, 2008). Existem dois tipos básicos de tecnologia para identificação por impressão digital: a ótica, que usa um CCD, que contém um grupo de diodos fotossensíveis e cada diodo grava um pixel da imagem. Um conversor analógico-digital é usado para converter o sinal elétrico dos diodos em uma imagem digital. O CCD ainda verifica se obteve uma imagem nítida da impressão digital através da penumbra média dos pixels. Outro tipo é a leitura capacitiva que utiliza uma corrente elétrica para formar a imagem da impressão digital, este sensor utiliza várias células com duas placas condutoras envoltas por um material isolante menores do que os sulcos dos dedos. Quando um sulco do dedo está em cima dessa célula, a capacitância desse sensor é maior do que se tivesse um vale da impressão digital e por consequência, a saída de tensão também é maior. Através da saída de tensão o processador do leitor diferencia se é um vale ou um sulco e forma a imagem da impressão digital. A impressão digital tem algumas características específicas que são bifurcações e terminações dos sulcos, essas características são chamadas minúcias e através delas o software do leitor compara a imagem capturada com as digitais anteriormente armazenadas no banco

de dados. O software dos leitores biométricos pode reconhecer mais de 40 minúcias da digital.

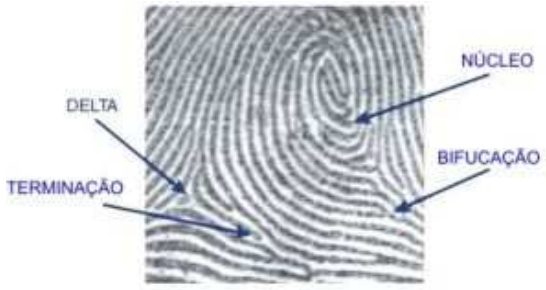


Figura 10: Minúcias de uma impressão digital
Fonte: (ACESSOEPONTO, 2011)

Após extrair a imagem do sensor, o algoritmo de análise de impressão digital aplica um filtro de Gabor para retirar os ruídos e realçar a imagem, depois reduz a largura das linhas para um *pixel*. A partir dessas linhas, o algoritmo utiliza um filtro de detecção de bordas para encontrar as terminações e bifurcações da impressão. É um sistema relativamente confiável, rápido e barato e o único problema da verificação é o dedo apresentar algum corte ou calo ou estiver muito seco ou úmido.

Figura 11: Imagem extraída de um leitor de impressão digital
Fonte: (FARIA, 2011).

Figura 12: Imagem após o filtro de Gabor
Fonte: (FARIA, 2011).

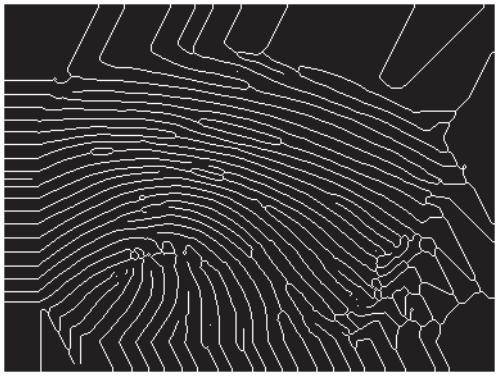


Figura 13: Imagem binarizada
Fonte: (FARIA, 2011).

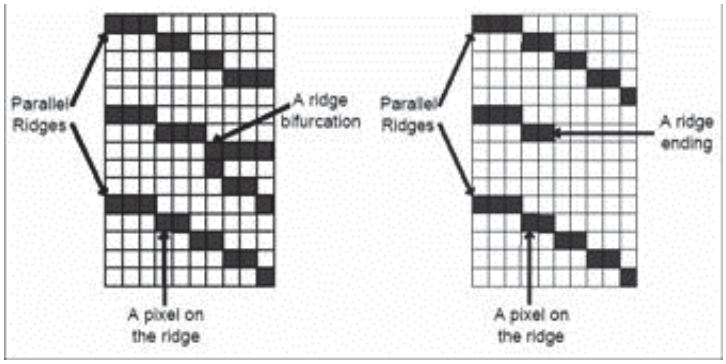


Figura 14: Funcionamento do filtro de detecção de bordas.
Fonte: (FARIA, 2011).

Para encontrar uma minúcia, o filtro de detecção de bordas faz uma varredura por todos os *pixels* da imagem e marca os que contêm 1, 3 ou 4 *pixels* vizinhos, se for 1, é uma terminação, se for 3 é uma bifurcação e 4 um cruzamento. O algoritmo

ainda marca a direção que a minúcia se propaga. Esse mapa de minúcias será comparado ao *template* cadastrado no banco de dados.

2.1.2.1.2 Reconhecimento facial

A tecnologia de reconhecimento facial baseia-se em características do rosto que são imutáveis mesmo após a pessoa ter passado por alguma cirurgia (PINHEIRO, 2008), e são usados pontos como linha da mandíbula, comprimento do nariz, distância entre os olhos, entre outros, conhecidos como pontos nodais. O leitor captura a imagem do rosto da pessoa e compara os pontos nodais já cadastrados anteriormente. É um método pouco invasivo para recolher a amostra, porém tem um custo de implantação alto e ainda é pouco confiável.

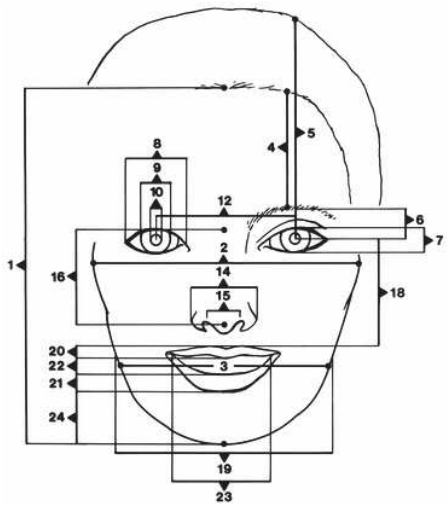


Figura 15: Pontos Nodais
Fonte: (ARAGÃO, 2011)

2.1.2.1.3 Identificação pela íris

A íris é a parte colorida do olho e não se altera com o passar do tempo. Nela podemos encontrar 249 pontos de diferenciação (PINHEIRO, 2008) e pode ser lida mesmo que a pessoa esteja usando lentes ou óculos. Neste processo é usado um *scanner* CCD para tirar uma foto da íris, depois o leitor separa a imagem da íris e compara com o modelo previamente cadastrado. É um método muito seguro porque a íris é única para cada indivíduo.

2.1.2.1.4 Reconhecimento pela retina

O reconhecimento pela retina é feito de forma parecida com o método de reconhecimento pela íris. A retina é formada por vasos sanguíneos que criam um desenho único. Segundo Pinheiro (2008, p. 71), “pesquisas tem comprovado que o padrão de veias da retina é a característica com maior garantia de singularidade que um indivíduo pode apresentar”. A leitura é feita através de uma câmera e o algoritmo reconhece e identifica o padrão da retina com o modelo cadastrado previamente. É um dos métodos mais seguros, porém tem alto custo de implantação e a leitura é difícil e incômoda, pois o usuário tem que olhar fixamente para um ponto até que a câmera capture a imagem (PINHEIRO, 2008).

2.1.2.1.5 Geometria da mão

Neste método é usado um *scanner* que captura uma imagem tridimensional das medidas da mão, da palma das mãos e dos dedos (PINHEIRO, 2008). A partir destes dados o sistema calcula as proporções das medidas e calcula as áreas. Este método também considera as linhas e detalhes da palma da mão. É um método com boa aceitação, simples e com baixo custo, mas tem alguns problemas como a utilização de anéis e se a pessoa ganhar peso ou sofrer algum acidente que deixe a mão deformada. É pouco confiável, pois a mão não tem características suficientes para que a pessoa possa ser identificada só por este método.

2.1.2.2 Características comportamentais

2.1.2.2.1 Assinatura

Na análise da assinatura, a forma como a pessoa assina o nome é mais importante do que a assinatura. No momento da assinatura são verificadas algumas características como velocidade, tempo que se leva para assinar, ângulo e pressão da caneta. A taxa de acerto é bem alta, pois é difícil imitar os traços da assinatura do verdadeiro dono. É bem aceita pelos usuários pelo hábito de usar a assinatura para autenticação e o arquivo gerado é pequeno. Porém tem algumas desvantagens

como modificação da assinatura com o passar do tempo ou alteração emocional, grande quantidade de amostras no cadastro e pouca aceitação em países com índice de analfabetismo alto.

2.1.2.2.2 Reconhecimento de voz

Este tipo de verificação “é uma tecnologia que analisa os padrões harmônicos e não apenas reproduções de sequências predefinidas de voz” (PINHEIRO, 2008, p.72). Nessa verificação, um microfone captura a voz e a processa digitalmente utilizando um algoritmo que separa o áudio em fonemas (PINHEIRO, 2008). No momento da verificação, o software pede ao usuário para pronunciar algumas palavras ou uma frase, separa em fonemas e verifica a probabilidade de cada fonema estar correto, liberando ou não o acesso. A utilização deste método é natural e simples devido ao fato do ser humano usar a fala para se comunicar com o mundo exterior, por isso é uma vantagem do seu uso (PINHEIRO, 2008).

2.1.3 *Radio Frequency Identification* – RFID

A identificação por meio de radio freqüência é uma tecnologia existente há mais de 80 anos, que nasceu como tantas outras tecnologias, com fins militares. Tem ganhado cada dia maior atenção por parte de grandes investidores e empresas de tecnologia e já pode ser sentida em vários ramos do cotidiano, como automóveis que podem ter acionada a ignição com ausência de chaves, portas e fechaduras que podem ser abertas à distância.

Não podemos classificar o RFID como uma tecnologia nova, pois teve sua primeira patente já há mais de 30 anos. Sua grande proposta é facilitar a vida das pessoas ou de distintas formas, da segurança delas e de seus bens.

Basicamente é uma tecnologia de comunicação que se vale de ondas de rádio para transmitir dados de uma fonte móvel para um leitor fixo. As etiquetas RFID, ou *tags* são componentes de hardware que possuem uma antena e um chip envoltos por algum material, que respondem a sinais remotos vindos de um leitor conectado a um computador (SANTINI,2008). Portanto, um sistema RFID é composto por pelo menos dois componentes: as *tags* e os leitores (SANTINI,2008).

A *tag* é um *transponder*, sua função é “transmitir e responder comandos que chegam por radiofreqüência” (SANTINI, 2008, p. 7). *Transponder* é uma junção das palavras em inglês *TRANSmitter*/*resPONDER*. Uma *tag* pode ter vários formatos como, cartões, chaveiros e etiquetas. Elas podem ser passivas, ativas ou via dupla.

2.1.3.1 *Tags* passivas

São as mais usadas por serem baratas e simples, não possuem transmissor, apenas refletem o sinal emitido pelo leitor. Têm uma vida útil maior porque normalmente não possuem baterias, usando a energia transmitida pelo leitor (SANTINI, 2008).

2.1.3.2 *Tags* ativas

Essas *tags* têm um transmissor interno e possuem baterias, mesmo que o leitor faça a comunicação, a *tag* é capaz de emitir o próprio sinal (SANTINI, 2008). São mais caras que as *tags* passivas.

2.1.3.3 *Tags* de via dupla

Elas sempre são ativas e sempre terão baterias para seu próprio uso. A diferença para as *tags* ativas é que elas não precisam ser ativadas por um leitor e podem comunicar-se entre si (SANTINI, 2008).

2.1.3.4 Alguns componentes de um sistema RFID

Além das *tags*, existem outros componentes que fazem parte de um sistema RFID, tais como a antena, que serve para propagar o sinal, o leitor, que faz a comunicação entre a *tag* e o software, a impressora RFID, que pode “imprimir diretamente em uma *tag* que será anexada a alguma item” (PINHEIRO, 2008, p. 9) e

o controlador. Este último tem a função de controlar o leitor, tratar as informações vindas da antena e fazer a integração do sistema RFID com o sistema do cliente.

2.2 CONCEITO

Devido à venda de drogas dentro de algumas universidades, inclusive na UNIARP, ficamos preocupados com o nosso ambiente acadêmico pois podemos ser vítimas de casos como esses. Com isto em mente, foi pensado em controlar o acesso na universidade para evitar a venda de substâncias ilícitas usando catracas eletrônicas.

A utilização de qualquer tecnologia biométrica sinaliza a busca pela segurança, seja no acesso físico, reconhecimento ou acesso a dados. Estes sistemas, que já são realidade, estão presentes em universidades, escolas, departamentos governamentais, e a cada dia crescem mais. Podem ser notados em ônibus, metrô, caixas eletrônicos e empresas privadas.

Ficou claro através deste estudo que os melhores sistemas biométricos como reconhecimento da íris são também os com maiores custos de implantação e manutenção. Por outro lado, sistemas que apresentam os menores custos apresentam proporcionalmente o menor índice de segurança, não resolvendo a questão inicial que é a segurança no acesso ao ambiente (estudante da universidade).

Registre-se que o melhor custo/benefício encontra-se em sensores biométricos com análise da digital. Sistemas baratos e eficientes podem ser encontrados a venda inclusive no mercado brasileiro. Sensores e equipamentos para armazenamento das leituras e banco de dados podem ser encontrados a custos relativamente baixos, podendo-se mesmo utilizar o banco de dados já existente na universidade para o armazenamento de mais um dado, nesse caso digitais associadas ao número de inscrição ou matrícula do aluno.

2.2.1 Comparação das tecnologias

Para obter um resultado que seja vantajoso e de baixo custo precisamos comparar as tecnologias e verificar qual se adapta melhor às necessidades da universidade. Tem-se que encontrar uma solução que seja segura e eficiente e ao mesmo tempo barata.

O código de barras é mais barato para implantar do que as outras tecnologias além de poder utilizar as carteirinhas dos estudantes já existentes, tem vida útil curta

mas nesse caso não deverá ser levada em consideração pois a carteirinha durará até o final do curso. Entre as desvantagens podem ser consideradas a possibilidade de fraude, tirando uma cópia do código de barras e enganando o leitor, comprometendo a segurança.

Já no caso da biometria, é mais difícil de fraudar, pois são características únicas e ainda tem-se a certeza de que a pessoa que está acessando é a própria e não alguém que tenha pego o cartão emprestado ou roubado. Reconhecimento facial ainda tem uma taxa de acerto muito pequena e o custo de implantação alto. Reconhecimento de íris e de retina também tem alto custo de implementação e são mais incômodos e intrusivos no momento da autenticação, porém bem mais seguros e confiáveis. Geometria das mãos é barato, mas pouco confiável. Impressão digital é confiável e barato.

As *tags* RFID não necessitam de contato para serem lidas, podem ser confeccionadas em diversos formatos, como chaveiros ou cartões, elas tem alta capacidade de armazenamento de dados, podendo guardar outras informações além do número da matrícula e tem alta segurança, mas o custo é muito elevado.

2.2.2 Solução encontrada entre as tecnologias

Devido ao alto custo de implantação de algumas tecnologias mais seguras e a pouca confiabilidade de tecnologias mais baratas serão usadas duas tecnologias conjuntas, de código de barras e impressão digital.

Serão utilizadas as carteirinhas de estudantes com código de barras para identificar o estudante dentro do banco de dados da universidade e a impressão digital para verificar se o aluno é quem diz ser.

2.2.3 Usuários

Os usuários serão os estudantes da universidade e do colégio de aplicação, funcionários e professores. Eles deverão ter as suas digitais cadastradas no sistema para ter acesso à UNIARP. Será feito um controle manual ou com crachá de visitante para as outras pessoas.

2.2.4 Desenvolvimento da catraca

A catraca foi desenhada no software *SolidWorks*. Ela conterá espaços para colocar um leitor de cartão com código de barras e um leitor biométrico além de um painel com informações. Esses leitores podem ser adquiridos por menos de cem reais cada e a conexão é feita via USB – *Universal Serial Bus*. Com um *hub* USB dentro da catraca para interligar os leitores e o painel, haverá somente um cabo que sairá para o computador que controla os acessos. O *hub* tem um custo na faixa de trinta reais.

2.2.5 Banco de dados

Para poder armazenar as impressões digitais dos usuários bem como os registros de entrada e saída dos mesmos, sugere-se a criação de duas tabelas no banco de dados da universidade, a de Digital para armazenar as impressões digitais e a tabela Histórico, para registrar o horário de entrada e saída do ambiente.

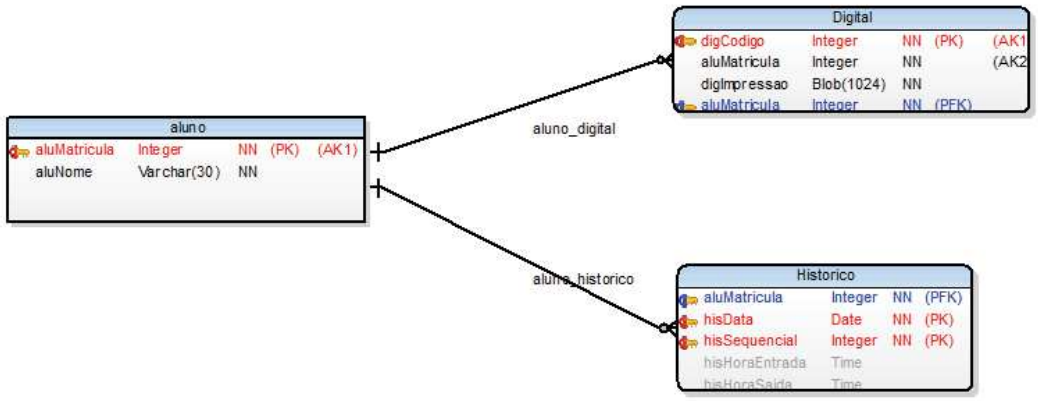


Figura 16: Tabelas adicionadas no banco de dados
Fonte: (AITA, 2011)

No diagrama Entidade-Relacionamento da Figura 15, a tabela Aluno foi criada só com os campos de matrícula e nome para demonstração do sistema.

2.2.6 Desenvolvimento do software

O software foi desenvolvido em linguagem *Delphi* e o banco de dados em *Interbase*. Como não se obteve acesso aos dispositivos de leitura biométrica e de código de barras, essas entradas no sistema foram simuladas manualmente.

O software fará o cadastro das digitais, o controle de acesso e criará gráficos com dados estatísticos das entradas e saídas dos usuários.

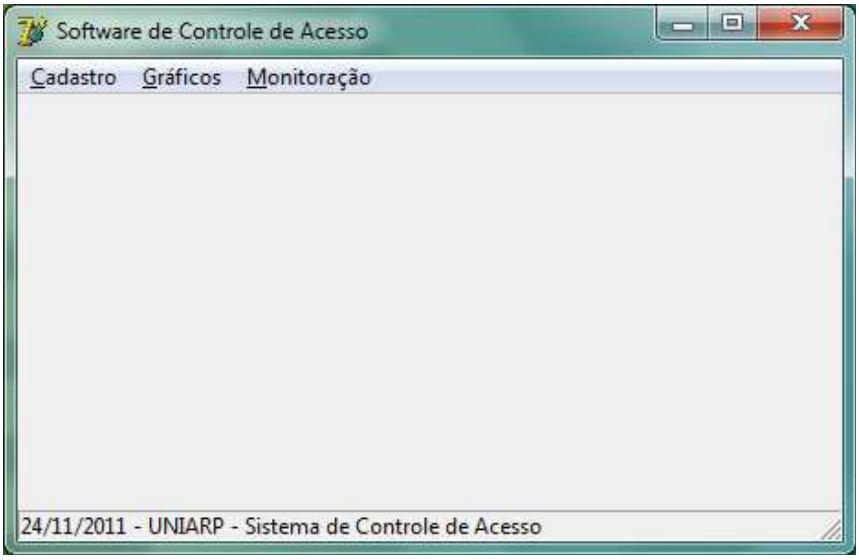


Figura 17: Tela principal do software
Fonte: (AITA, 2011)

A tela representada pela figura 15 apresenta os menus de acesso para as outras telas.

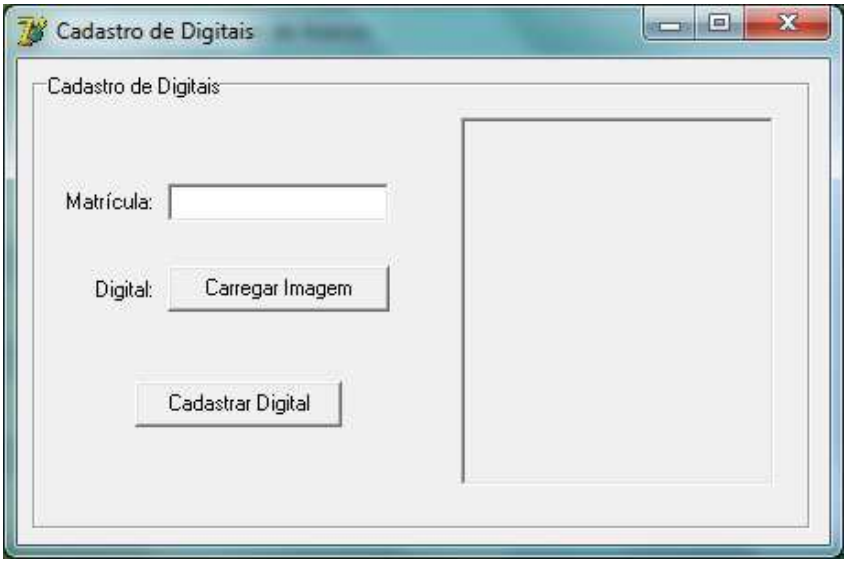


Figura 18: Tela de cadastro de digitais
Fonte: (AITA, 2011)

Na tela de cadastro serão cadastradas as impressões digitais dos usuários. O campo matrícula será preenchido depois que o usuário passar a carteirinha de estudante ou crachá de funcionários, no próximo momento serão cadastradas as impressões digitais de cada dedo.

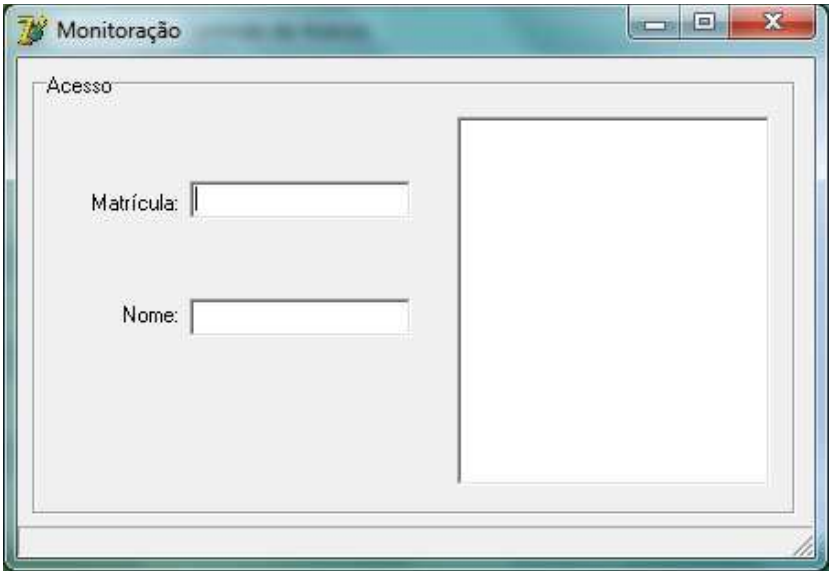


Figura 19: Tela de monitoração
Fonte: (AITA, 2011)

Esta tela simula o acesso do estudante pela catraca. O campo matrícula simula o usuário passando o cartão, neste momento o software faz uma busca no banco de dados selecionando o aluno e suas digitais. No próximo momento é simulada a solicitação da digital, o software compara com os registros selecionados anteriormente através de um algoritmo que extrai as minúcias da digital lida, cria um registro na tabela histórico e libera o acesso.

Figura 20: Tela de parâmetros
Fonte: (AITA, 2011)

A tela de parâmetros mostra os campos usados para a pesquisa no banco de dados e criação de um gráfico ou um relatório com as estatísticas de acesso.

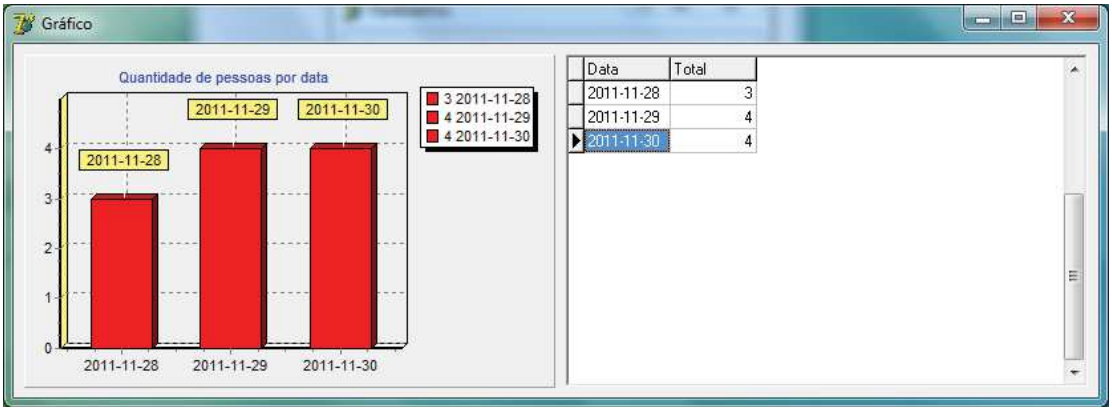


Figura 21: Tela de gráfico das estatísticas
Fonte: (AITA, 2011)

2.2.7 Registro de acesso de entrada e saída

A tabela Histórico do banco de dados conterá o horário de entrada e saída do estudante na universidade, assim como a quantidade de acessos, ou seja, o software verificará se ele entrou e saiu mais de uma vez por dia. Ainda assim não terá a certeza de que o estudante entrará na aula, somente nas dependências da universidade.

2.2.8 Dados estatísticos

A partir dos dados da tabela Histórico, o software mostrará gráficos com os dados estatísticos do acesso à universidade, podendo ser representado a quantidade total de acessos (contando com aqueles que saíram e entraram mais de uma vez), a quantidade de pessoas que acessaram a universidade (aqueles que entraram mais de uma vez serão contados só uma), quantidade de acessos por aluno em qualquer período de tempo e utilizando mais alguns dados do aluno como o curso e fase, poderá ter estatísticas mais pontuais.

2.2.9 Localização das catracas

As catracas serão implantadas em três entradas: no colégio de aplicação, na entrada da cantina e na escadaria localizada perto da passarela. As outras entradas serão fechadas. Cada entrada terá três catracas para o acesso dos estudantes e a entrada do colégio de aplicação possuirá uma catraca para portadores de necessidades especiais.

2.2.10 Custos

Esta seção do trabalho apresentará os custos do projeto, do software e o preço da catraca e software do fornecedor.

Tabela 3: Custos para construir a catraca

Materiais	Valor
1 tubo de aço carbono 700mm x 76,20 mm	R$ 65,00
1 chapa de aço carbono 400mm x 600 mm x 3 mm	R$ 85,00
1 chapa de aço carbono 90 mm x 130 mm x 5 mm	R$ 20,00
3 tubos de alumínio 550 mm x 31,75 mm	R$ 60,00
1 leitor de cartão com código de barras	R$ 35,00
1 leitor de impressão digital	R$ 109,00
1 hub *USB*	R$ 29,00
Total	R$ 403,00

Fonte: (AITA, 2011)

Tabela 4: Custo das catracas fornecedor Dimep

Catracas	Valor
Código de barras e biometria TCP-IP	R$ 6.700,00
Código de barras e biometria RS232	R$ 4.160,00
RFID Acura	R$ 10.100,00
RFID Motorola	R$ 12.750,00
RFID HID	R$ 11.280,00
RFID Mifare	R$ 12.200,00

Fonte: (SITE DIMEP, 2011)

Tabela 5: Custos do software

Software	Valor	Treinamento	Total
MPAcesso 1 catraca	R$ 1.620,00	R$ 534,00	R$ 2.154,00
MPAcesso 5 catracas	R$ 3.450,00	R$ 976,00	R$ 4.426,00
MPAcesso 10 catracas	R$ 5.076,00	R$ 1.972,00	R$ 7.048,00

Fonte: (SITE DIMEP, 2011)

2.2.11 Análise dos dados

Observando os dados da seção anterior, pode-se notar que o custo para criar uma catraca é muito inferior do que comprar uma pronta, embora a tecnologia

agregada seja maior nesta última. O custo de um programador em Delphi custa entre R$ 2.500,00 e R$ 5.000,00 por mês e dependendo do tempo que levaria para desenvolver o software poderia sair mais caro que o software pronto. Os projetos das catracas de algumas empresas contemplam ações em caso de emergência, como o giro livre em caso de queda de energia ou a queda do braço ao soar um alarme. Estas ações não foram inclusas no projeto da catraca, mas podem ser facilmente implantadas ligando o sinal de alarme no solenoide de liberação da catraca. Considerando que o solenoide fica aberto sem energia e com energia fica trancado.

3 CONCLUSÃO

Diante do que foi exposto, percebe-se que a tecnologia agregada neste tipo de produto é alta, encarecendo muito o preço. Porém é viável o desenvolvimento de um sistema de controle de acesso para uma aplicação na universidade, ainda podendo ser desenvolvida por acadêmicos, projetando a catraca, o software e a comunicação com o servidor, proporcionando o aprendizado dos estudantes na prática e reduzindo os custos que teria com mão de obra especializada. Durante o desenvolvimento deste trabalho, foi conversado sobre o projeto com o Vice Reitor de Administração e Planejamento da UNIARP, Prof. Almir Granemann Reis e ele já tinha tentado implantar um controle de acesso, mas que não daria certo, pois barra em aspectos legais de que a universidade não poderia restringir o acesso da comunidade em suas dependências. Essa questão ainda poderia ser pesquisada porque o objetivo deste projeto seria controlar a entrada de pessoas e não restringir.

REFERÊNCIAS

ACESSO E PONTO. **Leitor Biométrico de Impressão Digital.** Disponível em: <http://acessoeponto.mixlog.com.br/artigo/leitor-biometrico-de-impressao-digital/>. Acesso em: 11 nov. 2011.

ACTIVEBARCODE. **UPC-A/UPC-E**. Disponível em: <http://www.activebarcode.com/codes/upca_upce.html>. Acesso em: 30 ago. 2011.

ALECRIM, Emerson. **Introdução à Biometria.** Disponível em: <http://www.infowester.com/biometria.php>. Acesso em: 27 out. 2011.

ALLEN, Lee. **Code 128 Specifications.** Disponível em: <http://www.barcodeman.com/info/c128.php>. Acesso em 30 ago. 2011.

ALLEN, Lee. **Code 2 of 5 Specifications.** Disponível em: <http://www.barcodeman.com/info/c2of5.php>. Acesso em: 30 ago. 2011.

ARAGÃO, Francisco. **Login biométrico por reconhecimento facial.** Disponível em: <http://pplware.sapo.pt/windows/software/login-biometrico-por-reconhecimento-facial/>. Acesso em: 11 nov. 2011.

CONSULTORES BIOMETRICOS ASSOCIADOS. **Tipos de Biometria – Olho.** Disponível em: <http://www.consultoresbiometricos.com.br/05_Dbio_olho.php>. Acesso em: 05 nov. 2011.

CAVALCANTE, Adalberto L. S.: BACCI, Márcio Demetrio; HOKAMA, Marçal de Lima. **Assinatura de Documentos Digitais através da Biometria no Exército Brasileiro.** Disponível em: <http://www.ensino.eb.br/artigos/artigo_biometria.pdf>. Acesso em: 03 nov. 2011.

DIMEP. **Dimep Sistemas.** Disponível em: <www.dimep.com.br>. Acesso em: 30 nov. 2011.

ERDEI, Guillermo E. **Código de Barras: desenvolvimento, impressão e controle de qualidade.** 1 ed. São Paulo: Makron Books, 1994.

FARIA, Alessandro de Oliveira. **Biometria: Processamento de imagens capturadas em leitores de impressão digital.** Disponível em: <http://www.vivaolinux.com.br/artigo/Biometria-Processamento-de-imagens-capturadas-em-leitores-de-impressao-digital>. Acesso em: 11 nov. 2011.

GROSSMANN, Fábio; ZYNGIER, Mauro Luiz. **Código de Barras da teoria à prática.** 1. ed. São Paulo: Nobel, 1991.

HARRIS, Tom. **Como funcionam os leitores de impressões digitais.** Disponível em: <http://informatica.hsw.uol.com.br/leitores-de-impressoes-digitais.htm>. Acesso em: 27 out. 2011.

LINHABASE. **Enciclopédia sobre Código de Barras: 3 de 9.** Disponível em: <http://www.linhabase.com.br/codigodebarras/simbologias/3de9.asp>. Acesso em: 30 ago. 2011.

LINHABASE. **Enciclopédia sobre Código de Barras: EAN-13.** Disponível em: <http://www.linhabase.com.br/codigodebarras/simbologias/ean13.asp>. Acesso em: 30 ago. 2011.

PINHEIRO, José Maurício. **Biometria nos Sistemas Computacionais – Você é a senha.** 1.ed. Rio de Janeiro: Ciência Moderna, 2008.

PSITECNOLOGIA. **Conceitos Básicos sobre Código de Barras.** Disponível em: <http://www.psitecnologia.com.br/Marketing/saiba_mais.asp>. Acesso em: 05 nov. 2011.

QUADROS, Daniel. **Código de Barras – EAN-8**. Disponível em: <http://dqsoft.blogspot.com/2008/07/cdigo-de-barras-ean-8.html>. Acesso em: 30 ago. 2011.

QUADROS, Daniel. **Código de Barras – EAN-13**. Disponível em: <http://dqsoft.blogspot.com/2008/07/cdigo-de-barras-ean-13.html>. Acesso em: 30 ago. 2011.

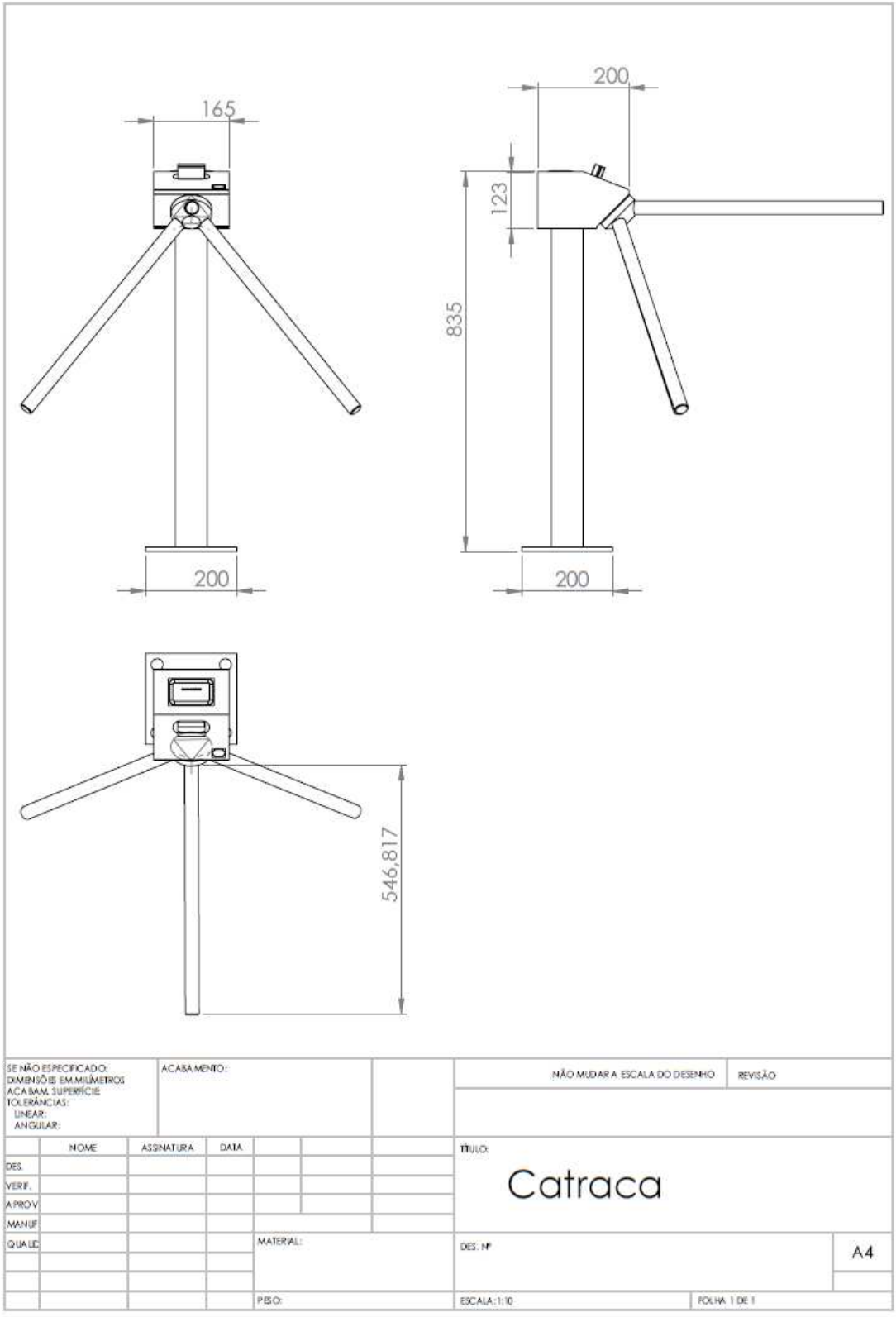
QUADROS, Daniel. **Código de Barras – UPC-A**. Disponível em: <http://dqsoft.blogspot.com/2008/07/cdigo-de-barras-upc.html>. Acesso em: 30 ago. 2011.

QUADROS, Daniel. **Código de Barras – UPC-E**. Disponível em: <http://dqsoft.blogspot.com/2008/07/cdigo-de-barras-upc-e.html>. Acesso em: 30 ago. 2011.

ROCHA, Luiz Cláudio C. V. da. **Código de barras sem mistérios.** Disponível em: <http://msdn.microsoft.com/pt-br/library/cc580676.aspx>. Acesso em: 30 ago. 2011.

SANTINI, Arthur Gambin. **RFID: Conceitos, Aplicabilidades e Impacto.** 1.ed. Rio de Janeiro: Ciência Moderna, 2008.

APÊNDICE


165
200
200
123
835
200
546,817
SE NÃO ESPECIFICADO:
DIMENSÕES EM MILÍMETROS
ACABAM. SUPERFÍCIE
TOLERÂNCIAS:
LINEAR:
ANGULAR:
ACABAMENTO:
NÃO MUDAR A ESCALA DO DESENHO
REVISÃO
NOME
ASSINATURA
DATA
DES.
VERIF.
APROV
MANUF
QUALID
MATERIAL:
PESO:
TÍTULO:
Catraca
DES. Nº
A4
ESCALA: 1:10
FOLHA 1 DE 1