**UNIVERSIDADE DE TAUBATÉ**

MESTRADO PROFISSIONAL


Marcos Paulo Sanchez

# REGISTRO DE FREQUÊNCIA DE DISCENTES POR MEIO DE BIOMETRIA

TAUBATÉ - SP

2011

**UNIVERSIDADE DE TAUBATÉ**

MESTRADO PROFISSIONAL


Marcos Paulo Sanchez

# REGISTRO DE FREQUÊNCIA DE DISCENTES POR MEIO DE BIOMETRIA

Dissertação apresentada para obtenção do Título de Mestre pelo Curso de Pós-Graduação do Departamento de Engenharia Mecânica da Universidade de Taubaté.
Área de Concentração: Automação.

Orientador: Prof. Dr. Márcio Abud Marcelino

TAUBATÉ - SP

2011

**UNIVERSIDADE DE TAUBATÉ**

MESTRADO PROFISSIONAL

# REGISTRO DE FREQUÊNCIA DE DISCENTES POR MEIO DE BIOMETRIA

Marcos Paulo Sanchez

Orientador: Professor Doutor Márcio Abud Marcelino

TAUBATÉ - SP

2011

SANCHEZ, MARCOS PAULO

Registro de Frequência de Discentes por Meio de Biometria / Marcos Paulo Sanchez. Taubaté: Unitau, 2010.

70 f.: il.

Dissertação (Mestrado) – Universidade de Taubaté. Faculdade de Engenharia Mecânica. Curso Mestrado em Engenharia Mecânica.

Orientador: Márcio Abud Marcelino

1. Biometria. 2. Impressão Digital. 3. Registro de Frequência em IES. I. Título.

**MARCOS PAULO SANCHEZ**

# REGISTRO DE FREQUÊNCIA DE DISCENTES POR MEIO DE BIOMETRIA

Dissertação apresentada para obtenção do Título de Mestre pelo Curso de Pós-Graduação do Departamento de Engenharia Mecânica da Universidade de Taubaté.
Área de Concentração: Automação.
Orientador: Prof. Dr. Márcio Abud Marcelino

Data: 12 de Novembro de 2011.

Resultado: _____

BANCA EXAMINADORA

Prof. Dr. Márcio Abud Marcelino – UNESP / Universidade de Taubaté

Assinatura _____

Prof. Dr. Francisco José Grandinetti - UNITAU

Assinatura _____

Prof. Dr. José Feliciano Adami – UNESP/FEG

Assinatura _____

Dedico este trabalho antes de tudo aos meus pais, Miguel e Regina, os quais investiram seu tempo, dinheiro e principalmente carinho para que eu pudesse realizar tudo que tenho realizado até agora, sem os quais eu não teria a formação que tenho. Dedico, também, a minha esposa Tiessa a qual sempre me apoiou e me ajudou a progredir em meu trabalho e seguir a busca deste título independente dos percalços que ocorreram. Não posso esquecer-me de meus companheiros de estrada Magalhães e Mauro, que compartilharam comigo esta jornada, onde juntos temos centenas de histórias a contar. Muito importante a participação de meu orientador Márcio Abud, o qual acreditou em meu empenho e trabalho e me deu forças para conseguir finalizar este trabalho. Agradeço a todos que me ajudaram neste caminho, e também a nosso Deus Jeová o qual me abençoa todos os dias com a dádiva de uma vida com saúde e paz.

O que veio a ser, já tem sido, e o que virá a ser, já veio a ser; e o próprio [verdadeiro] Deus continua a procurar aquilo pelo qual há empenho.

Eclesiastes 3:10

# AGRADECIMENTOS

Ao Prof. Dr. Márcio Abud Marcelino pela orientação e direcionamento atribuído ao desenvolvimento deste trabalho.

Ao Prof. Dr. Cao Jin Kan por suas importantes opiniões, contribuições e incentivo no aprimoramento deste trabalho.

Ao Prof. Dr. João Bosco Gonçalves por seu direcionamento e ajuda na busca de um orientador para finalização deste trabalho.

Aos amigos de mestrado Mauro e Magalhães pela interação constante, apoio para realização deste mestrado.

# RESUMO

A necessidade de um registro rápido e eficiente de frequência do corpo discente de instituições de ensino mostrou uma grande oportunidade de automação com a utilização da identificação biométrica por impressão digital, tornando o controle de frequência integro e ágil, otimizando o tempo de aula e garantindo a disponibilidade da informação, atingindo assim a eficiência necessária no sistema de apuração como um todo. Este trabalho mostra a utilização da biometria como mecanismo seguro dentro de sala de aula na identificação de alunos e a eficiência do sistema aplicando o algoritmo linear a partir de um universo selecionado. A busca pela identificação deve ser feita registro a registro, o que aumenta e muito o custo da aplicação e desta forma aplicou-se o algoritmo linear dentro de um universo selecionado, através de uma chave, diminuindo e muito o custo de busca de um registro. Outro fator é a possibilidade de se diminuir a quantidade de pontos equivalentes, uma vez que a comparação é executada dentro de um universo menor. Os resultados se mostraram favoráveis uma vez que a performance de busca dentro do universo total sofre depreciação cada vez que este universo aumenta e a busca linear dentro de um universo selecionado mantém a performance que inicialmente já é superior, uma vez que esta seleção mantém uma média linear entre todas as turmas dentro de uma instituição de ensino. Outro fator importante para os resultados na utilização do algoritmo linear é que o comparador de características pode ser otimizado, diminuindo a quantidade de características a serem comparadas, uma vez que o universo selecionado para comparação sendo menor, a probabilidade do encontro de impressões digitais com características semelhantes é bastante reduzido.

**Palavras chave:** Biometria, Digital, Frequência Acadêmica

# ABSTRACT

A great deal of the most critical systems of the current civilization depends on the surveillance, analysis and modulation of biometric signs. The security of several automatic systems is based more and more on biometric data namely by the identification of fingerprints. In spite of the recognition of fingerprints be an already quite studied and well documented issue still subsist enough challenges for investigate, improve and resolve. The necessity an efficient control fast e in the register of frequency of the student of college showed a great chance of automation with the use of the biometric access with fingerprint, becoming the control of efficient, integral and agile frequency, optimizing the lesson time and guaranteeing the availability of the information. This work studied the use of the biometry as mechanism of security inside of classroom in the identification of students, applying the linear algorithm in a selected universe. The search for a biometric identification must be made register to register, what it increase the cost of the application, applying the linear algorithm in the selected universe, through a key, diminishing the cost of search of a register. Another factor is the possibility of the diminishing the amount of points equivalents, in the time that the comparison is executed inside of a minor universe. The results had shown favorable a time that the performance of search inside of the total universe suffers to depreciation each time that this universe increases and the linear search inside of a selected universe keeps the performance that initially already is superior, a time that this selected universe keeps a linear average enters all inside the groups of an education institution. Another important factor for the results in the use of the linear algorithm is that the comparator of characteristics can be optimized, diminishing the amount of characteristics to be comparative, a time that the universe selected for comparison being lesser, the probability of the meeting of fingerprints with similar characteristics sufficiently is reduced.



**Keywords:** Biometric signs, Fingerprints, current civilization

# ÍNDICE

# ÍNDICE DE FIGURAS

# ÍNDICE DE TABELAS

# ABREVIATURAS E SIGLAS

| | |
|---|---|
| **ANSI**: | American National Standard Institute |
| **API**: | Application programming interface |
| **BLOB**: | Binary Large Object |
| **CCD**: | Charge-coupled device |
| **CMOS**: | Complementary Metal-Oxide-Semiconductor |
| **CN**: | Crossing Number |
| **CPF**: | Cadastro de pessoa física |
| **DPI**: | Dots per inch |
| **EER**: | Equal Error Rate |
| **FAR**: | False Aceptance Rate |
| **FRR**: | False Rejectection Rate |
| **FTIR**: | Fourier transform infrared spectroscopy |
| **IES:** | Instituição de Ensino Superior |
| **ISO**: | Internation Standard Organization |
| **RG**: | Registro Geral |
| **SDK**: | Software Development Kit |

# 1. INTRODUÇÃO

## 1.1. Descrição do problema

Ainda hoje a maior parte de instituições de ensino utilizam listas em papel para o controle da frequência de alunos em sala de aula. Algumas instituições utilizam listas de presença onde o professor deve efetuar a "chamada" para identificar os alunos que estão presentes, outras utilizam listas de assinatura. Em ambas as situações, o controle de frequência em sala de aula traz dois paradigmas a serem quebrados:

1. Ou o docente demanda tempo para realização da chamada, uma vez que o docente necessita identificar cada discente presente e registrar em seu diário;

2. Ou a integridade dos dados perde a confiabilidade com listas de presenças assinadas pelos alunos, uma vez que o professor não será capaz de identificar se os discentes presentes assinaram apenas em seu nome, ou o docente despenderá de boa parte da aula para acompanhar aluno a aluno na assinatura de listas.

A produção das informações físicas geradas, seja em diários ou listas de presenças, deverá ser imputada no sistema de gerenciamento da instituição e estas tarefas exigem um retrabalho para digitação ou digitalização dos dados coletados, o que decorrerá longos intervalos de tempo até a apuração total dos dados e disponibilização para consulta ou processamento.

A biometria é uma ciência que possibilita o reconhecimento e identificação por uma análise de características físicas de uma pessoa tais como geometria da mão, impressão digital, íris, retina, reconhecimento facial e voz, entre algumas outras. Estas características consideradas únicas de pessoa para pessoa (PINHEIRO, 2008). Este trabalho mostra a utilização da coleta biométrica por impressão digital na identificação dos discentes em sala de aula para registro de frequência, sendo que tal identificação deve ser realizada de forma que o discente necessite apenas inserir sua digital em um leitor biométrico e o sistema identifica automaticamente sua identidade, registrando então sua presença na aula, não havendo qualquer outro tipo de interação, como, por exemplo, a digitação de seu registro acadêmico. Inicialmente este processo requer um tempo maior de processamento, pois a impressão digital colhida terá que ser comparada, uma a uma, com cada impressão digital armazenada no

sistema, uma vez que o formato de armazenamento da informação biométrica não permite a indexação[1] ou busca imediata a partir de filtros ou condições.

Na aplicação da biometria como coleta de frequência de discentes em uma instituição de ensino o problema encontrado é o universo de *templates*[2], que são dados biométricos armazenados, existentes na procura 1:N, uma vez que para otimizar a coleta o aluno não deve ter interação alguma com a aplicação a não ser a inserção de sua impressão digital no sensor biométrico.

A aplicação que realiza a procura com o método 1:N na base de dados biométricos em uma instituição de ensino traz um grande problema: tempo de pesquisa, fato por que a *template* biométrica é um dado binário formado a partir das extração de uma imagem, sendo assim não podendo indexar a informação e como consequência é necessário uma busca sem índice ou informações que possam ser filtradas, demandando tempo o que pode inviabilizar a utilização da biometria como um meio de coleta da informação da frequência acadêmica em uma sala de aula.

Já existem outras soluções no mercado sendo vendidas comercialmente e até em testes. No 2º semestre de 2011 a Escola Municipal Roberto Mário Santini, da cidade de Praia Grande (SP), instalou um sistema biométrico para controlar a presença dos alunos, este projeto está por uma parceria entre a fabricante Madis e a Secretaria de Educação e usa um software desenvolvido pela Coordenadoria de Programas de Inclusão Digital do município. Neste projeto eles utilizam o próprio leitor biométrico para gravar as digitais dos alunos e este aparelho pode ser consultado via rede. A diferença aqui é que cada aparelho deve armazenar as digitais dos alunos, sendo assim caso haja troca de sala o aparelho tem que ser levado junto ou então é necessário regravar todas as digitais.

Outras entidades tentaram a implantação de sistemas similares, mas encontraram problemas de desempenho, infraestrutura e até problemas com sindicatos de professores ou mesmo com agremiações de alunos. Os trabalhos abandonados por problemas de infraestrutura se deram pelo fato de que a biometria precisa ser estruturada corretamente para

---

[1] Organização de dados em seu armazenamento, com o intuito de melhorar a busca de dados; Normalmente esta organização é feita em ordem alfabética ou numérica.

[2] *Template* - É constituído pelos dados biométricos significativos, extraídos das linhas da impressão digital e capturados a partir de um sensor.

ser distribuída, ou seja, uma infraestrutura de rede funcional é necessária, não necessariamente a mais cara ou então a de última geração, mas sim uma estrutura que funcione e permita o tráfego dos dados de forma adequada e sem "congestionamentos de redes" (CEZAR, 2001).

O enfoque dado neste trabalho levou em consideração a *performance* da busca em si, entretanto será mostrado o que foi feito com o corpo docente, discente e infraestrutura para que o projeto fosse viável.

O objetivo deste trabalho é definir um método de pesquisa de modo a otimizar o processo de localização da informação biométrica armazenada em um banco de dados, reduzindo o tempo de identificação na comparação entre a informação coletada e as informações armazenadas, utilizando para isso o algoritmo de busca linear dentro de um universo menor de informações biométricas armazenadas, ou seja, estabelecer um filtro a partir das informações ambientais, de tal forma que o universo utilizado para busca seja reduzido drasticamente, através das informações de ambiente já registradas no sistema, como, por exemplo, o cruzamento do professor que abriu o sistema com o horário de aula registrado, carregando assim apenas os dados biométricos das turmas selecionadas.

Outros objetivos do trabalho estão relacionados à:

1. Regular o número de coincidências necessárias para identificação de um indivíduo uma vez que o universo é menor, a probabilidade de coincidências entre impressões, também, é menor.
2. Realizar a coleta de pelo menos 75% da sala de aula nos quinze primeiros minutos.

## 1.2. Motivação

A possibilidade de tirar do professor um trabalho burocrático de dentro da sala de aula, fazendo com que o professor não tenha que se preocupar com a integridade da informação, com sua tabulação ou mesmo com o seu registro físico, passando para o sistema automatizado a captação dos dados e apuração dos mesmos, retirando praticamente todo o processo manual de coleta, registro, apuração, processamentos e disponibilização destes dados.

A disponibilidade no mercado de equipamentos e kits de desenvolvimento utilizando a biometria, que mesmo com um custo não tão baixo a primeira vista, ainda sim com um ganho operacional e até mesmo financeiro maior em médio prazo.

## 1.3. Metodologia

No sistema de identificação biométrica para controle de frequência de discentes foi utilizado o algoritmo de busca linear, uma vez que o trabalho irá apresentar que se trata de um algoritmo ótimo para localização de dados não indexados, pois neste caso o número máximo de pesquisa estará restrito ao número de elementos a ser pesquisado. Para otimização do processo, foram utilizadas as variáveis de ambiente como curso, turno, turma e docente, todas pré-cadastradas no sistema, e obrigatórias para o sistema, reduzindo o universo de informações biométricas, como também a quantidade real de coincidências que devem ser consideradas no comparativo entre a informação biométrica colhida e a armazenada.

## 1.4. Descrição dos demais capítulos

No capítulo 2 será apresentado o que é a biometria e o porquê da escolha da impressão digital como mecanismo de identificação em sala de aula, incluindo um estudo da identificação por impressão digital, mostrando quais são os tipos existentes, como se pode efetuar a classificação através das minúcias e assim como a identificação única pode ser obtida. Como o foco do trabalho é a identificação automatizada, serão apresentados os sensores que podem ser utilizados para o funcionamento do sistema, deixando claro suas vantagens e desvantagens.

No capítulo 3 é apresentado o modelo de sistema biométrico, apresentando suas fases e detalhando-as, desde a aquisição do exemplar biométrico até o seu armazenamento e posteriormente a comparação entre o exemplar colhido e o exemplar armazenado identificando a similaridade ou não. Este capítulo finaliza com uma avaliação de desempenho do sistema biométrico e a identificação e controle da falsa aceitação e falsa rejeição.

No capítulo 4 mostra a aplicação do sistema proposto, identificando qual foi o ambiente utilizado para o desenvolvimento deste trabalho, os recursos que foram necessários, como foi feita a escolha do algoritmo proposto para o sistema, apresenta como o algoritmo foi utilizado e define a proposta do trabalho descrevendo os ganhos propostos a serem obtidos

com o sistema. É apresentado também o protótipo desenvolvido e utilizado em sala de aula para obtenção dos dados que ajudaram na conclusão do trabalho.

No capítulo 5 são apresentados os resultados obtidos na prática com o trabalho, bem como a parametrização que foi necessária e ajustada durante a utilização do sistema em sala de aula e a visão que o corpo docente junto com coordenação tiveram na implantação e ajustes do sistema desenvolvido.

No capítulo 6 são apresentadas as conclusões após a finalização da implantação e porque os resultados se mostraram satisfatórios.

# 2. BIOMETRIA

A Biometria é o estudo das características únicas dos indivíduos, utilizado para sua identificação (LIU, 2001). Ela permite a identificação de indivíduos, a partir das características de cada um. Para tanto, ela baseia-se nas características comuns que são distinguíveis entre pessoas diferentes, isto é, características físicas ou comportamentais que são comuns a todos, porém únicas para cada indivíduo (CONSORTIUM, 2006).

## 2.1. Impressão Digital

Neste trabalho foi feita a escolha pela impressão digital por ser o meio de identificação biométrica atualmente mais barata e, também, por ser relativamente seguro. É a técnica de identificação biométrica mais antiga, e tem sido utilizada com sucesso em inúmeras aplicações e nos dias de hoje, tem-se o exemplo do Registro Geral (RG) ou identidade, utilizadas pelas Secretarias de Segurança Pública em todo o Brasil (DOS SANTOS, 2007). A identificação biométrica por impressão digital é definida como segura pelo princípio da unicidade, onde são estimados que a possibilidade de duas pessoas, incluindo gêmeos, terem a mesma impressão digital é menor que um em um bilhão. Essa segurança é aceita pelo meio científico desde 1823, quando o cientista tcheco Jan Evangelista Purkinje durante suas pesquisas sobre glândulas sudoríparas, constatou que a pele dos dedos possuía desenhos formados por sulcos e ranhuras únicos para cada indivíduo, conforme apresentado na Figura 1 (ASHBOURN, 2000).

**Figura 1 – Impressão Digital (ARAÚJO, 2009)**

Maltoni (2003) comparou as tecnologias biométricas e mostrou que a impressão digital possui alto desempenho, média acessibilidade e nível médio de fraudes (MALTONI, MAIO, JAIN, & PRABHAKAR, 2003).

## 2.2. Estudo da biometria

As impressões digitais são formadas geralmente no sétimo mês de gestação e permanecem intactas por toda a vida, se não houver um ferimento ou corte profundo (JAIN, PRABHAKAR, & PANKANTI, 2002). Esta propriedade faz com que a impressão digital seja um grande atrativo na identificação biométrica.

As impressões digitais são formadas por ranhuras ou cristas, que são as partes mais elevadas do desenho, e os sulcos (vales) que são a parte mais baixa do relevo da pele, conforme Figura 2. Segundo Maranhão (1989), as minúcias são resultados de acidentes apresentados pelas cristas e representam a garantia de unicidade em impressões digitais. Existem 5 tipos de impressões digitais, identificadas pelo estudo da datiloscopia, como apresentado na Figura 3. O formato da impressão pode definir os extremos da imagem coletada, uma vez que o tipo de impressão tem um padrão já estudado (MARANHÃO, 1989).

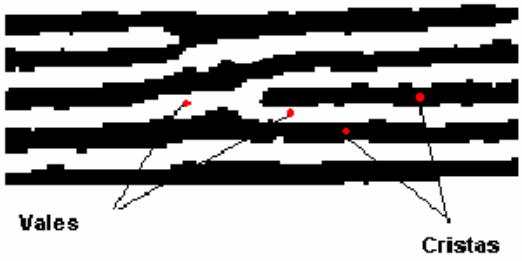



**Figura 2 – Formação das digitais (MAZETTI, 2006)**


**Figura 3 – Tipos de impressões digitais (KEHDY, 1968)**

Essas classes servem apenas para separar as impressões digitais em grandes grupos, e são baseadas no número de deltas com suas respectivas posições, não sendo possível identificar unicamente uma pessoa (GUMZ, 2002). Pode ser utilizada para verificar se a impressão colhida faz parte de um determinado grupo ou não.

Os tipos de impressões digitais, Figura 4, também são utilizados para identificar o centro da imagem, o alinhamento da imagem com base no centro, o tamanho da digital que é calculado através da medida central, criando assim uma área para comparação entre duas imagens, que tenham as mesmas condições. Desta forma é assegurada pelos algoritmos de comparação uma segurança ajustável com alteração dos limiares mínimos para coleta ser considerada uma correta identificação (LOPES, 2009).

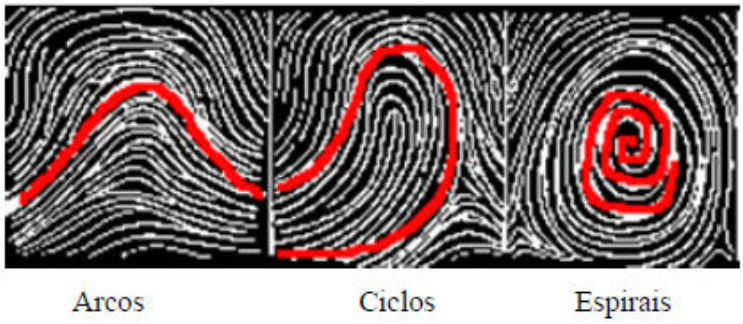



**Figura 4 – Tipos de impressões digitais e sua formação (LOPES, 2009)**

As cristas e os sulcos em cada terminação ou bifurcação de suas linhas formam um desenho geométrico chamado minúcia. É através das características das minúcias (formato e posição) que a identificação de indivíduos pode ser feita. As minúcias permitem que um perito possa identificar uma pessoa de forma bastante confiável. A identificação da minúcia é feita sempre que uma linha é finalizada, a finalização ocorre de duas formas: o fim seco da linha, ou seja, o término abrupto, chamado Fim de Linha; ou então pela continuação da mesma linha por dois caminhos, que é chamado de Bifurcação, como apresentado na Figura 5 (FONTANA, 2009).


**Figura 5 – Identificação da Minúcia (HEMERLY & Peres, 2006)**

Apesar das duas formas como as minúcias são identificadas, elas se apresentam em formas bastante particulares, como apresentado na Figura 6. Kehdy identificou em seu estudo de 1968, 4 tipos de minúcias, Ilha, Cruzamento, Espora e Crista Curta. Por ilha identifica-se uma minúcia com duas bifurcações ligadas, ou seja, o seu desenho é obtido por uma linha,

bifurcação, transformando-se em linha novamente. O cruzamento apresenta duas linhas interligadas por uma linha perpendicular, encontrando-se então duas bifurcações, mas sem a continuidade como visto na ilha. A Espora é identificada por uma linha contínua que possui uma bifurcação com uma linha curta, representando a imagem de uma espora. E a Crista Curta que é uma linha com dois fim de linhas próximos. Uma imagem de boa qualidade deve encontrar entre 40 e 100 minúcias para identificação (CAMPESTRINI, 2003).


Fonte: Kehdy, 1.968, p.150

**Figura 6 – Tipos de minúcias (KEHDY, 1968)**

Em sua grande maioria, os sistemas de reconhecimento biométrico através de impressões digitais utilizam o método de análise das posições das minúcias para identificação de padrões. Para este tipo de reconhecimento deve-se levar em consideração a posição de leitura da impressão digital, possíveis ruídos (gordura, cortes, cicatrizes etc), entre outros aspectos variáveis no momento da leitura. Para que estas barreiras sejam eliminadas, um algoritmo sofisticado deve ser utilizado para leitura e processamento da impressão digital colhida.

## 2.3. Classificação por Minúcias

Minúcias são características únicas conhecidas, nomeadamente descontinuidades locais, que identificam pontos da impressão digital onde as cristas se bifurcam ou terminam. Formam a base de qualquer sistema que utilize as técnicas de comparação de impressões digitais para propósitos de identificação e verificação. Existem vários tipos de minúcias ilustradas na Figura 6 – Tipos de minúcias que podem ser reduzidos a dois grandes tipos: terminações e bifurcações, conforme Figura 7. Tipicamente uma imagem de boa qualidade tem entre 40 a 100 minúcias (LOPES, 2009).

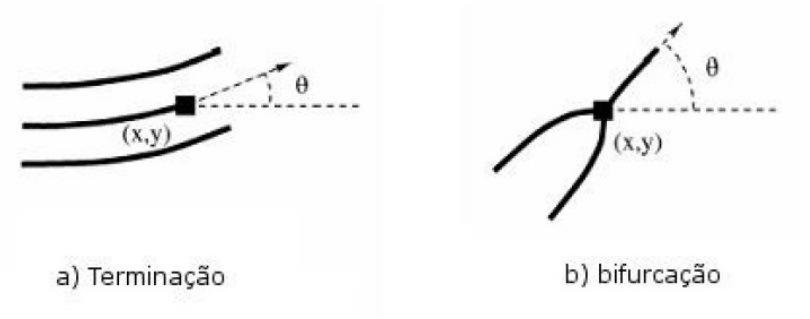



**Figura 7 – Os dois tipos de minúcias (LOPES, 2009)**

Conforme apresentado na Figura 7, a terminação é o ponto onde uma linha termina abruptamente; já a bifurcação é o ponto onde uma linha se separa em duas. O tipo da minúcia define se estamos na presença de uma terminação ou de uma bifurcação. A posição indica o local onde se verifica a existência da minúcia e a orientação dá-nos a direção da risca que originou a minúcia.

## 2.4. Sensores biométricos

A qualidade e a segurança do sistema de reconhecimento biométrico dependem, além do software, do tipo de sensor que é utilizado para coleta da informação biométrica. No caso da informação biométrica por impressão digital, os dois tipos de sensores mais utilizados são o óptico[3] e o capacitivo. Apesar do tipo de imagem coletada entre os 2 tipos de sensores serem diferentes, ambas possuem melhor qualidade para identificação através de um sistema, comparando com o método tradicional com tinta e papel. A Figura 8 mostra a diferença da imagem através dos 3 tipos de coletas.

[3] A Espectroscopia no infravermelho por transformada de Fourier (FTIV) é uma técnica de análise para colher o espectro infravermelho mais rapidamente. Em vez de se coletar os dados variando-se a freqüência da luz infravermelha monocromática, a luz IV (com todos os comprimentos de onda da faixa usada) é guiada através de um interferômetro. Depois de passar pele amostra o sinal medido é o interferograma. Realizando-se uma transformada de Fourier no sinal resulta-se em um espectro idêntico ao da espectroscopia IV convencional (dispersiva).

Os espectrofotômetros FTIV são mais baratos do que os convencionais porque é mais simples construir um interferômetro do que um monocromador. Em adição, a medida de um único espectro é bem mais rápida nessa técnica porque as informações de todas as freqüências são colhidas simultaneamente. Isso permite que se faça múltiplas leituras de uma mesma amostra e se tire a média delas, aumentando assim a sensibilidade da análise. Devido às suas várias vantagens, virtualmente todos os espectrofotômetros de infravermelho modernos são de FTIV;

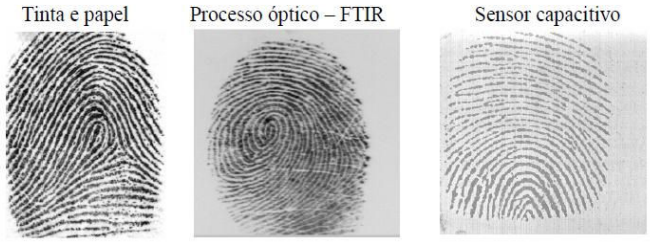



**Figura 8 - Diferença da imagem na variação do método de coleta**

A maior diferença entre os dois tipos de sensores, está no fato de que o sensor capacitivo pode trazer maior segurança na identificação, devido ao seu mecanismo de leitura permite maior segurança do que o sensor óptico, ou seja, o sensor óptico é mais fácil de ser burlado, como, por exemplo, através de uma imagem em papel.

### 2.4.1. Sensor óptico

O sensor óptico é construído através de uma câmera CCD[4] (dispositivo de carga acoplada), que consiste em uma série de diodos foto sensíveis recobertos por uma camada de cristal ou acrílico com silicone, onde o dedo é colocado e uma foto é tirada da impressão digital. Este tipo de sensor foi o primeiro a ser utilizado para converter diretamente a impressão digital em imagem. A imagem da impressão digital é obtida de forma semelhante a uma câmera eletrônica (CCD ou CMOS[5]), ou seja, através da emissão de luz, conforme Figura 9.

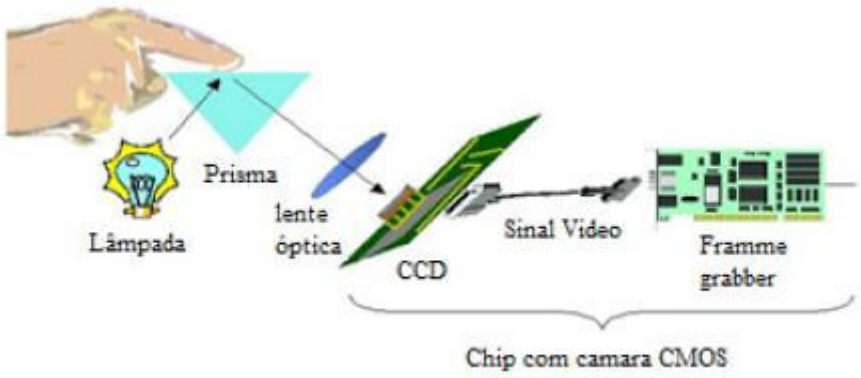



**Figura 9 - Esquema ilustrativo do funcionamento dos sensores ópticos (LOPES, 2009)**

O sensor óptico é o sensor mais barato do mercado, entretanto, dependendo da aplicação, a facilidade de burlar o mecanismo de reconhecimento é muito alta, pois a extração

[4] CCD – Charge-Coupled Device

[5] CMOS - Complementary metal-oxide-semiconductor

é feita através de uma imagem 2D. A sujeira, oleosidade da pele e riscos na resina sobre o local de inserção digital afeta diretamente na extração do exemplar. A Figura 10 apresenta um modelo de sensor óptico. Este sensor destaca-se pelo atual baixo custo e facilidade de utilização pelo usuário.

**Figura 10 - Sensor óptico**

### 2.4.2. Sensor Capacitivo

O sensor capacitivo tem o funcionamento muito parecido com o sensor óptico para geração da imagem. O sensor capacitivo é formado por uma camada de silicone, onde são colocados sensores capacitivos condutores cobertos por uma capa isolante. Esse sensor utiliza a tecnologia capacitiva e a captura é executada através do movimento de *swipe*, ou seja, de deslizamento ou passagem do dedo no sensor. A tecnologia capacitiva captura a imagem em três dimensões, mensurando a diferença de capacitância entre o dedo e o sensor, isto é, captura também a profundidade dos sulcos[6] da impressão digital, com isso o sensor gera um tom de cinza correspondente à distância da pele do dedo e a superfície do sensor, conforme ilustrado na Figura 11.

[6] Os sulcos são formados pela diferença de altura entre as cristas (ridge) e o vale (valley).

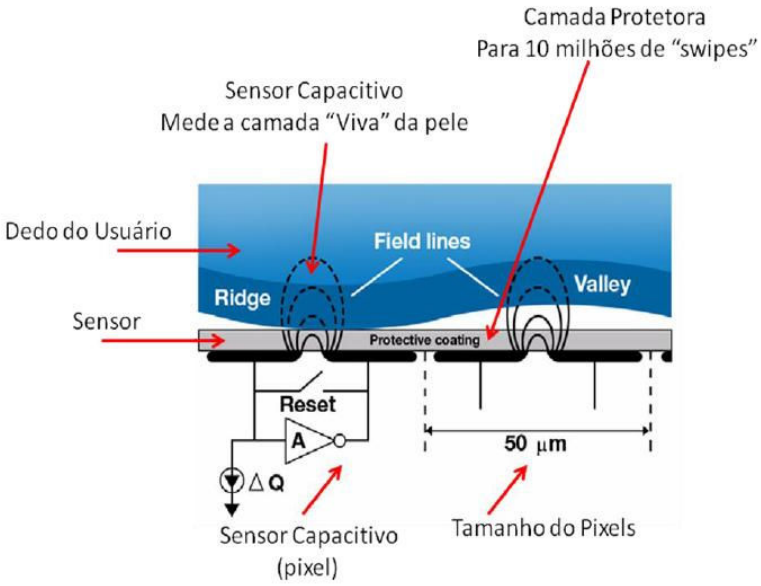



**Figura 11 - Esquema ilustrativo do funcionamento dos sensores capacitivos – EIKON D2 PRO**

A captura da impressão digital é feita por faixas através do posicionamento do sensor (*field lines*), sendo que a abertura do sensor define o tamanho da faixa em pixel[7], conforme a rolagem do dedo sobre o sensor, de acordo com a Figura 12.

**Figura 12 - Sensor Capacitivo modelo EIKON**

Conforme Figura 13, a montagem da impressão digital é feita por um algoritmo que posiciona a faixa de captura para formar uma imagem única com deformação desprezível, fazendo inclusive a correção lateral e minimizando a variação lateral na leitura da impressão na rolagem para captura, ou seja, o algoritmo do sensor reposiciona a imagem minimizando o fato de que pode ter havido tremor na rolagem do dedo.

[7] Um pixel é o menor ponto que forma uma imagem digital.

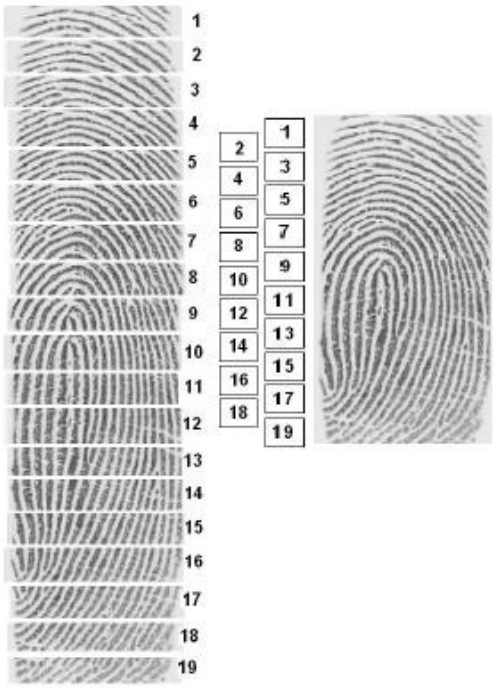



**Figura 13 - Remontagem da imagem da impressão digital – Manual EIKON**

A maior vantagem do sensor capacitivo está no fato de que é preciso um dedo físico para gerar a diferença de capacitância e com isso a burla do sistema é muito mais difícil. Entretanto a variação de humidade pode prejudicar o sistema de extração da imagem da impressão digital, uma vez que o dielétrico é alterado (HENRIQUE, 2009).

# 3. MODELO DE SISTEMA BIOMÉTRICO

A aquisição das imagens de uma impressão digital, por muitos anos foi baseada em tinta e papel (SENIOR, 2002) utilizando-se dois métodos: o primeiro método e mais comum é quando o dedo coberto de tinta é rolado de um lado ao outro num pedaço de papel, de maneira que o desenho digital não apresente borrões ou manchas. Este método captura uma superfície maior do dedo, mas na prática, estas imagens apresentam problemas no ato de rolar o dedo, podendo causar distorções no resultado da imagem por excesso ou falta de tinta, afetando notavelmente a qualidade da imagem. O segundo método implica em apenas pressionar o dedo coberto de tinta sobre o papel, sem rolar o dedo.

A premissa para identificação biométrica é a aquisição da imagem da impressão digital do indivíduo, que na Figura 14 é chamado de usuário. A partir desta imagem é adquirido o exemplar e deste exemplar são extraídas as minúcias, obtendo-se assim os atributos (ZHAO & TANG, 2002). A partir destes atributos é gerado um código binário que será armazenado no banco de dados, o que é chamado de *Template*, apresentado na Figura 14, por Pinheiro (2008), como Perfil.

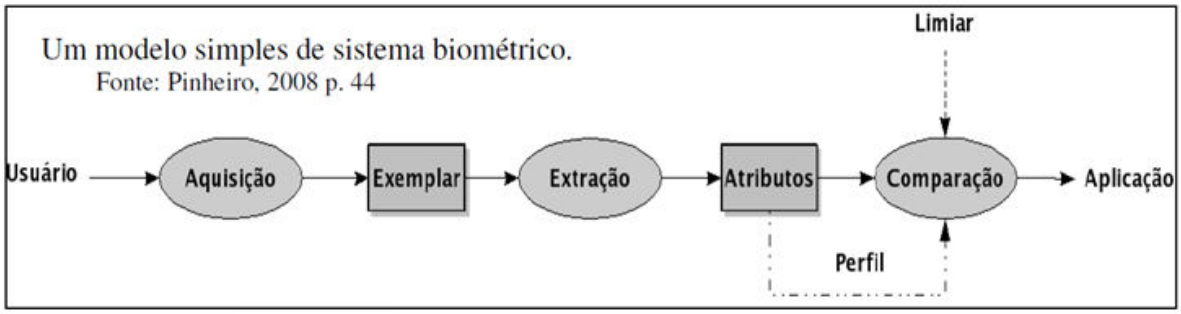
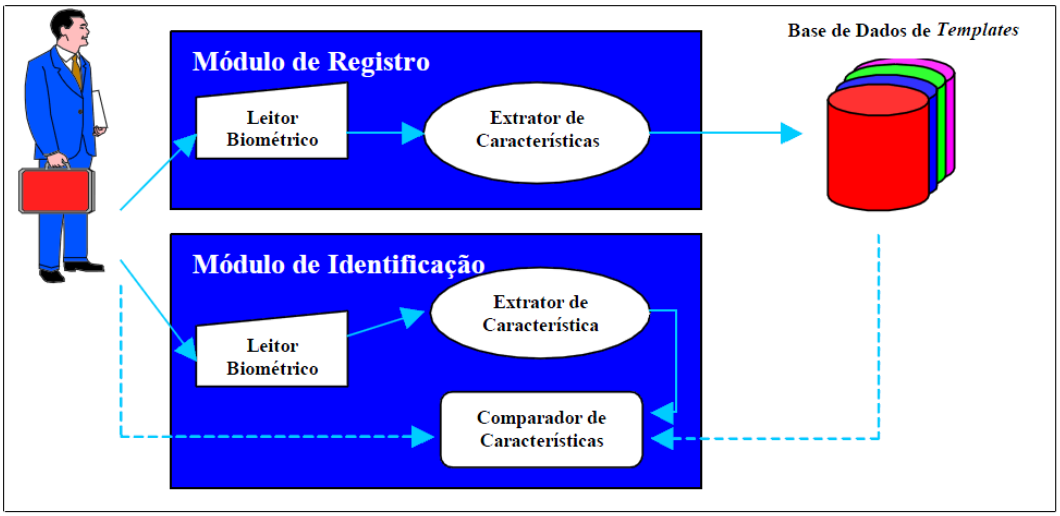



**Figura 14 – Modelo simples de um sistema biométrico (PINHEIRO, 2008)**

A comparação dos dados biométricos é feita através de comparações ponto a ponto, minúcia a minúcia, e um a um, ou seja, para encontrar uma digital dentro de um universo armazenado, deve-se comparar o exemplar colhido com cada *template* armazenado (uma a uma) e em cada digital comparar cada ponto obtido, verificando o número de coincidências (ponto a ponto). O limiar descrito na Figura 14, indica a quantidade mínima de pontos para o reconhecimento por semelhança, já que na comparação entre o exemplar colhido na hora e a *template* armazenada, nem sempre o número de pontos é igual. A comparação ponto a ponto

para cada digital é necessário, por este fato, que a cada coleta há variações na quantidade e qualidade dos pontos digitalizados, podendo variar posição, iluminação, tipo de sensor, e até mesmo a quantidade de gordura pode interferir em uma leitura exata. Desta forma a extração exatamente igual dos pontos torna-se inviável devido ao alto custo, tanto de software como de hardware, e também na preparação ambiental para coleta (limpeza e higienização da superfície do dedo, do visor do scanner, iluminação do local, ângulo de leitura, etc). Em uma escola, por exemplo, seria impossível garantir as mesmas condições ambientais a cada leitura, a diversificação de salas, computadores e volume de pessoas é grande, além disso, o tempo para realização da tarefa é extremamente limitado.

Um sistema para identificação biométrica simples é composto por pelo menos dois módulos conforme apresenta a Figura 15. O Módulo de Registro, responsável por gerar a *template* do indivíduo e armazená-la na base de dados e o Módulo de Identificação, que é utilizado para coleta e identificação do indivíduo. No caso deste estudo o foco está no Módulo de Identificação que foi desenvolvido para identificar o discente de forma rápida e segura.




Fonte: Hong, 1.998, p.4

**Figura 15 – Estágios de um sistema biométrico (HONG & JAIN, 1998)**

Como descrito por Hong quando o registro biométrico é cadastrado ele é armazenado em um banco de dados e amarrado a uma chave de identificação do indivíduo (HONG & JAIN, 1998). Para o resgate deste registro, pode-se optar por duas formas: 1) o usuário utiliza a chave de identificação, que pode ser o registro acadêmico, CPF, RG etc, para localizar a *template* no banco de dados e então coleta o exemplar para ser comparado, e este processo é chamado “um para um”; 2) ou então é feita uma varredura registro a registro no banco de

dados até encontrar a *template* semelhante ao exemplar colhido e confirmar a identificação do usuário, e este processo é chamado “um para muitos”.

Através da aquisição das características da impressão digital é criado um modelo computacional normalmente denominado *template* biométrico, conforme apresentado na Figura 16. Este modelo é gerado com propriedades particulares contendo uma síntese de todas as características extraídas, com o tamanho adequado, de modo a permitir um processo de identificação correto e ágil, para uma dada aplicação.

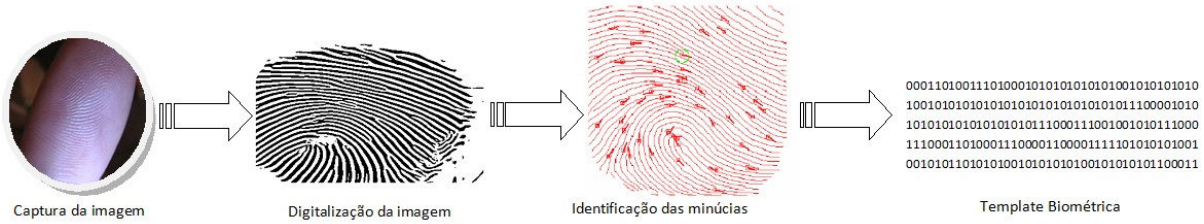



**Figura 16 – Esquematização da montagem da *template* (CURADO, 2006)**

Entre a fase de captura da imagem e a definição das minúcias para formação da *template*, existem algumas etapas essenciais no processo. A imagem colhida pelo sensor deve ser tratada para que as minúcias possam ser identificadas. Essas etapas contemplam: a) definir a região a ser trabalhada; b) qual a orientação que deve ser considerada para processamento; c) processamento das linhas formadas pelos sulcos para definição do exemplar a ser trabalhado; d) suavização da imagem para aumentar a definição da imagem para identificação das minúscias e; e) a extração das minúcias que serão utilizadas (LOPES, 2009).

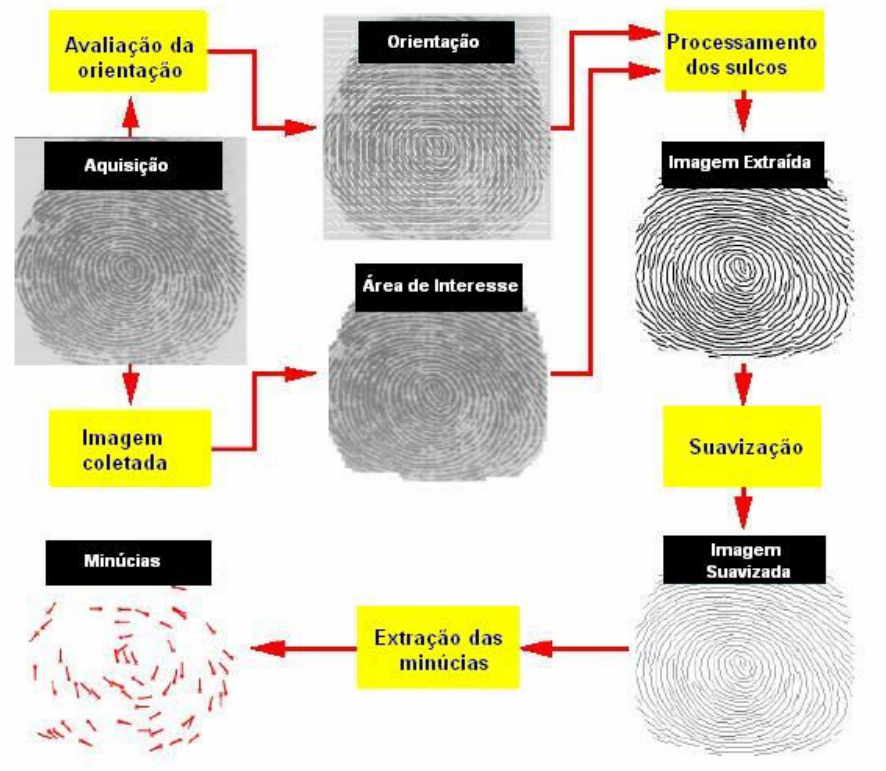



**Figura 17 – Diagrama da extração das características biométricas (JAIN, PRABHAKAR, & PANKANTI, 2002)**

## 3.1. Descrição do modelo de sistema biométrico

### 3.1.1. Aquisição

A aquisição é a etapa onde se captura a impressão digital do indivíduo através de um sensor biométrico (óptico ou capacitivo no caso). A aquisição nada mais é do que uma foto ou imagem da impressão digital colhida que será tratada para posterior armazenamento. O resultado da aquisição é apresentado na Figura 18.

**Figura 18 – Aquisição da Impressão Digital (ARAÚJO, 2009)**

### 3.1.2. Exemplar

A qualidade das imagens das impressões digitais varia bastante e em geral, ao serem adquiridas, a sua qualidade não é satisfatória. A qualidade da imagem influencia todas as etapas de um sistema de reconhecimento biométrico. Uma fraca qualidade da imagem poderá dar origem a falsas minúcias bem como a omissão de minúcias existentes e que deveriam ser consideradas na construção do *template* biométrico. O pré-processamento da imagem é uma etapa crucial num sistema de reconhecimento baseado em impressões digitais. O conjunto de técnicas utilizadas no pré-processamento para obtenção do exemplar de uma imagem de impressão digital engloba a aplicação de filtros de imagem e de operadores morfológicos, nomeadamente os operadores de binarização de imagem e esqueletização da mesma, além de utilização de um algoritmo de reconstrução de imagem em zonas onde são apresentadas distorções consideradas como reparáveis (LOPES, 2009).

A Figura 19 apresenta o Exemplar que é o resultado do tratamento da imagem adquirida. Para obtenção do exemplar, são aplicados filtros para renderizar[8] a imagem obtida e realçar as linhas formadas pelas cristas e sulcos e desta forma fazer com que seja mais fácil identificar as minúcias para binarização da imagem e montagem do *template*.

**Figura 19 – Exemplar (GUMZ, 2002)**

### 3.1.3. Extração

Nesta fase as linhas do exemplar são reduzidas a um único pixel de largura, conforme Figura 20. Para este tratamento são utilizados filtros de imagem, que suavizam as linhas e as

[8] Renderizar – processamento da imagem para obter o resultado final da imagem após aplicação de filtros.

reduzem, facilitando assim a análise computacional da imagem. A suavização tem como objetivo suavizar a imagem original e eliminar ruído existente, verificou-se que o filtro que apresenta melhores resultados é o filtro passa-baixo, pois consegue suavizar a imagem e ao mesmo tempo manter a imagem próxima da imagem original. Em contrapartida, o filtro gaussiano é o filtro que apresenta piores resultados, pois torna a imagem muito desfocada (FONTANA, 2009).

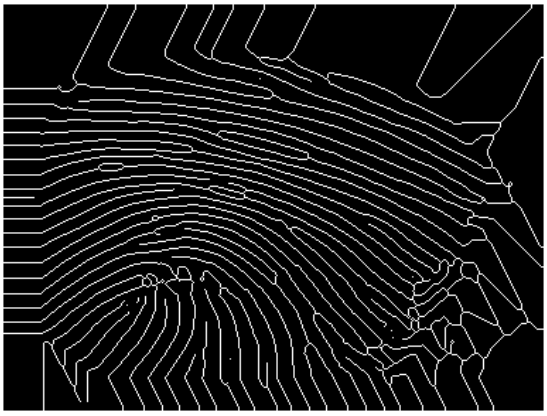


**Figura 20 – Suavização da imagem (COSTA, 2001)**

Fazendo um exame de cada pixel na imagem, se houver um pixel vazio sem vizinhos (sem que existam outros pixels preenchidos ao redor) significa que encontramos um ponto terminal, caso um pixel vazio possua 3 pontos vizinhos preenchidos, significa que encontramos uma bifurcação, conforma apresentado na Figura 21.

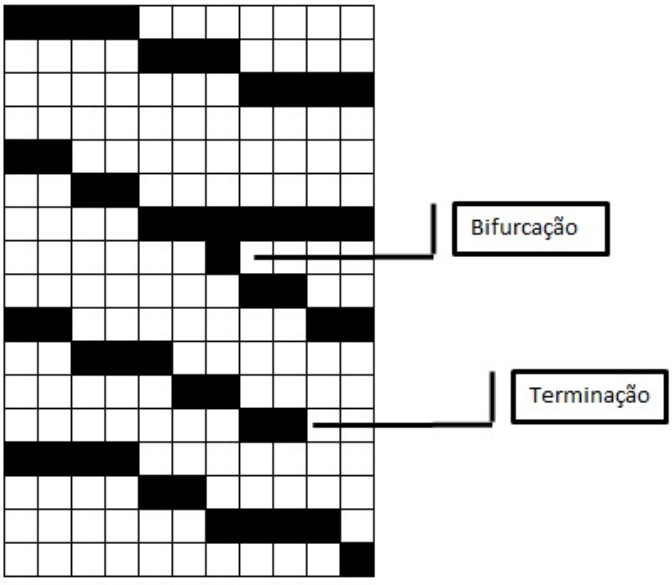



**Figura 21 – Mapeamento dos pixels na binarização (COSTA, 2001)**

O tamanho do pixel varia de acordo com o sensor de obtenção da imagem, o padrão normalmente é de 508 dpi (ASHBOURN, 2000). O processo de binarização é dado pelo diagrama de blocos mostrado na Figura 22.

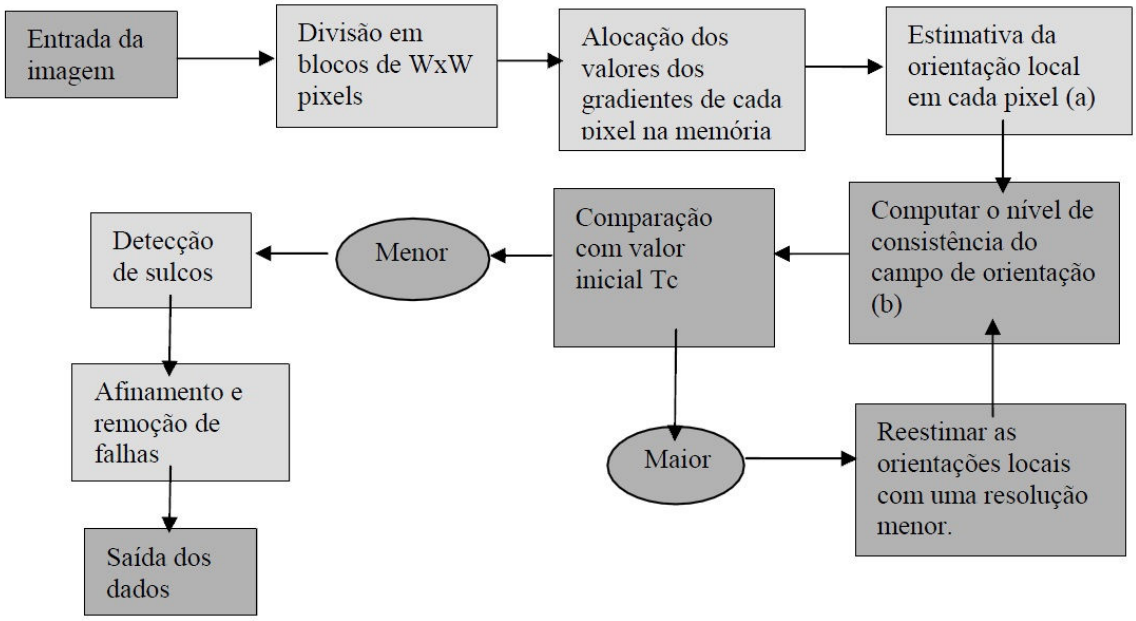



**Figura 22 – Fluxograma de Binarização da imagem (HEMERLY & Peres, 2006)**

A binarização é feita em duas etapas: estimação do campo de orientação e detecção de sulcos e vales, através de um filtro vertical. Dentro do processo de binarização, o trabalho foi desenvolvido até o procedimento de estimativa da orientação local em cada pixel, já que foi considerado que apenas uma impressão digital está presente na imagem. O nível de consistência serve justamente para eliminar pixels de segundo plano. Posteriormente procedeu-se com a detecção de sulcos e as remoções de pequenas falhas sejam das digitais ou decorrentes do processo de binarização (HEMERLY & Peres, 2006).

### 3.1.4. Detecção de Falsas Minúcias

Um erro inevitável em um sistema de reconhecimento de impressões digitais é a detecção de falsas minúcias. Minúcias falsas são inevitáveis devido às distorções existentes tais como cicatrizes, cortes nos dedos e transpiração. A existência de falsas minúcias força a que o processo de comparação as leve em conta. Não é aconselhado que o algoritmo lide com um número excessivo de minúcias, levando a que, após a fase de extração de minúcias, a lista obtida seja analisada de modo a eliminar o máximo de falsas minúcias existentes. Os mecanismos de eliminação de falsas minúcias são essenciais de forma a manter um sistema de identificação eficaz (LOPES, 2009).

Uma das técnicas mais utilizadas para a detecção de minúcias é conhecida como *Crossing Number* (CN), essa técnica foi citada nos trabalhos de Lopes (2009), Costa (2001) e Neves (1996). A técnica de CN determina as propriedades de um pixel contando o número de transições preto e branco existentes na vizinhança do pixel que está sendo processado. O CN de um ponto P é dado pela equação:

$$\boldsymbol{CN = \frac{1}{2}\sum P_i - P_{i+1}}$$

Onde *Pi* é o valor do pixel na vizinhança *P*. *Pi* = (0 ou 1) e i é um ciclo de período 8, ou seja, P9 = P1.

Para um pixel P, denominado pixel central, considera-se oito (8) vizinhos na vizinhança 3x3, sendo que cada pixel pode ter valores zero (0) ou um (1), conforme apresentado na Tabela 1.

**Tabela 1 - Organização dos Pixel na aplicação da técnica Crossing Number**

| | | |
|---|---|---|
| $P_4$ | $P_3$ | $P_2$ |
| $P_5$ | P | $P_1$ |
| $P_6$ | $P_7$ | $P_8$ |

As cristas finais e as cristas bifurcadas em uma imagem de impressão digital são detectadas utilizando-se as propriedades de *Crossing Number*. O valor obtido por essa técnica indica a propriedade do pixel, ou seja, se o pixel é referente a uma crista final, o valor obtido é um (1) ou bifurcada, o valor obtido é três (3). Essas cristas são relatadas para posterior comparação na fase de identificação.

Assumindo-se duas imagens de mesmo tamanho, cujas aquisições foram feitas sob mesma condição de pressão, sem influência de rotação e translação, faz-se o cálculo do *Crossing Number* até que seja satisfeita a condição de similaridade, onde duas minúcias são coincidentes quando localizadas na mesma posição, pertencerem ao mesmo tipo e tem a mesma direção, ou seja, duas minúcias são consideradas pares se seus atributos são próximos uns dos outros.

### *3.1.5. Template* Gerado

A formação do *template* é gerado conforme demonstrado na Figura 23, pelo armazenamento das informações das minúcias colhidas que devem ser armazenadas, levando-se em consideração as falsas minúcias descartadas, ou seja, após a extração das minúcias, estas foram avaliadas e apenas aquelas selecionadas como verdadeiras são armazenadas. Neste modelo são apresentadas as informações relevantes para identificação de cada minúcia colhida, como o tipo e coordenadas utilizadas para identificação. Estas informações são as utilizadas para binarização.

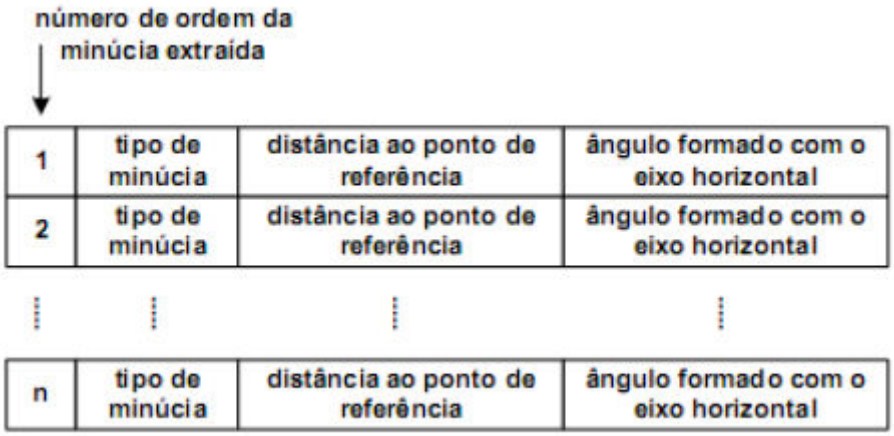



**Figura 23 – Modelo de *template* (LOPES, 2009)**

### 3.1.6. Comparação

O próximo passo para o modelo computacional é a comparação entre o *template* adquirida e o *template* armazenada, em termos de desenvolvimento é a comparação dos pontos de minúcias para obter o índice de similaridade entre duas impressões digitais, conforme apresentado na Figura 24. Para realizar a comparação tem-se como principio o conceito de que duas impressões digitais só serão consideradas idênticas quando apresentarem doze ou mais "pontos característicos", com a mesma configuração e que tenham exatamente a mesma localização, conforme o professor de datiloscopia José Bombonatti da Academia De Polícia Civil do Estado de São Paulo, publicou em seu estudo (BOMBONATTI, 2005).

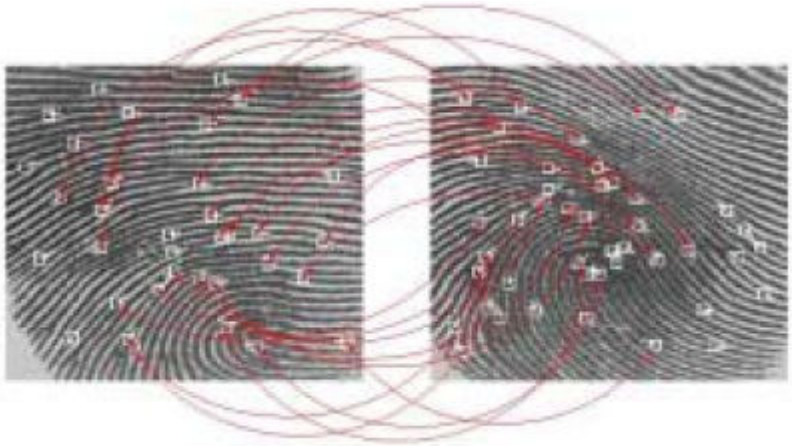


**Figura 24 – Comparação de Minúcias (MAZETTI, 2006)**

A Figura 24 ilustra como esta comparação seria feita graficamente, ou seja, através da imagem propriamente dita. Para a análise através de um sistema computacional algumas características devem ser levadas em consideração:

• Deve-se definir um ponto central na imagem da impressão colhida e este será utilizado como ponto de referência no alinhamento das imagens;

• Para criação do *template*, um vetor é gerado para cada minúcia contendo o seu tipo, coordenadas, ângulo de orientação e qualidade da imagem;

• É utilizada a distância euclidiana entre as minúcias para realização da comparação;

• *Templates* gerados apresentam uma dimensão média de 120 a 350 bytes, conforme características técnicas dos sensores de mercado que geram imagens com resolução de 500 a 600 dpi.

Existem duas formas de efetuar a comparação de 1:1, chamados sistemas de autenticação, ou 1:N, chamados sistemas de identificação, além do módulo de registro, que apenas armazena o *template* no banco de dados.

O sistema biométrico de autenticação autentica a identidade declarada de uma pessoa comparando a característica biométrica capturada com seu próprio "*template*" biométrico armazenado num sistema. Isso conduz a uma comparação "um para um" para determinar se a identidade declarada da pessoa é verdadeira. A pergunta utilizada nesse sistema será: "Eu sou quem declaro ser?" (MAZETTI, 2006).

O sistema biométrico de identificação determina a identidade de uma pessoa sem ela ter declarado um número de identificação ou o nome. Isso conduz a uma comparação "um

para muitos", pois procura num banco de dados inteiro uma identidade compatível. A pergunta utilizada nesse sistema será: "Quem sou eu?" (MAZETTI, 2006). Essas considerações podem ser entendidas conforme o diagrama de bloco apresentado na Figura 25.

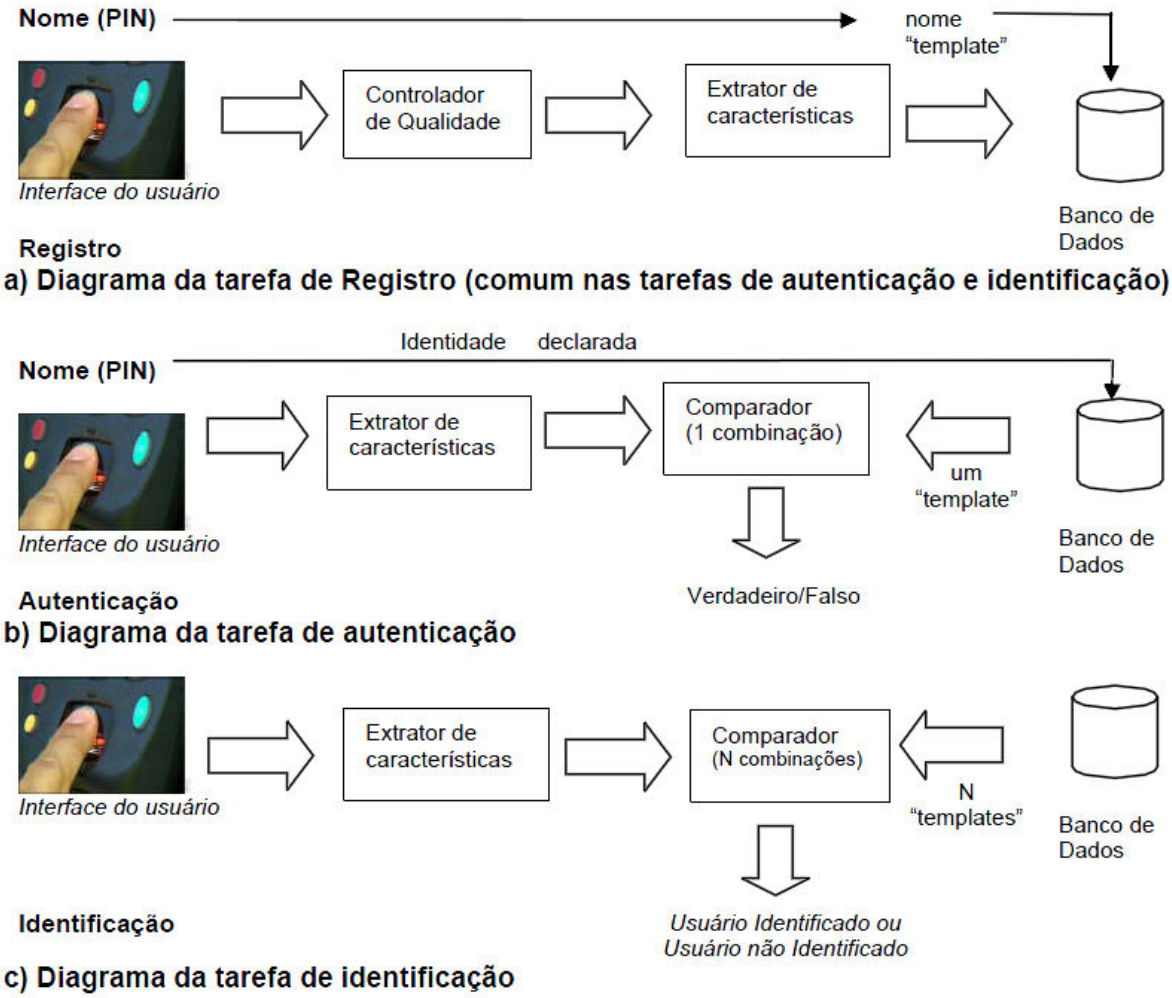



**Figura 25 - Diagramas das tarefas de registro, autenticação e de identificação (MALTONI, MAIO, JAIN, & PRABHAKAR, 2003)**

## 3.2. Avaliação de desempenho

A escolha do(s) método(s) a utilizar depende da análise de risco que necessariamente deve ser feita, relativamente à informação/infraestrutura que se pretende proteger (LIU, 2001). Cada um dos métodos de autenticação pode ser avaliado através de vários parâmetros como o grau de confiabilidade, o nível de conforto, o nível de aceitação e o custo de implantação (LOPES, 2009). O nível de conforto e aceitação são padrões subjetivos, uma vez que dependem do usuário para sua definição. Certamente pode-se afirmar que quanto menos invasivo seja o método, maior será a aceitação do usuário.

O custo total de implantação de um sistema utilizando biometria depende dos seguintes fatores:

• Hardware – tipo de equipamento utilizado. Existem equipamentos com maior ou menor sensibilidade e agilidade na coleta do dado biométrico, que poderá influenciar na velocidade, bem como, na qualidade da coleta, gerando dados com maior ou menor qualidade. Quanto maior a qualidade necessária, maior o custo;

• Software – além da compatibilidade com o hardware escolhido, o grau de confiabilidade e complexidade afetam diretamente ao valor do software desejado. Deve-se tomar cuidado com este item, pois uma arquitetura fechada ou proprietária pode diminuir o custo inicial, mas aumentar futuramente o custo com manutenção;

• Integração com hardware/software – importante que a escolha entre hardware e software sejam feitas com critérios, principalmente porque esta escolha pode afetar a complexidade do projeto, entretanto, é importante que o software seja compatível com mais de um padrão de hardware, uma vez que a aplicação não deve ficar dependente de um único fabricante ou padrão, podendo arruinar o projeto caso o custo do hardware torne-se alto demais ou o equipamento saia de linha;

• Treinamento dos usuários – a confiança do usuário é primordial para a aceitação do projeto; alguns pontos como credibilidade, praticidade e facilidade devem ser levados em consideração. O treinamento é primordial para o sucesso do projeto, uma vez que usuários mal treinados podem não utilizar o sistema de forma adequada e, desta forma, tirar a credibilidade do mesmo. A facilidade de utilização do sistema pode estar ligada a um bom treinamento dos usuários;

• Banco de dados – é importante que o banco de dados seja monitorado e que seja feita manutenção adequada em suas tabelas e índices. Um banco de dados mal cuidado pode perder performance e, desta forma, desestabilizar o sistema. O mecanismo de busca de um sistema biométrico deve estar totalmente otimizado para que o desempenho seja adequado.

A fiabilidade é a característica mais importante de um sistema de identificação biométrico, pois um sistema de reconhecimento biométrico deve ser capaz de identificar um *template* original de uma falta. (LOPES, 2009)

## 3.3. Falsa aceitação x Falta Rejeição (FAR X FRR)

A configuração de um sistema de reconhecimento biométrico, onde são definidos a quantidade de pontos a serem comparados e a quantidade de pontos que devem coincidir para que a identificação seja dada como positiva. O sistema retorna com dois status possíveis: o de reconhecimento ou não, e para cada resultado há duas possibilidades, permitindo assim quatro situações possíveis:

1. Identificação correta ou identificação positiva, o indivíduo foi reconhecido corretamente;
2. Identificação errônea ou falsa identificação, o indivíduo reconhecido não condiz com a realidade;
3. Indivíduo correto é rejeitado;
4. Impostor rejeitado.

A taxa de erro de um algoritmo de identificação pode ser calculada a partir do número de indivíduos corretos que foram rejeitados e quantos impostores foram aceitos. Importante ressaltar que quanto maior número de pontos, apesar da taxa de erro ser menor, o desempenho de processamento, também, é reduzido, ou seja a resposta do sistema é mais lenta. As taxas de erro podem ser definidas através do Índice de Falsas Aceitações – FAR (*False Acceptance Rate*) e o Índice de Falsas Rejeições FRR (*False Rejection Rate*).

O FAR e o FRR são dependentes e inversamente proporcionais, sendo assim quando da configuração de um sistema para um FAR baixo, automaticamente o FRR será alto, pois os critérios de compatibilidade serão mais exigidos. A alta taxa de FRR pode acarretar em baixa conveniência ou facilidade de uso, enquanto a baixa taxa de FAR acarreta em diminuição da segurança. Desta forma é importante chegar a uma configuração balanceada, levando em consideração o nível de segurança desejado e o nível de usabilidade[9] requerido.

Para configuração da tolerância entre as taxas de FAR e FRR deve ser definido pelo sistema um limiar, ou *threshold*, que definirá o número mínimo de coincidências encontrado no algoritmo de comparação para que uma identificação positiva seja realizada.

[9] Usabilidade – facilidade de interação entre o usuário e a interface, quanto maior a usabilidade mais fácil ou interativa é a interface.

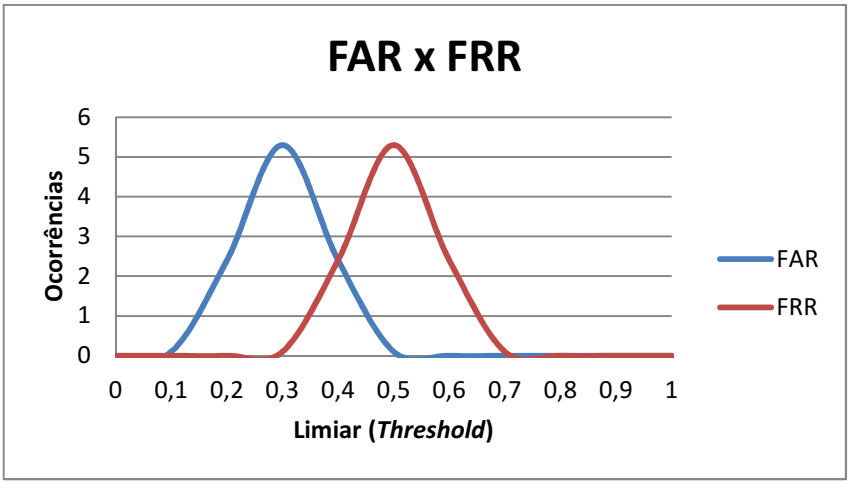



**Figura 26 - FAR x FRR**

### 3.3.1. EER – Equal Error Rate

O algoritmo jamais encontrará duas imagens idênticas, mesmo sendo da mesma impressão digital. Como numa fotografia, a imagem sofre variações a cada captura, ainda que muito pequenas. 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 pertencem à mesma impressão digital. Esta taxa jamais será de 100% e é uma característica de cada algoritmo. A determinação desta taxa é feita a partir da medição de dois parâmetros: a taxa de falso aceite e a taxa de falsa rejeição. 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. Este é um parâmetro importante na avaliação de algoritmos de reconhecimento e identificação de impressão digital. Quanto menor a EER, melhor o algoritmo.

# 4. APLICAÇÃO DO SISTEMA

O sistema desenvolvido foi aplicado em uma Instituição de Ensino Superior – IES em Guarulhos, Faculdade ENIAC, que tinha na época da coleta dos resultados 8079 alunos. A implantação do sistema se deu de forma geral, sendo em todas as turmas. Para esta implantação foram envolvidas as áreas pedagógicas, de sistemas e infraestrutura.

## 4.1. SDK[10] Utilizado

Para este trabalho foi utilizado o SDK da Griaule Biometrics e a escolha foi feita por ser um pacote de desenvolvimento de fácil acesso ao mercado e que oferece todo o suporte ao desenvolvedor (BIOMETRICS, 2008).

A utilização da licença Griaule é independente do sensor a ser utilizado, existem 19 modelos de sensores que podem ser utilizados com estes SDK, além de que é compatível com a ISO 19794-2 e a ANSI 378-2004 que determinam padrões de intercâmbio de dados e interoperabilidade (BIOMETRICS, 2008).

A API[11] da Griaule disponibiliza os mecanismos para captura da imagem através de um sensor biométrico pré-configurado. A partir da imagem da impressão digital é possível extrair a *template* em um padrão genérico que pode ser armazenado onde e como o programador escolher. Também é fornecido o método de comparação entre *templates*, que pode ser configurado através de resolução e uma pontuação de comparação entre minúcias, chamada de *score*. O *score* pode ser obtido no momento da extração na comparação, através do *score* pode-se definir a qualidade da *template* obtida.

[10] Software Development Kit

[11] API - Application Programming Interface (ou Interface de Programação de Aplicativos) é um conjunto de rotinas e padrões estabelecidos por um software para a utilização das suas funcionalidades por aplicativos que não pretendem envolver-se em detalhes da implementação do software, mas apenas usar seus serviços.

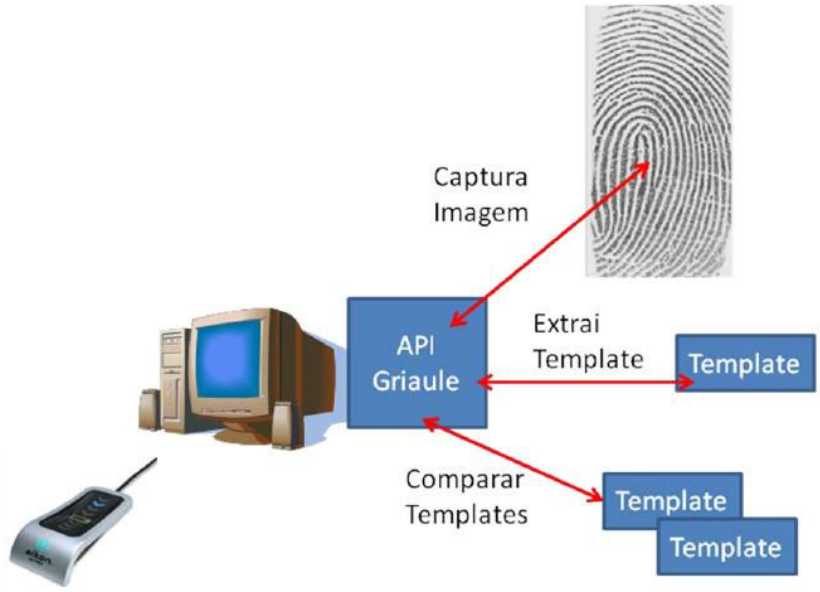



**Figura 27 - Mecanismo de funcionamento da API Griaule (BIOMETRICS, 2008)**

A Tabela 2, mostra as características técnicas que a API Griaule possui.

**Tabela 2 - Características técnicas do SDK (BIOMETRICS, 2008)**

| | |
|---|---|
| Plataforma | Fingerprint SDK para Windows: Windows 2000, Windows XP, Windows 2003, Windows Vista<br>Fingerprint SDK para Java: Windows 2000, Windows XP, Windows 2003, Windows Vista, Linux x86 |
| Velocidade de comparação de identificação (1:N) | Fingerprint Identification SDK: até 35.000 impressões digitais por segundo |
| Velocidade de comparação de verificação (1:1) | 10 milissegundos |
| Velocidade de extração de template | 100 milissegundos |
| Tamanho do template | 900 bytes (média) |
| Banco de Dados | O Fingerprint SDK não utiliza nenhum banco de dados. Os Templates são fornecidos à aplicação do integrador que deve armazená-las conforme decisão do desenvolvedor |
| Resolução da imagem | Recomendada: 500 DPI<br>Mínima: 125 DPI<br>Máxima: 1000 DPI |
| Tamanho da imagem | Mínima: 50x50 pixels<br>Máxima: 500x500 pixels |

## 4.2. Ambiente utilizado

A proposta deste estudo foi viabilizar a utilização da identificação biométrica por impressão digital em sala de aula, onde cada sala é munida de sensor biométrico conectado a um computador em rede, conforme Figura 28, com a possibilidade de consulta a um servidor de aplicação, onde o sistema biométrico está disponibilizado em um banco de dados responsável por armazenar as *templates* dos discentes.

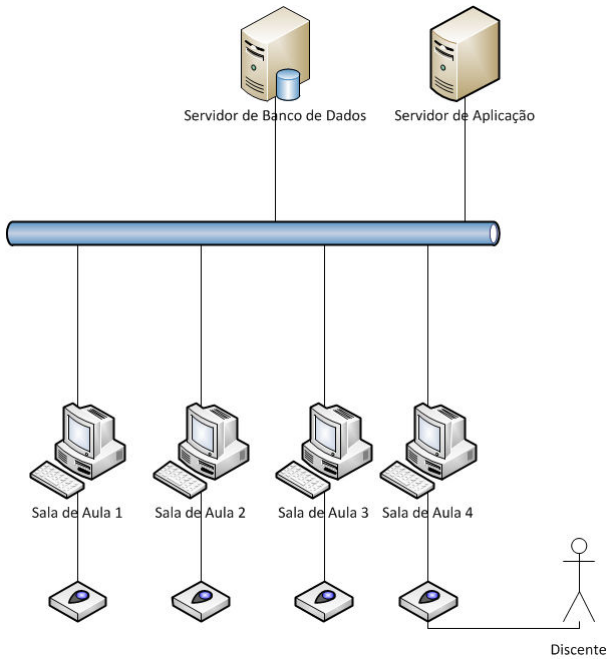



**Figura 28 – Arquitetura Física Proposta**

Os problemas encontrados em ambientes deste tipo é o número de consultas necessárias para identificar um discente e o número de pesquisas concomitantes necessárias para atender a todas as salas de aula. O ambiente considerado no teste é descrito conforme a Tabela 3 (SANCHEZ & MARCELINO, 2011).

**Tabela 3 – Dados do Universo utilizado no trabalho**

| **Número de alunos** | ***Templates* existentes** |
|---|---|
| 8079 | 16329 |

Neste universo a

Tabela 4 indica o ambiente de teste utilizado, correspondente ao turno noturno com o maior número de alunos e salas simultâneas:

**Tabela 4 – Turno com maior utilização do sistema**

| Turno | Salas de Aula | Média de alunos por sala |
|---|---|---|
| Matutino | 20 | 45 |
| Vespertino | 70 | 55 |
| Noturno | 64 | 55 |

Neste ambiente tem-se o total de tempo necessário para identificação de todos os alunos, conforme a expressão (1):

$$t_T = t_r \times \sum P \quad (1)$$

Onde:

$t_T$ – tempo total necessário para realização de todas as pesquisas;

$t_r$ – tempo de resposta para cada pesquisa;

$\sum P$- Total de pesquisas realizadas, que é dado por:

$$\sum Alunos \times \sum Templates$$

Considerando os cálculos estabelecidos, os números já mostrados na Tabela 3 e Tabela 4 e definindo $t_r$=100 ms[12], pode-se calcular o tempo necessário para pesquisas em vários ambientes, conforme a Tabela 5 (SANCHEZ & MARCELINO, 2011).

**Tabela 5 – Descrição do ambiente inicial de estudo**

| Ambiente | $\sum Alunos$ | $\sum P$ [13] | $t_T$ |
|---|---|---|---|
| Em uma sala de aula | 60 | 974.340 | 1.624 min |
| Turno matutino | 900 | 14.615.100 | 24.359 min |
| Turno vespertino | 3850 | 62.520.150 | 104.200 min |
| Turno noturno | 3520 | 57.161.280 | 95.269 min |

[12] Tempo definido na tabela de características técnicas da API da Griaule, confome Tabela 2.

[13] Foram consideradas 16.239 *templates* armazenadas no banco de dados, considerando a busca pela *template* de 1:N em toda a base de dados.

Na Tabela 5 a melhor das hipóteses apresentada seria a coleta de biometria de uma sala de aula por vez, mesmo assim seriam necessárias 974.340 pesquisas por sala, o que demandaria 1.624 minutos por sala, ou seja, aproximadamente 27 horas. Esta situação seria degradada a cada discente acrescentado ao sistema, uma vez que o universo seria aumentado.

Os tempos obtidos com os cálculos a partir do ambiente a ser utilizado e considerando condições ideais de aplicação, já fazem com que a aplicação da biometria em sala de aula seja inviável. A proposta então é diminuir estes tempos de modo a viabilizar a implantação do sistema, considerando que na aplicação real as condições não são ideais, pois deve-se acrescer no processo o tempo de posicionamento do indivíduo para leitura e as possíveis impurezas da impressão digital que pode aumentar a taxa de Falsa Rejeição.

## 4.3. Escolha do Algoritmo

A preocupação com a complexidade de algoritmos é fundamental para projetar algoritmos eficientes. Pode-se desenvolver um algoritmo e depois analisar a sua complexidade para verificar a sua eficiência, mas o melhor ainda é ter a preocupação de projetar algoritmos eficientes desde a sua concepção.

Precisa-se definir alguma medida que expresse a eficiência. Costuma-se medir um algoritmo em termos de tempo de **execução** ou o **espaço** (ou memória) usado, sendo assim temos duas situações:

**Complexidade Espacial**: Quantidade de recursos utilizados para resolver o problema e;

**Complexidade Temporal**: Quantidade de tempo utilizado. Pode ser visto também como o número de instruções necessárias para resolver determinado problema.

Em ambos os casos, a complexidade é medida de acordo com o tamanho dos dados de entrada **n**.

Para este trabalho optou-se pela utilização da solução e escolha do algoritmo através da complexidade temporal, uma vez que o problema apresentado está em função do tempo que será utilizado para encontrar o ***template*** desejada, pois a partir de uma lista tem-se **n** dados a serem comparados, fazendo com que o número máximo de instruções executadas seja o número máximo de elementos no universo selecionado.

### 4.3.1. Complexidade temporal

A complexidade temporal de um programa ou algoritmo tem por definição o tempo que o algoritmo demora em executar sua tarefa, ou seja o seu tempo de execução. O tempo de execução é dado em função do número de elementos de entrada: ***T(n)*** (STEARNS & RICHARD, 1965).

Análise precisa é uma tarefa complicada, pois o algoritmo é implementado numa dada linguagem; a linguagem é compilada e o programa é executado num dado computador, sendo então difícil prever tempos de execução de cada instrução e antever otimizações. Outro ponto é o fato de muitos algoritmos serem "sensíveis" aos elementos de entrada e de muitos algoritmos não serem bem compreendidos.

***Complexidade de Algoritmos – Melhor Caso (Ω)***

Definido pela letra grega Ω (*Ômega*), é o menor tempo de execução em uma entrada de tamanho ***n.*** É pouco usado, por ter aplicação em poucos casos.

Exemplo:

Se tivermos uma lista de **n** números e quisermos encontrar algum deles assume-se que a complexidade no melhor caso é f(n) = **Ω**(1), pois assume-se que o número estaria logo no topo da lista.

***Complexidade de Algoritmos – Caso Médio (Θ)***

Definido pela letra grega Θ (*Theta*), dos três, é o mais difícil de determinar, pois se deve obter a média dos tempos de execução de todas as entradas de tamanho ***n***, ou baseado em probabilidade de determinada condição ocorrer, exemplo:

A complexidade média é $P(1) + P(2) + \cdots + P(n)$

Dado que $P_i = \frac{1}{n};\ 1 \leq i \leq n$

Segue que: $P(1) + P(2) + \cdots + P(n) =$

$$\frac{1}{n} + \frac{2}{n} + \cdots + 1 =$$

$$\frac{1}{n}(1 + 2 + \cdots + n) = \frac{1}{n}\left(\frac{n(n+1)}{2}\right)$$

$$f(n) = \theta\left(\frac{n+1}{2}\right)$$

***Complexidade de Algoritmos – Pior Caso (O)***

Representado pela letra grega O (O maiúsculo - trata-se da letra grega ômicron maiúscula).

É o método mais fácil de obter, baseia-se no maior tempo de execução sobre todas as entradas de tamanho ***n***.

Exemplo:

Se tivermos uma lista de **n** números e quisermos encontrar algum deles, assume-se que a complexidade no pior caso é ***O(n)***, pois assume-se que o número estaria, no pior caso, no final da lista.

***Crescimento das funções***

O crescimento das funções está ligado ao tempo de execução, que geralmente é dependente de um único parâmetro ***n*** (número de elementos), que no caso deste trabalho é representado pelo número de *templates* a serem comparadas.

Os Algoritmos têm tempo de execução proporcional a:

a) ***1*** : muitas instruções são executadas uma só vez ou poucas vezes (se isto acontecer para todo o programa diz-se que o seu tempo de execução é constante);
b) ***log n*** : tempo de execução é logarítmico (cresce ligeiramente à medida que ***n*** cresce; quando ***n*** duplica ***log n*** aumenta mas muito pouco; apenas duplica quando n aumenta para $n^2$);
c) ***n*** : tempo de execução é linear (típico quando algum processamento é feito para cada dado de entrada; situação ótima quando é necessário processar ***n*** dados de entrada, ou produzir ***n*** dados na saída);
d) ***n log n*** : típico quando se reduz um problema em subproblemas, se resolve estes separadamente e se combinam as soluções (se ***n*** é igual a 1 milhão, ***n log n*** é perto de 20 milhões);

e) $n^2$ : tempo de execução quadrático (típico quando é necessário processar todos os pares de dados de entrada; prático apenas em pequenos problemas, ex: produto de vetores);

f) $n^3$ : tempo de execução cúbico (para $n$ = 100, $n^3$ = 1 milhão, ex: produto de matrizes);

g) $2^n$ : tempo de execução exponencial (provavelmente de pouca aplicação prática; típico em soluções de força bruta; para $n$ = 20, $2n$ = 1 milhão; se $n$ duplica, o tempo passa a ser o quadrado).

A Figura 29 apresenta as ordens de complexidade mais comuns:

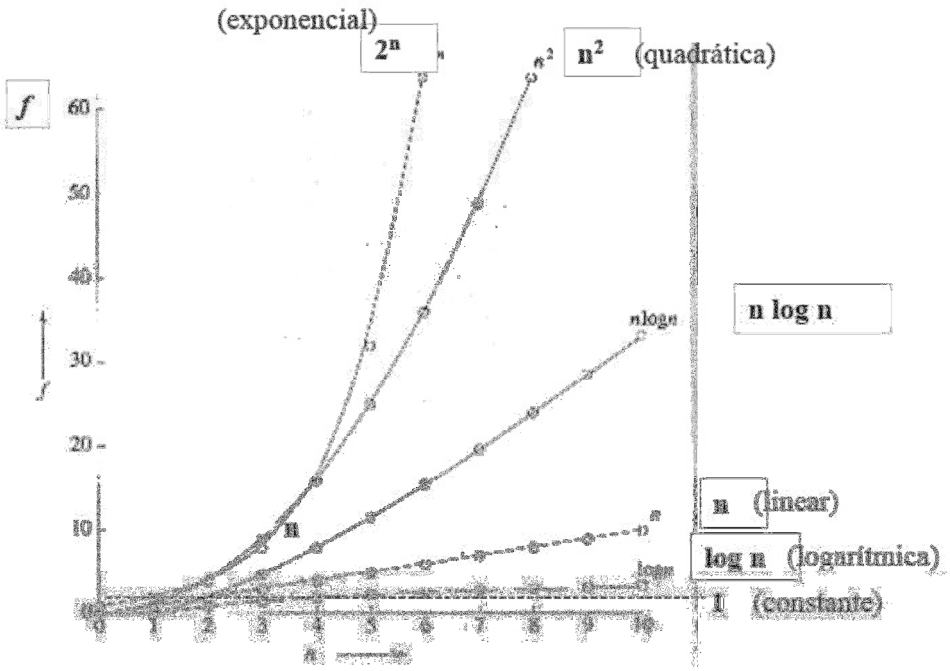



**Figura 29 - Ordens de complexidade mais comuns (STEARNS & RICHARD, 1965)**

Na prática, é difícil, senão impossível, prever com rigor o tempo de execução de um algoritmo ou programa. Para obter o tempo a menos de:

• constantes multiplicativas (normalmente estas constantes são tempos de execução de operações atômicas);

• parcelas menos significativas para valores grandes de $n$;

Identificam-se as operações dominantes (mais frequentes ou muito mais demoradas) e determina-se o número de vezes que são executadas (e não o tempo de cada execução, que seria uma constante multiplicativa).

### 4.3.2. Utilização do Algoritmo de Busca Linear (Busca Sequencial)

A utilização do Algoritmo de busca linear foi escolhida, pois o universo onde os dados são lidos podem estar em qualquer ordem, já que as *templates* biométricas não são indexáveis, isto por se tratar de elementos de dados do tipo *BLOB*[14].

Os dados do universo estão, então, armazenados em uma ordem não rastreável de busca, como, por exemplo, na ordem em que os registros de *templates* foram gravadas, sendo assim a operação de busca por um valor tem que ser exaustiva, ou seja, eventualmente todas as entradas devem ser pesquisadas a fim de determinar se a chave está ou não presente na tabela.

Este procedimento de busca linear está descrito de forma simplificada na Figura 30. Neste algoritmo, os argumentos de entrada são o universo onde a busca será realizada e a chave de busca.

Esse algoritmo começa a analisar o universo a partir da primeira posição, podendo potencialmente analisar todas as posições do universo, sendo que a máxima quantidade de posições analisáveis está restrita ao número de elementos no universo. A chave associada a cada elemento no universo é comparado com a chave de busca. Caso as duas chaves sejam iguais, a entrada foi encontrada e o algoritmo encerra retornando o valor associado à chave para essa entrada. Caso a busca chegue ao final da tabela sem que a chave especificada tenha sido encontrada, o algoritmo encerra retornando o valor especial de não encontrado ou busca nula.

O atrativo desse procedimento é a simplicidade, porém, seu uso é mais eficiente em universos pequenos, pois para universos grandes ele é muito ineficiente, pois o tempo de pesquisa cresce linearmente com o número de elementos no universo, ou seja, o algoritmo apresenta complexidade temporal ***O(n)***.

---

[14] Objetos de dados que armazenam informações multimídias no formato binário em tabelas de banco de dados.

Como ele é um objeto de armazenamento de dados pode ser chamado também de campo de dados.

*Blob* se origina do nome *lob* que *significa Large Object* (objeto grande), sendo então *Binary Large Objetct*.

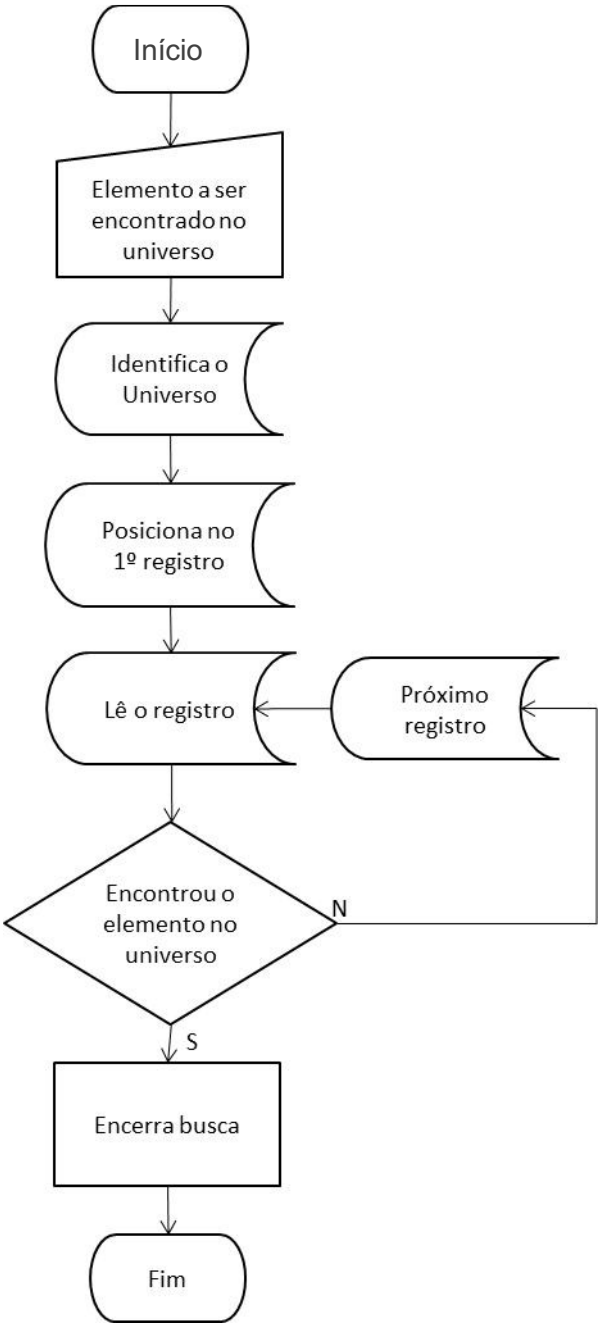



**Figura 30 - Algoritmo de busca linear**

Para que o uso deste algoritmo seja sempre eficiente, foram utilizadas variáveis encontradas no ambiente para que o universo de busca seja sempre o menor possível, conforme será visto na proposta do trabalho.

## 4.4. Proposta do trabalho

A proposta do trabalho visa à criação de um universo de pesquisa único por sala de aula, estabelecendo então uma média de pesquisas, onde independente do universo total de

*templates* armazenado, o tempo de busca se manteria dentro de uma média, podendo até estabelecer-se um tempo médio de pesquisa por aluno. A Figura 31 apresenta a arquitetura proposta, onde é extraída uma base de dados de *template* do banco de dados original e armazenada temporariamente no computador da sala de aula. Esta extração pode ser feita no momento em que o docente aciona o sistema biométrico, a partir daí o sistema verifica as atribuições do docente a partir do horário de aula, e carrega as possíveis *templates* que serão pesquisadas.

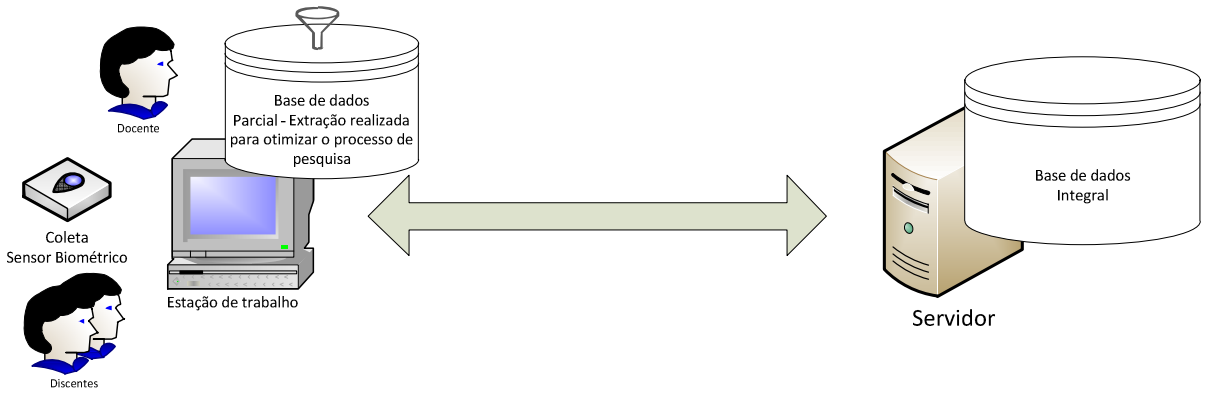



**Figura 31 - Diminuição do ambiente de pesquisa para otimização do processo de pesquisa**

Ao se considerar apenas estas modificações o ganho já seria significativo, conforme apresentado na Tabela 6.

**Tabela 6 – Modificações realizadas no universo de pesquisa para uma sala de aula**

| **Ambiente** | $\sum \boldsymbol{Alunos}$ | $\sum \boldsymbol{P}$ | $\boldsymbol{t_T}$ |
|---|---|---|---|
| Em uma sala de aula | 60 | 3600 | 0,6 min |

Com a redução do universo de pesquisa a otimização do algoritmo linear, para o ambiente proposto é o mostrado na Figura 32.

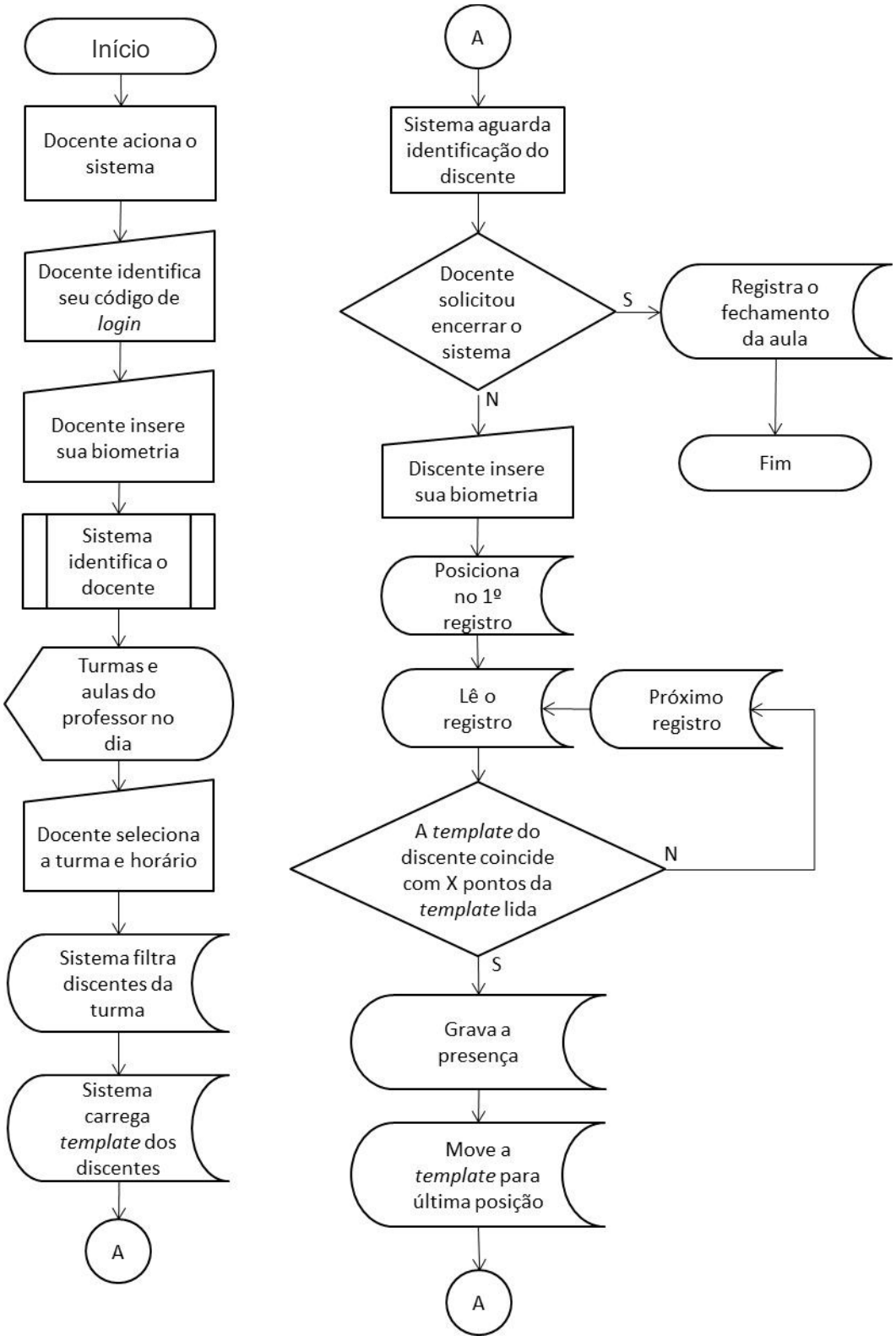



**Figura 32 - Algoritmo proposto**

Além da redução do número de elementos através do isolamento de um universo selecionado, utilizando para isso a informação dos discentes que são esperados para aquela

aula, a cada ciclo de identificação a *template* já lida é posicionada no fim da lista, o que faz com que a cada identificação positiva o universo selecionado seja diminuído em 1 (uma) *template*.

Outro fator estudado foi o número de coincidências necessárias para afirmar o reconhecimento da identidade de um indivíduo. No processo de comparação ou *matching* a aplicação gera uma pontuação ou *score* indicando quantos pontos foram reconhecidos por semelhança, para definir se houve identificação ou não da impressão digital colhida. A aplicação deve ter como parâmetro um limiar a ser considerado, ou seja, o número mínimo de pontos a serem identificados. O aumento ou identificação destes pontos pode influenciar diretamente no tempo de resposta da aplicação. Ao se considerar o número do limiar como número de pontos a serem considerados, ou então fixar um teto de números de pontos a serem considerados, pode-se aperfeiçoar o processo de reconhecimento, uma vez que a comparação de pontos não será mais necessária já que tem-se a identificação do indivíduo.

## 4.5. Aplicação desenvolvida

A aplicação desenvolvida permite que o universo de *templates* a serem utilizados para identificação dos alunos seja restringida a sala de aula em que será colhida a frequência. Para isso são utilizadas as informações cadastradas no sistema de gerenciamento da instituição de ensino, como cadastro do professor e horário de aula. As informações biométricas de alunos e professores foram colhidas anteriormente a esta fase da aplicação.

A identificação da turma é feita através dos dados informados pelo professor. A busca biométrica da identificação do professor é feita no método 1:1, sendo assim o professor deve inserir seu código de acesso e identificar-se através da biometria, conforme a Figura 33. Desta forma o sistema irá localizar a *template* biométrica do professor através do código e apenas comparar se a digital informada pertence mesmo ao professor.


**Figura 33 – Início da aplicação identificação do professor (login)**

Em seguida à identificação do professor, o sistema identifica através da data quais aulas o professor irá ministrar no dia, conforme Figura 34. São apresentadas as informações de hora, turma, curso e disciplina. O sistema poderia ser configurado para abrir diretamente a turma através do horário, neste caso não está configurado desta forma por uma questão de liberdade de configuração do docente.

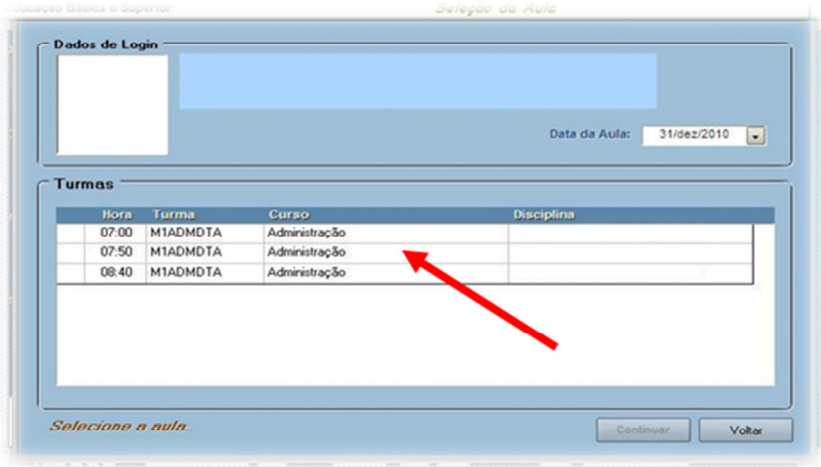



**Figura 34 – Identificação da turma (seleção da aula)**

Escolhida a turma/aula, os alunos da turma selecionada são apresentados, conforme a Figura 35, e o sistema então separa estas *templates* localmente no computador onde o sistema foi aberto para que o reconhecimento biométrico seja feito de forma mais rápida. O isolamento destas informações na estação local otimiza o sistema de busca, fazendo com que haja ganho na identificação do discente.

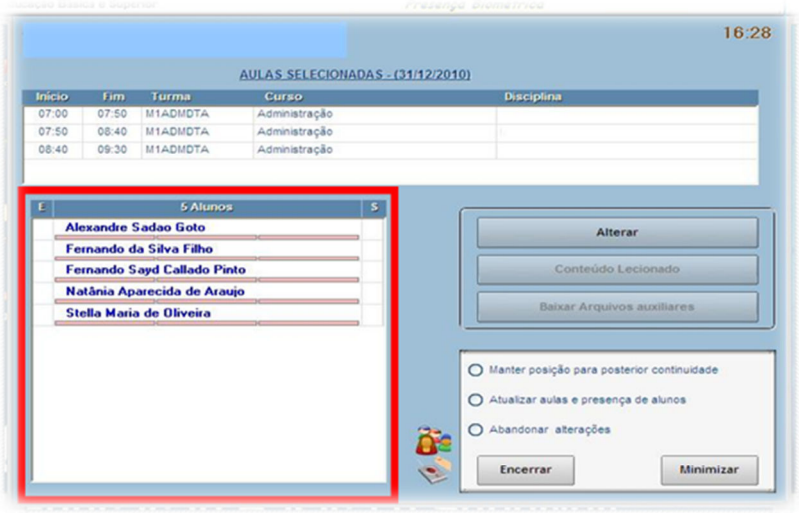



**Figura 35 – Universo de alunos selecionados**

Neste momento o sistema está disponível para que o discente interaja colocando sua digital, pré-cadastrada, no leitor biométrico que irá identificá-lo automaticamente e registrar sua presença na sala de aula, conforme apresentado na Figura 36. As informações de frequência são armazenadas automaticamente no servidor de rede, mantendo a informação segura.

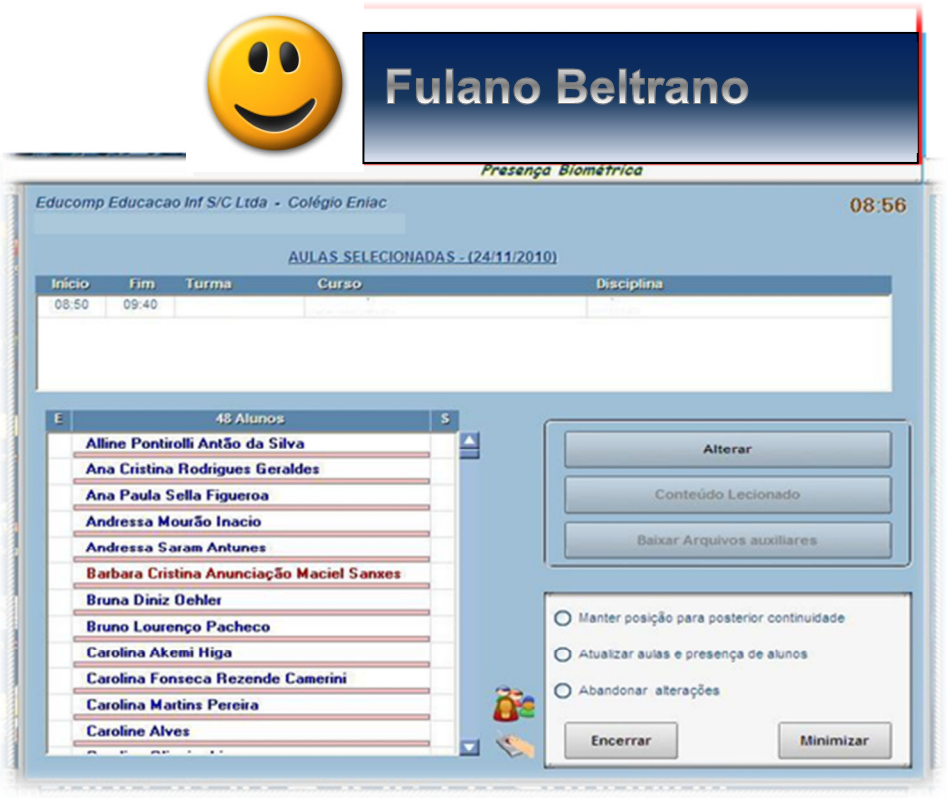



**Figura 36 – Identificação do aluno**

O professor pode fechar a biometria após a coleta inicial e reabrir depois, para isso ele deve fechar o sistema utilizando a opção “Manter posição para posterior continuidade”, as informações de coleta ficam armazenadas, mas não atualizam o histórico do aluno. Para que as informações de frequência sejam atualizadas no banco de dados o professor deve utilizar a opção “Atualizar aulas e presença de alunos”, desta forma o professor não mais poderá reabrir a biometria deste dia. Caso o professor queira cancelar a coleta feita ele deve utilizar a opção “Abandonar alterações”.

# 5. RESULTADOS

Os resultados obtidos após implantação do sistema proposto se mostraram satisfatórios. A, mostra que a solução proposta ao problema atingiu seu objetivo. Em 90% dos casos o número de alunos identificados antes dos 15 minutos de aulas iniciais foram superiores a 85%. Este resultado se mostra satisfatório, pois foi comprovado também que cerca de 20% dos alunos não chegam antes dos 15 minutos iniciais de aula, este dado foi possível de ser apurado, pois a instituição onde foi instalado o sistema possui catracas de acesso, sendo assim foi possível apurar a quantidade de alunos que chegam a instituição neste intervalo de tempo. Um dado importante que foi considerado nas constatações, é que nem sempre o aluno ao chegar na instituição se dirige diretamente a sala de aula, esta informação foi obtida através do intervalo entre a passagem na catraca de acesso e o registro da frequência na sala de aula.

## 5.1. Parâmetros utilizados

### 5.1.1. Pontos de coincidência

Para parametrização do sistema de modo a ajustar os índices de Falsa Aceitação x Falta Rejeição foi utilizado o número de 35 pontos de coincidência na biometria, desta forma não foram identificados nenhuma falsa aceitação, entretanto o índice de falsa aceitação foi de cerca de 3%, ou seja, para o universo total implantado de 8079 discentes, foram rejeitados 243 discentes.

No caso dos 243 discentes que foram impossibilitados da identificação por impressão digital, notou-se que em sua maioria estes possuíam algum tipo de deformação em suas digitais, sendo os principais motivos:

a. Alunos do curso de engenharia que trabalham com materiais corrosivos apresentaram perda parcial ou total de sua digital, o que impossibilitou a identificação de suas digitais, cerca de 1,5% (132 discentes);
b. Cerca de 1% do universo, 81 discentes, apresentaram má formação da digital, nestes casos a pele apresentou ser extremamente fina e com aspecto brilhoso;

c. Os demais casos apresentaram problemas com cicatrizes, cortes, alergias e outros tipos de deformações que impossibilitaram a leitura da impressão digital.

Para estes casos de rejeição o sistema foi adaptado para que o professor pudesse intervir e inserir manualmente a presença para estes discentes.

### 5.1.2. Registro da frequência

O sistema pode ser parametrizado para registrar a frequência do aluno uma vez ao dia, ou ao entrar e sair, também podem ser configurados os limites de horário em minutos para que o aluno ganhe presença ou falta na aula, estes limites são configurados para o início e fim da aula.

Para a situação aplicada, a coordenação e o corpo docente da instituição parametrizou o sistema para que a presença do aluno fosse atribuída com as seguintes regras parametrizadas:

a. Ao chegar no início da aula, o aluno deve registrar a biometria. O sistema acolhe a presença da primeira aula com tolerância de até 15 minutos do início oficial, observando que o horário válido é o visualizado na interface da biometria;
b. Se por acaso o aluno não conseguir registrar até os 15 minutos tolerados pelo sistema, ele pode – a critério do professor - fazer a biometria a qualquer momento. Entretanto, terá perdido a primeira aula do dia;
c. No término da aula, o aluno deverá fazer a biometria para que o sistema possa processar o tempo de permanência em aula. É importante seguir o horário de saída. Caso ele faça a biometria antes do horário regimental, levando em conta a tolerância de 15 minutos, perderá o registro de frequência da última aula;

Exemplos de um aluno que tem seu horário das 18h às 20h30 (Noite I):

**Exemplo 1** – Aluno chegou às 18h30, fez a biometria na entrada e depois no horário de saída às 20h.

***Conclusão*:** Atrasou-se na entrada e antecipou-se na saída. Com isso o sistema não computou sua presença, e foram registradas três faltas.

**Exemplo 2** – Aluno chegou às 18h10, fez a biometria na entrada e depois no horário de saída às 20h25.

***Conclusão***: Embora o aluno tenha se atrasado por 10 minutos na entrada, ainda ficou dentro da tolerância e saiu na tolerância permitida. Com isso o sistema considerou presença nas três aulas.

**Exemplo 3** – O aluno chegou às 18h17, NÃO fez a biometria na entrada e fez depois no horário de saída às 20h30.

***Conclusão***: O aluno, ao atrasar-se mais do que os 15 minutos tolerados, perdeu a primeira aula, entretanto saiu no horário regimental. Com isso o sistema considerou presença nas duas últimas aulas.

## 5.2. Visão dos docentes

Os docentes em geral aprovaram a utilização do sistema para apuração da frequência dos discentes. Em geral o fato da aprovação se deu pelo motivo de a responsabilidade do registro passar diretamente ao discente, sendo que o mesmo deve estar em sala de aula no horário estipulado para registrar a sua frequência.

A alteração do sistema para que o docente pudesse registrar a frequência dos discentes com problemas na leitura de sua impressão digital agradou principalmente porque a mesma solução serviu para que os docentes, mantendo sua soberania em sala de aula, pudessem retirar a frequência daqueles alunos que chegaram no final da aula ou não se mantiveram na sala de modo a justificar a sua frequência.

Na visão dos docentes o sistema de controle de presença visa estimular a participação cada vez maior de alunos e professores em sala de aula, bem como é uma medida de segurança, pois favorece a circulação de alunos em grupo para o retorno às suas residências, coibindo eventual ação de marginais.

## 5.3. Descrição dos resultados

A apresenta os resultados apurados na implantação do sistema. Para montagem da tabela foram utilizados os meses de março e abril, pois representam no 1º semestre o pico de alunos, ou seja, números de alunos estáveis para serem comparados, devido a ser o meio do semestre.

**Tabela 7 - Resultados apurados**

| Turmas/Disciplinas | 20:40-20:55 | | 20:56-21:10 | | 21:10-21:25 | | Total Alunos |
|---|---|---|---|---|---|---|---|
| | Alunos | % | Alunos | % | Alunos | % | |
| **N2BASICOH** | **329** | **87,50%** | **47** | **12,50%** | | **0,00%** | **376** |
| **Comunicação Empresarial** | | | | | | | |
| 31/03/2011 | 40 | 78,43% | 11 | 21,57% | | 0,00% | 51 |
| 07/04/2011 | 33 | 58,93% | 23 | 41,07% | | 0,00% | 56 |
| 14/04/2011 | 44 | 88,00% | 6 | 12,00% | | 0,00% | 50 |
| **Organização e Processos Gerenciais** | | | | | | | |
| 16/03/2011 | 54 | 98,18% | 1 | 1,82% | | 0,00% | 55 |
| 23/03/2011 | 51 | 96,23% | 2 | 3,77% | | 0,00% | 53 |
| 13/04/2011 | 55 | 93,22% | 4 | 6,78% | | 0,00% | 59 |
| **N2PIPROA** | **164** | **78,47%** | **39** | **18,66%** | **6** | **2,87%** | **209** |
| **Projeto de Produtividade** | | | | | | | |
| 05/04/2011 | 34 | 66,67% | 14 | 27,45% | 3 | 5,88% | 51 |
| 19/04/2011 | 42 | 77,78% | 9 | 16,67% | 3 | 5,56% | 54 |
| 25/04/2011 | 35 | 68,63% | 16 | 31,37% | | 0,00% | 51 |
| 26/04/2011 | 53 | 100,00% | | 0,00% | | 0,00% | 53 |
| **N2GQPROA** | **164** | **78,47%** | **39** | **18,66%** | **6** | **2,87%** | **209** |
| **Projeto de Produtividade** | | | | | | | |
| 05/04/2011 | 34 | 66,67% | 14 | 27,45% | 3 | 5,88% | 51 |
| 19/04/2011 | 42 | 77,78% | 9 | 16,67% | 3 | 5,56% | 54 |
| 25/04/2011 | 35 | 68,63% | 16 | 31,37% | | 0,00% | 51 |
| 26/04/2011 | 53 | 100,00% | | 0,00% | | 0,00% | 53 |
| **N2PIGQA** | **164** | **78,47%** | **39** | **18,66%** | **6** | **2,87%** | **209** |
| **Projeto de Gestão da Qualidade** | | | | | | | |
| 05/04/2011 | 34 | 66,67% | 14 | 27,45% | 3 | 5,88% | 51 |
| 19/04/2011 | 42 | 77,78% | 9 | 16,67% | 3 | 5,56% | 54 |
| 25/04/2011 | 35 | 68,63% | 16 | 31,37% | | 0,00% | 51 |
| 26/04/2011 | 53 | 100,00% | | 0,00% | | 0,00% | 53 |
| **N2GQGQA** | **164** | **78,47%** | **39** | **18,66%** | **6** | **2,87%** | **209** |
| **Projeto de Gestão da Qualidade** | | | | | | | |
| 05/04/2011 | 34 | 66,67% | 14 | 27,45% | 3 | 5,88% | 51 |
| 19/04/2011 | 42 | 77,78% | 9 | 16,67% | 3 | 5,56% | 54 |
| 25/04/2011 | 35 | 68,63% | 16 | 31,37% | | 0,00% | 51 |
| 26/04/2011 | 53 | 100,00% | | 0,00% | | 0,00% | 53 |

A Tabela 7 apresenta o movimento de alunos nos primeiros 45 minutos de aulas, as aulas consideradas são de 150 minutos. São apresentados os alunos registrados entre as 20h45 min e 20h55 min, entre as 20h56 min e 21h10 min e entre as 21h10 min e 21h25 min. E a última coluna representa quantos alunos estiveram presentes no dia. A análise dos três primeiros quinze minutos visa mostrar a viabilidade da aplicação do sistema, uma vez que 15 minutos, é considerado um tempo viável para apuração da frequência, conforme reunião com docentes.

Na amostragem apresentada na  pode-se ver que o resultado foi satisfatório, uma vez que mais de 80% da sala, na média, efetua a biometria antes dos primeiros 15 minutos de aulas e em média 97% da sala já haviam efetuado o registro de presença nos primeiros 30 minutos. Para analisar estes dados temos que levar em consideração que nem todos os alunos chegam antes do início da aula e parte dos alunos chegam após os primeiros 15 minutos de aula.

Já a Figura 37 nos mostra que quando levado para o universo total estudado de 8079 alunos, considerando o intervalo de 01 de fevereiro de 2011 e 10 de maio de 2011, 83,87% do corpo discente realizam a biometria nos 15 primeiros minutos de aula, enquanto aproximadamente os mesmos 97% realizam a biometria do dia nos trinta primeiros minutos de aula (sendo 83,87% nos primeiros 15 (quinze) minutos e 13,08% nos seguintes 15 (quinze) minutos).

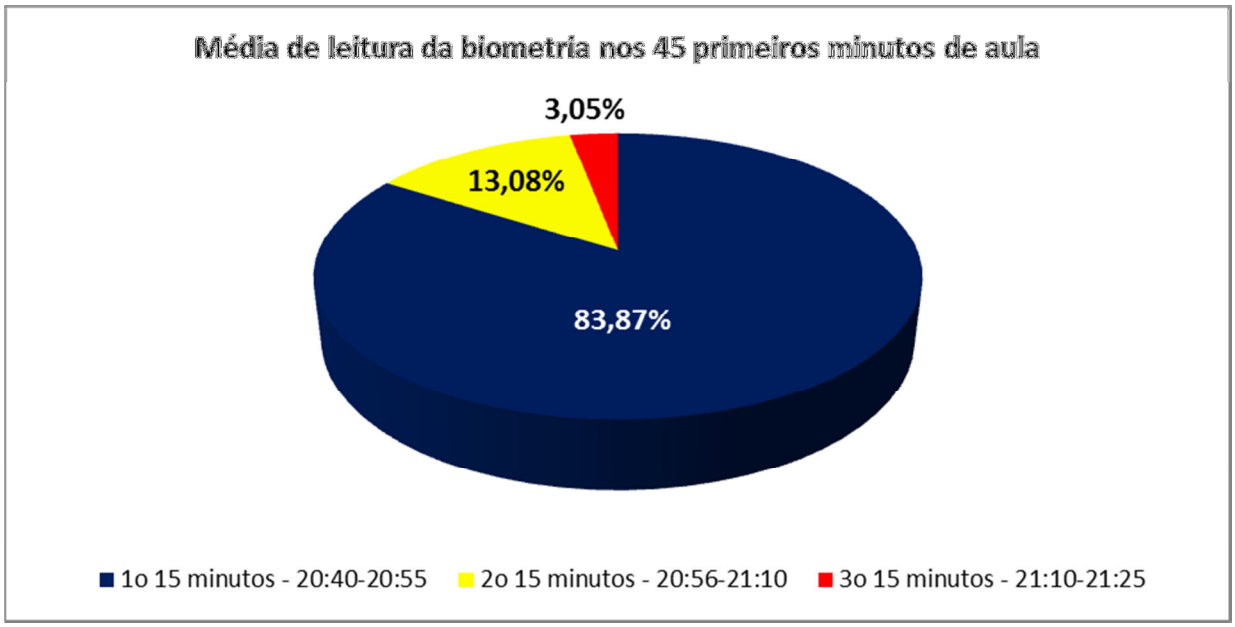



**Figura 37 - Gráfico de resultados**

## 5.5. Discussão dos resultados

Para obtenção destes resultados foram necessários 4 anos de trabalhos, sendo 1 ano para desenvolvimento da ferramenta. A aceitação por parte dos discentes foi boa, não houve qualquer tipo de retaliação ou rejeição, entretanto foram necessárias épocas de adaptação, avisos contínuos e uma comunicação boa entre coordenação e professores com os discentes.

Já por parte dos docentes foram necessárias algumas alterações, conforme já citado neste trabalho, mas, também, tornou-se necessário uma campanha de conscientização e treinamentos intensivos sobre o uso da biometria. Um aspecto importante é o treinamento do professor para utilização do recurso completo em sala de aula, conexão de cabos, ajuste de monitor e até separação entre o monitor da mesa do professor e a projeção, pois com isso o mesmo computador é utilizado para o ministério da aula e a coleta da biometria simultaneamente, sem que um interfira no outro.

Houve problemas de *performance* na implantação da ferramenta, devido a busca dos *templates* diretamente no servidor, para solução, como já tratado anteriormente, criou-se uma cópia dos *templates* dos discentes na máquina local, enquanto o sistema está em funcionamento, desta forma logo que o professor abre o software de coleta e seleciona a turma, os *templates* daquela turma são baixadas localmente e então quando o aluno se identifica a busca fica sendo local e não na rede. Estes *templates* são criados em arquivos temporários que são apagadas logo que o professor encerra a aplicação.

# 6. CONCLUSÕES

A aplicação do algoritmo de busca linear em universos limitados de *templates* permitiu que fosse estipulado um tempo padrão de resposta para o sistema de identificação biométrica, uma vez que o número de pesquisas ao banco de dados sempre será conhecido, conforme o universo estipulado de uma sala de aula não importando o número de alunos. É importante considerar que mesmo que o universo dobre, o tempo aumentado será relativamente curto, comparado ao de pesquisa ao universo total. Desta forma o objetivo geral deste processo foi alcançado com êxito, pois o sistema de busca a universos limitados, filtrados por variáveis de ambiente, irá manter a estabilidade do sistema, pois este processo permitiu a distribuição do processamento do sistema biométrico entre várias estações da instituição, aumentando a *performance* do sistema e diminuindo a necessidade de potência no servidor de banco de dados e de aplicação, uma vez que uma simples estação pode executar o processo de comparação (*matching*) das *templates* com performance superior ao processamento centralizado.

Com a definição de um número de pontos limiar e de teto para efetuar a comparação de pontos da *template* diminuindo o custo de pesquisa e otimizando o processo de reconhecimento biométrico utilizado, foi possível configurar o sistema para que fosse utilizado apenas 35 pontos de coincidência, sendo que nenhuma ocorrência de falta aceitação foi identificada e o número de falsas rejeições foi diminuído consideravelmente.

A utilização da biometria permitiu que cada discente pudesse ser identificado de forma única e íntegra, uma vez que a fraude deste tipo de informação traz maiores dificuldades do que assinar a lista ou registrar a presença em um diário. A identificação eletrônica e automática permitiu a disponibilização da informação de forma on-line eliminando o trabalho da secretaria de digitação das informações contidas no diário, uma vez que o sistema se auto alimenta. A qualidade das informações coletadas, bem como a confiabilidade da informação disponibilizada teve significativo aumento, uma vez que foi eliminada a possibilidade de erro de digitação.

A aceitação de todo o corpo docente e discente foi bastante positiva, uma vez que todos entenderam a importância da automação, as facilidades de registro, o tempo economizado em processamento e a rapidez e confiabilidade com que as informações passaram a ser geradas.

Com certeza os resultados obtidos foram acima da expectativa e alcançaram todos os objetivos do trabalho. Para uma sequência deste trabalho seria muito interessante o desenvolvimento de um kit de desenvolvimento (SDK) próprio, onde pudesse criar um padrão novo de *templates* e assim poder aplicar outros tipos de filtros, o que poderia reduzir ainda mais o tempo de pesquisa, como por exemplo, a classificação das *templates* entre os cinco tipos de impressões digitais Arco Plano, Arco Angular, Presilha Interna, Presilha Externa e Verticilo, ou então classificar a biometria pela maior ou menor incidências de tipos de minúcias.

Outra sequência possível para este trabalho é a adaptação do sistema de frequência de sala de aula para o acesso a Instituições de Ensino Superior (IES) utilizando um algoritmo de 1:N, este algoritmo poderia ser otimizado com a utilização de estatísticas de chegada de discentes, poderia ser utilizado o turno de entrada e depois a estatística de chegada na instituição por cada aluno.

# REFERÊNCIAS


ARAÚJO, E. C. (2009). *A BIOMETRIA COMO MECANISMO SEGURO DE IDENTIFICAÇÃO E AUTENTICAÇÃO DE INDIVÍDUOS EM SISTEMAS DE INFORMAÇÃO.* Instituto de Educação Superior de João Pessoa. JOÃO PESSOA - PB: FATEC-PB.

ASHBOURN, J. (2000). *Biometrics: Advanced Identity Guide The Complete.* London: Springer-Verlag.

BIOMETRICS, G. (2008). *Griaule Biometrics*. Acesso em 04 de 2011, disponível em http://www.griaulebiometrics.com/en-us/fingerprint_sdk/features#biometrics_for_all

BOMBONATTI, J. (2005). *História da Datiloscopia.* Acesso em Dezembro de 2010, disponível em Departamento de Odontologia Social - Universidade de São Paulo: http://www.fo.usp.br/departamentos/social/legal/historia_dactiloscopia.htm

CAMPESTRINI, J. R. (2003). *AUTENTICAÇÃO SEGURA UTILIZANDO BIOMETRIA.* UNIVERSIDADE DA REGIÃO DE JOINVILLE – UNIVILLE., Mestrado Profissional em Bacharelado em Sistemas de Informação. JOINVILLE: UNIVERSIDADE DA REGIÃO DE JOINVILLE – UNIVILLE.

CEZAR, G. (Abril de 2001). *Hora da Prova Biológica*. (VIEIRA, Editor) Acesso em Dezembro de 2010, disponível em CSO Online: http://www.csoonline.com.br

CONSORTIUM, B. (2006). *Introduction to Biometrics*. Acesso em DEZEMBRO de 2010, disponível em http://www.biometrics.org/intro.htm

COSTA, S. M. (2001). *Classificação e verificação de impressões digitais.* UNIVERSIDADE DE SÃO PAULO. USP.

CURADO, M. (2006). Pessoas transparentes, Base de dados e Biometria.

DOS SANTOS, A. L. (2007). *Gerenciamento de Identidades.* Brasport.

FONTANA, D. R. (2009). *Sistema de Autenticação/Identificação pessoal biométrica através da palma da mão com o auxílio de redes neurais artificiais.* Instituto Tecnológico de Aeronáutica.

GUMZ, R. A. (2002). *Protótipo de um sistema de identicão de minúcias em impressões digitais utilizando redes neurais artificiais feedforward multicamada.*

HEMERLY, E. M., & Peres, T. M. (2006). PROCESSAMENTO DIGITAL DE IMPRESSÕES DIGITAIS. pp. p. 5, Figura 4.

HENRIQUE, L. (26 de 06 de 2009). *Mini Curso de Biometria utilizando o Eikon D2 PRO.* Acesso em 04 de 2011, disponível em DUODIGIT: http://www.duodigit.com.br

HONG, L., & JAIN, A. (1998). Fingerprint Image Enhancement: Algorithm and Performance Evaluation. In: L. HONG, & A. JAIN, *IEEE Transactions on Pattern Analysis and Machine Intelligence* (pp. pp. 777-789). IEEE.

JAIN, A., PRABHAKAR, S., & PANKANTI, S. (2002). *On the similarity of identical twin fingerprints.* Pattern Recognition Society.

KEHDY, C. (1968). *Elementos de criminalística* (3.ed. ed.). São Paulo: Sugestões Literárias.

LIU, S. e. (2001). A Practical Guide to Biometric Security. In: S. e. LIU, *A Practical Guide to Biometric Security* (pp. p. 27-32). IT Pro.

LOPES, B. M. (2009). *Modelos Computacionais para Sistemas Automáticos de Identificação de Impressões Digitais.* Universidade de Lisboa, Departamento de Informática. Lisboa: Universidade de Lisboa.

MALTONI, D., MAIO, D., JAIN, A., & PRABHAKAR, S. (2003). *Handbook of Fingerprint.* New York: Springer-Velag.

MARANHÃO, O. R. (1989). *Curso Básico de Medicina Legal.* São Paulo: Revista dos Tribunais.

MAZETTI, C. M. (2006). Metodologia para extração de características invariantes à rotação em Imagens de Impressões Digitais. São Carlos: UNIVERSIDADE DE SÃO PAULO.

NEVES, S. G. (1996). *Classificação e Identificação de Impressões Digitais.* Teste de Mestrado, Universidade Federal do Rio Grande do Sul.

PINHEIRO, J. M. (2008). *Biometria nos Sistemas Computacionais - Você é a senha.* Rio de Janeiro: Ciência Moderna.

SANCHEZ, M. P., & MARCELINO, M. A. (2011). APLICAÇÃO DA BIOMETRIA NA APURAÇÃO DE FREQUÊNCIA EM IES. *REVISTA SODEBRAS, 6*(No 69).

SENIOR, A. e. (2002). Fingerprint minutiae: a Constructive Definition.

STEARNS, J. H., & RICHARD, E. (1965). *On the computational complexity of algorithms.* Trans. American Mathematical Society.

ZHAO, F., & TANG, X. (2002). Preprocessing for skeleton-based fingerprint minutiae extration. pp. p. 742-745.