

Um Estudo do Processo de Reconhecimento de Indivíduos pelo Método da Impressão Digital

Alexandre de O. Zamberlam, Marta R. Bez, Paulo R. Ferreira Jr, Luis E. Pettinari Acuña, Paulo R. M. Barros

Grupo de Pesquisa em TI, Centro Universitário Feevale Novo Hamburgo, RS, Brasil.
E-mails: {alexz, martabez}@feevale.br; paulo.ferreira.jr@gmail.com; lpettina@hotmail.com; pbarros@comusa.com.br

Resumo

Este artigo apresenta os conceitos fundamentais em torno do tema biometria, com ênfase na biometria da impressão digital. São demonstradas as fases do processo de verificação/identificação de indivíduos num sistema informatizado com o uso de impressões digitais. Além disso, é apresentado um estudo dos principais trabalhos encontrados na literatura, classificando-os de acordo com o método empregado, com destaque para o método de detecção por minúcias, que é amplamente explorado, demonstrando-se os algoritmos utilizados para ele. Para a fase de comparação de minúcias, são abordados os principais métodos utilizados.

Palavras-chave: Sistemas de Reconhecimento, Impressão Digital, Processamento de Imagens.

Abstract

This paper presents the fundamental concepts regarding the biometry subject, focused on the fingerprint biometry. We demonstrate the phases of individual's identification/verification through a computer system using their fingerprints. Besides, we present an overview of the main works available on the literature, classified according the used methods, emphasizing the minutiae based one. This method is widely applied and we will discuss its algorithm in details. We also show the main methods of minutiae comparison.

Keywords: Recognition Systems, Fingerprint, Images Processing.

Introdução

A segurança é uma preocupação em ambientes com acesso restrito. Tais ambientes podem ser os mais variados possíveis: prédios, salas, sistemas, máquinas, etc. - e os acessos, tanto físicos quanto virtuais. Inseridos nesse contexto, surgem os sistemas biométricos como uma forma ágil e precisa de garantir um nível mais elevado de segurança no processo de reconhecimento de usuários.

Segundo Costa (2001), sistemas biométricos são sistemas que manipulam características físicas ou comportamentais, consideradas únicas, mensuráveis e que possibilitam identificar pessoas. Conforme Romagnoli (2002), os indivíduos possuem algumas dessas características que podem ser identificadas, como, por exemplo, a digital, a retina, a íris, a formação da face, a geometria da mão, o DNA, a voz, assinatura, entre outros. A diferença em relação às outras formas de identificação, como a senha ou o cartão de acesso, é que não se pode perder ou esquecer tais características biométricas, pois é exigida a presença do usuário no ato do reconhecimento.

Para que uma característica física ou comportamental possa ser utilizada como característica biométrica [Muniz, 2004], deve satisfazer os seguintes requisitos:

- universalidade: todos os seres humanos devem possuir essa característica;
- singularidade: essa característica não pode ser igual em pessoas diferentes;
- permanência: a característica não pode variar com o tempo;
- mensurabilidade: a característica pode ser medida.

Atualmente, o sistema biométrico mais difundido é o de Identificação Digital, por ser o mais acessível no que se refere a *hardware*, *software*, implementação, manutenção, etc. Entretanto, apesar das inúmeras pesquisas realizadas nos mais variados centros de desenvolvimento tecnológico, dos produtos existentes no mercado, ainda há problemas relacionados ao processo de identificação de usuários pela digital. Esses problemas estão no âmbito:

- da qualidade do leitor/*scanner*;
- dos algoritmos/técnicas de tratamento da imagem;
- dos algoritmos/técnicas de extração e classificação de minúcias;
- do desempenho e portabilidade desses sistemas.

Dessa forma, para compreender a idéia de sistemas biométricos, por meio de impressões digitais, bem como seu funcionamento, este texto trata os principais conceitos e técnicas relacionadas ao processo de manipulação de impressões digitais. Finalmente, para melhor entendimento do trabalho, o artigo está dividido em 5 seções: a seção 2 descreve o método da impressão digital pesquisado e utilizado atualmente, esclarecendo seus fundamentos conceituais baseados em alguns autores da área. A terceira seção apresenta alguns trabalhos na área de reconhecimento de usuários pelo uso da impressão digital, detalhando seus principais algoritmos que auxiliam tanto no melhoramento de imagens quanto na extração de minúcias. Na seção 4, é abordada a etapa de comparação de minúcias, apresentando trabalhos realizados. E, na última seção, são apresentadas as considerações sobre o estudo.

1 Método Biométrico da Impressão Digital

Conforme Yang (2003), sistemas de reconhecimento biométrico oferecem maior segurança e praticidade do que os métodos tradicionais de reconhecimento pessoal, baseados em usuário e senha, pois estes já não satisfazem às demandas exigidas. Os métodos biométricos são aplicados, basicamente, em dois tipos de sistemas de reconhecimento: verificação (autenticação) e identificação.

Sistemas de verificação (Automatic Fingerprint Recognition System - AFRS) utilizam um código inicial de acesso - número identificador ou cartão magnético - e uma característica física particular de usuário, que funciona como a senha de validação desse código. Ou seja, por meio do código de acesso é realizada uma busca na base de dados à procura de um usuário em específico e, que pela característica física, o código informado é validado; sistemas de identificação (Automatic Fingerprint Identification System - AFIS) possuem um processo mais complexo e, muitas vezes, lento, já que a característica física funciona, ao mesmo tempo, como código de acesso e senha de autenticação.

Independente do tipo do sistema de reconhecimento, o processo se dá em duas fases. Na primeira, o usuário é registrado no sistema, através da captura de suas características biométricas, as quais são convertidas em um modelo matemático de representação (template). Na segunda fase, o usuário novamente apresenta suas características biométricas, mas agora são comparadas e validadas com o modelo armazenado, a fim de executar a verificação ou identificação. Enfim, a utilização da biometria tem basicamente dois propósitos: validar e/ou identificar usuários. A Figura 1 ilustra melhor o descrito

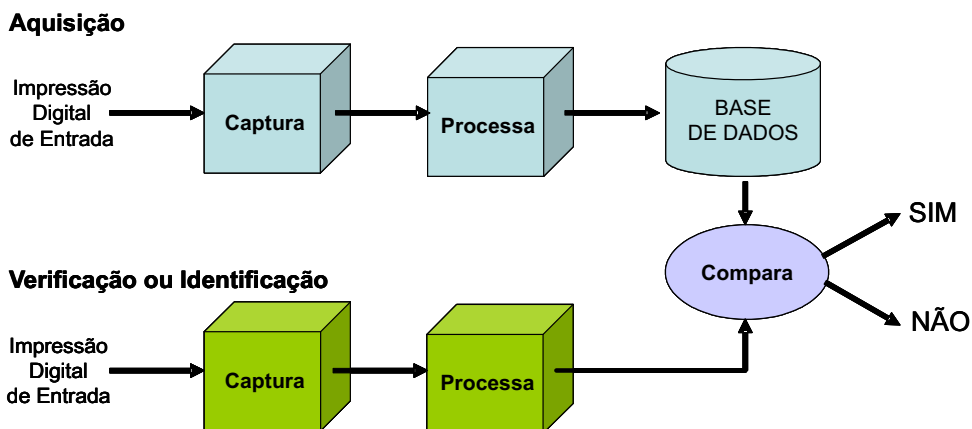


Figura 1: Fases do processo de Verificação/Identificação [Costa, 2001].

Segundo Silva (2002), na escolha de qualquer sistema biométrico, o aspecto desempenho é muito importante. Este pode ser categorizado de duas maneiras distintas: a taxa de falsa aceitação (FAR - False Acceptance Rate), que representa a percentagem de usuários não autorizados que são incorretamente aceitos pelo sistema, e a taxa de falsa rejeição (FRR - False Rejection Rate), que representa a percentagem de usuários autorizados que são incorretamente rejeitados. FAR e FRR são dependentes uma da outra. Normalmente, uma pequena FRR conduz a uma alta FAR e vice-versa.

O método da impressão digital trata da análise das características existentes nas digitais, ou seja, pequenas marcas na imagem do dedo, conhecidas como minúcias, que são pontos

característicos que podem ser identificados, classificados, medidos e comparados, garantindo assim a unicidade de uma impressão digital (ID). Conforme Costa (2001), as minúcias são acidentes que se encontram nas cristas papilares e têm a finalidade de estabelecer a unicidade das IDs. As cristas papilares são as linhas pretas (ou cinza escuro), as quais devem ser levadas em consideração na comparação, e os sulcos interpapilares são as linhas brancas (ou cinza claro), as quais separam as cristas papilares (veja Figura 2).



Figura 2: Classificação da Minúcia [Silva, 2002].

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. Essa propriedade faz com que a impressão digital seja um grande atrativo na identificação biométrica [Silva, 2002]. O primeiro estudo das características das impressões digitais foi realizado por Francis Galton (ibidem), que as dividiu de acordo com alguns aspectos que são a base para o reconhecimento. Costa (2001) afirma que as minúcias são resumidamente classificadas dentro de duas categorias: aspectos básicos e compostos. Como exemplos de aspectos básicos têm-se (Figura 3):

- crista final: é definida como um ponto onde a crista termina;
- crista bifurcada (bifurcação): definida como um ponto onde a crista diverge dentro de cristas brancas, onde a linha se divide em duas.

Como exemplos de aspectos compostos têm-se:

- ilhas: ou lagos - são formados por duas bifurcações conectadas, que se contornam e retornam ao rumo de origem;
- cruzamentos: ou pontes - são definidos como duas ou mais bifurcações com um caminho conectando-as;
- esporas: são formadas pela combinação de cristas bifurcadas e cristas finais;
- cristas curtas: são definidas como cristas finais muito pequenas.

Para facilitar o entendimento e a manipulação automática, o American National Standards Institute (ANSI) propôs uma classificação das minúcias em 4 tipos: terminações, bifurcações, cruzamentos e

indeterminado, conforme também apresentado na Figura 2.

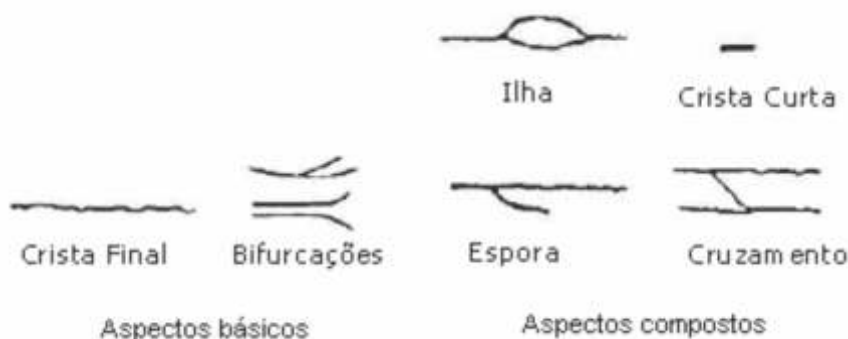


Figura 3: Minúcias [Costa, 2001].

Já o Federal Bureau of Investigation (FBI) considera apenas terminações (fim de linha) e bifurcações. Conforme Pacheco (2003), cada minúcia é caracterizada pelo seu tipo, sua coordenada x, y e o ângulo entre a tangente da crista da minúcia e o eixo horizontal. Pacheco (2003) afirma que as cristas formam padrões geométricos, em que se identificam 3 tipos de pontos: LOOP, WHORL e DELTA, ou seja, pontos de singularidade (Figuras 4 e 5)

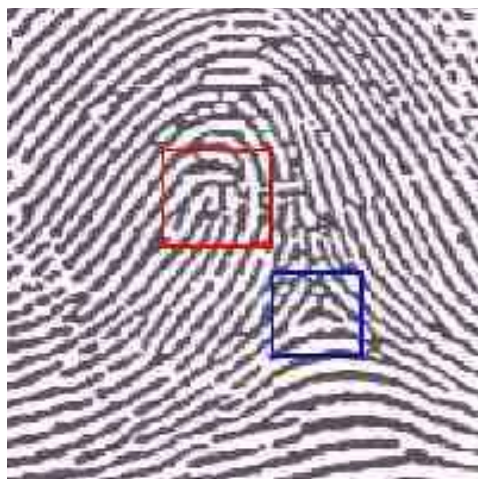


Figura 4: LOOP (vermelho ou esq. acima) e DELTA (azul ou dir. abaixo) [Pacheco, 2003].

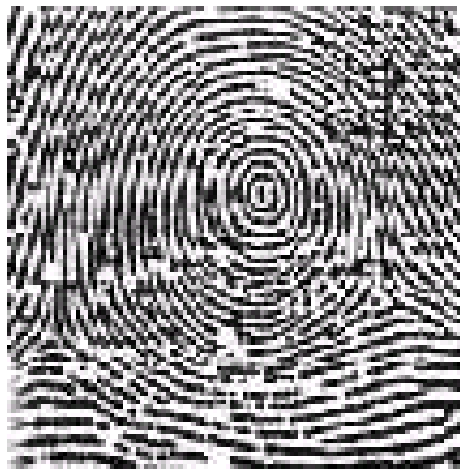


Figura 5: WHORL [Pacheco, 2003].

Os pontos de singularidade Loop e Whorl, conhecidos também como ponto de singularidade NÚCLEO, são usados em muitas abordagens para o processo de autenticação/identificação por impressão digital, para encontrar um ponto de referência conhecido como core point (núcleo), mostrado na Figura 4 com os quadrados azul e vermelho. As impressões digitais são classificadas com base nos seus padrões globais.

Assim, o American National Standards Institute (ANSI) classificou as impressões digitais, baseando-se nos pontos de singularidade (Loop, Delta e Whorl), em cinco classes distintas: (I) arco plano - arch; (II) arco angular - tented arch; (III) verticilo - whorl; (IV) presilha externa - right loop; (V) presilha interna - left loop, como ilustra a Figura 6.

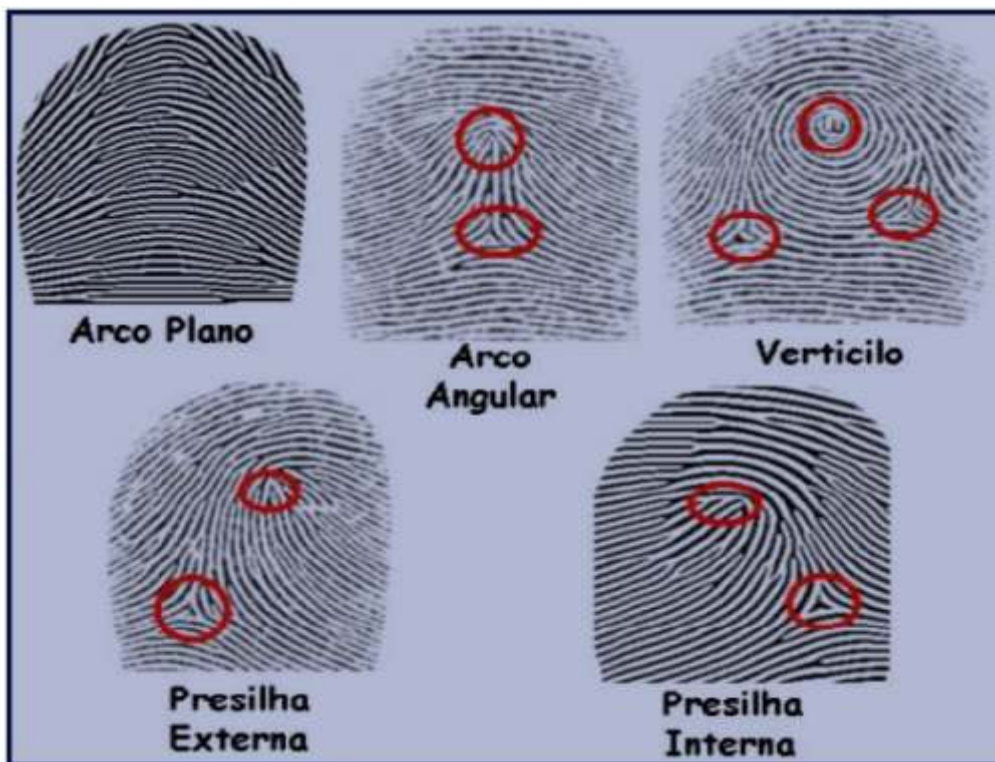


Figura 6: Classificação das Impressões Digitais [Costa, 2001].

Enfim, a biometria da impressão da digital é considerada uma técnica bem difundida e acessível, sendo utilizada em aplicações como controle de acesso, caixas automáticos de bancos, registros de saúde, entre outras. As principais vantagens desse método são: velocidade, baixo custo e aceitação por parte dos usuários [Romagnoli, 2002].

Na próxima seção, são apresentados algumas técnicas, seus algoritmos e os processos utilizados no reconhecimento de indivíduos com uso de impressões digitais.

2 Trabalhos Relacionados com Impressões Digitais

Os sistemas projetados nos últimos anos, para identificação ou para autenticação de impressões digitais, seguem um fluxo básico, como ilustrado na Figura 1 da segunda seção. Porém, na fase PROCESSA, exibida nessa figura (tanto na aquisição quanto na verificação/identificação), existem variações em suas subfases.

Uma das linhas de raciocínio para o processo de identificação/verificação através de digitais utiliza o método de detecção estrutural da Impressão Digital por meio das minúcias. Outra linha usa o método orientado à textura, que se baseia nos padrões que as linhas da digital formam entre si e da quantidade de perturbações existentes na vizinhança de um ponto [Pacheco, 2003]. Nesses dois métodos é necessário obter um ponto de referência na impressão digital, pois esse será a base de partida para a extração de características (para uma classificação prévia ou para comparação direta). Define-se como ponto de referência o ponto de máxima curvatura côncava da imagem. No método de extração de minúcias, é a partir do ponto de referência que se mede a localização de cada minúcia. No outro método, define-se a área circular de interesse centrada nesse ponto. A Figura 7 ilustra a localização do ponto e o posicionamento das características a analisar, a partir dele. Lembrando que, para todas as classes de impressão digital, existem zonas onde as cristas descrevem curvaturas acentuadas na zona central da impressão digital.

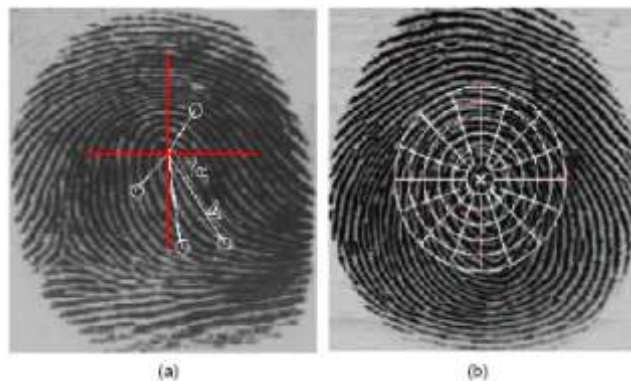


Figura 7: Exemplo da localização das características com base no ponto de referência: (a) minúcias; (b) textura orientada [Pacheco, 2003].

No texto que segue, é somente descrito o método que utiliza minúcias, visto que é uma técnica bastante utilizada e referenciada nos principais trabalhos sobre o tema.

2.1 Método por detecção de minúcias

Novamente, dentro desse método, também há variações de técnicas a serem utilizadas para detecção de minúcias. A Figura 8 mostra os passos utilizados na maioria dos trabalhos que utilizam esse método.

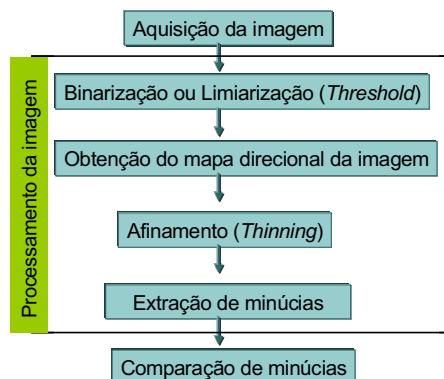


Figura 8: Fluxo com orientação direcional.

2.1.1 Aquisição da imagem

A aquisição da imagem pode se dar de duas formas distintas: captura da imagem por um leitor de impressões digitais ou a leitura a partir de digitais gravadas com tinta em papel. Normalmente, as imagens em papel possuem má qualidade de aquisição, dificultando o trabalho com a imagem escaneada [Jain, 1996]. Na maioria dos trabalhos científicos, é utilizada uma base de dados com imagens de IDs de boa resolução, ou recebidas através do leitor de impressões digitais, ou geradas automaticamente.

Em imagens adquiridas através de scanner, ou seja, digitais obtidas pela pressão do dedo tintado no papel, normalmente algumas técnicas posteriores devem ser utilizadas, como extração de ruídos, técnicas de realce, entre outras. Já nas imagens adquiridas pelo leitor, essas técnicas não se fazem necessárias, pois a imagem capturada é, normalmente, de boa qualidade.

2.1.2 Binarização ou Limiarização (Threshold)

A maioria dos algoritmos de extração de minúcias trabalha com imagens binarizadas, ou seja, com dois valores de interesse: pixels brancos representando os vales, e pixels pretos, representando as linhas.

Para transformar uma imagem em tons de cinza em uma imagem binarizada, existem vários métodos. A implementação estudada calcula um threshold (valor limiar) para cada janela 3 x 3 (matriz 3 x 3), com a média dos valores dos *pixels*. O que estiver acima da média adquire o valor 256 (branco - representando vales), o que estiver abaixo, adquire o valor 0 (preto - representando as linhas). Segundo Matias (2004), limiarização é a operação mais comum de segmentação, que é a técnica para isolar regiões de *pixels* e aplicar operações para “extração de atributos”.

Vale citar que a limiarização pela média se aplica bem em função do tamanho de pequenas janelas. Para janelas maiores, o uso da mediana ou da moda pode ser uma melhor solução.

2.1.3 Obtenção do mapa direcional da imagem

A imagem direcional é utilizada para fornecer informações contidas na imagem original, funcionando bem mesmo em imagens com ruídos, pois os atenua. Entende-se como ruído distorções na imagem.

Encontraram-se na literatura, dois métodos para calcular a imagem direcional, que podem ser encontrados em Ratha (1995) e Muniz (2004). O algoritmo utilizado no sistema desenvolvido pelo Grupo de Pesquisa em TI (GPTI-Feevale) para encontrar o campo direcional é apresentado a seguir.

Cria a matriz Temp como cópia da Imagem

Para cada ponto P(i,j) da imagem fazer

Para k de -2 até 2 fazer

*s[0] recebe s[0] + Temp[i, j+2*k]*

*s[1] recebe s[1] + Temp[i+k, j-2*k];*

*s[2] recebe s[2] + Temp[i+2*k, j-2*k];*

*s[3] recebe s[3] + Temp[i+2*k, j-k];*

*s[4] recebe s[4] + Temp[i+2*k, j];*

*s[5] recebe s[5] + Temp[i+2*k, j+k];*

*s[6] recebe s[6] + Temp[i+2*k, j+2*k];*

*s[7] recebe s[7] + Temp[i+k, j+2*k];*

Calcula Min e p, o menor valor de s e seu índice respectivo

Calcula Max e q, o maior valor de s e seu índice respectivo

Calcula Total, a soma de todos os valores de s

*Se ((Temp[i,j] * 4 + Min + Max)) < (Total * 3 / 8), então*

$P(i,j)$ recebe $p * 22.5$
 Senão $P(i,j)$ recebe $q * 22.5$

Algoritmo 1: Busca do campo direcional.

Suavização do mapa direcional

Para suavizar o mapa direcional, são propostos dois métodos: o método seno-cosseno e a moda [Karu, 1996]. Para o método seno-cosseno, bons resultados são obtidos dobrando-se os valores dos ângulos e então se calculando os cossenos e senos. Usando esse método para 1° (0,999391; 0,034900) e 179° (0,999391; -0,034900), a média é a horizontal (0,999391; 0). Dessa forma, obtém-se um vetor unitário na direção $v = (\cos 2\alpha; \sin 2\alpha)$. Para o método da moda, divide-se a imagem em blocos onde serão considerados os vizinhos para calcular o valor médio de direção. Para suavizar o mapa direcional, considera-se a direção que aparece com maior frequência, atribuindo-a ao bloco (direção mais freqüente). A seguir, pode ser observado o algoritmo de suavização do mapa direcional.

```
// Calcula o valor da moda de um bloco de um campo
//                               direcional calculado anteriormente
// i, j - coordenadas do ponto superior esquerdo do bloco
// KernelSize - tamanho do bloco
// Temp - matriz do campo direcional
Para cada ponto do B(x,y) do bloco fazer
    Incrementa Count[B(x,y)]
Calcula Max como o índice do valor com mais ocorrências
Retorna Max * 22.5
```

Algoritmo 2: Suavização do mapa direcional.

A Figura 9 apresenta a classificação da imagem logo após a suavização.

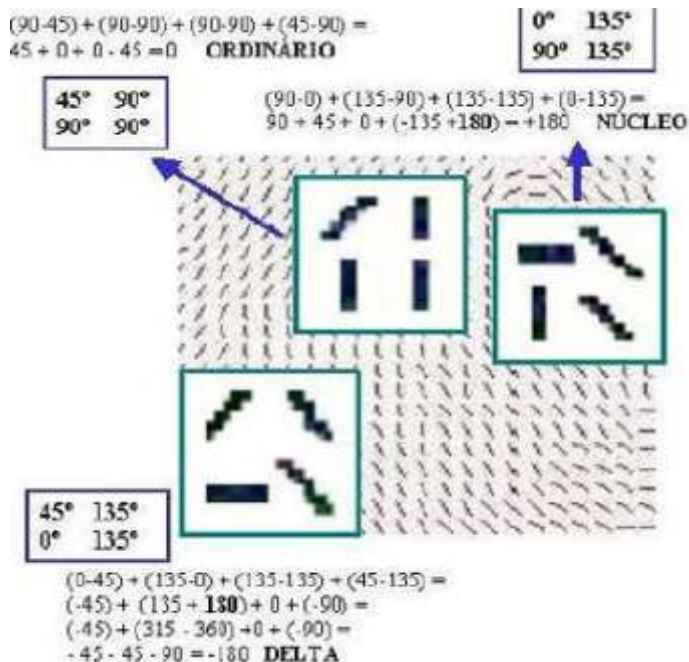


Figura 9: Suavização do mapa direcional.

Classificação com o índice de Poincaré

Um *pixel*, na imagem direcional, é classificado como ordinário, núcleo ou delta através do cálculo de Poincaré [Kawagoe, 1984]. O índice de Poincaré é uma pequena curva fechada em torno de um *pixel* calculado pela somatória das mudanças dos ângulos direcionais em torno da curva. Ao completar uma volta no sentido anti-horário, observa-se que o ângulo direcional se fixa em 0° , $+180^\circ$ ou -180° durante esse ciclo. Enfim, um *pixel* é classificado conforme segue.

- **Ordinário**: se o ângulo está fixado em 0° ;
- **Núcleo**: se o ângulo está fixado em $+180^\circ$;
- **Delta**: se o ângulo está fixado em -180° .

Considerando-se uma vizinhança 2×2 (matriz 2×2), calcula-se a diferença entre dois ângulos no sentido anti-horário. O módulo não pode ser maior do que 90° . Se for maior, deve ser analisado o sinal: se negativo, adiciona-se $+180^\circ$; se positivo, adiciona-se -180° . Com isso a diferença estará sempre no primeiro quadrante, ou seja, sempre menor que 90° .

A partir disso (conhecendo os núcleos e deltas), a imagem é classificada com base no número e na localização desses pontos [Kawagoe, 1984]. O Algoritmo 3 ilustra o processo de reconhecimento de imagens das digitais distribuídas nas cinco classes propostas por Edward Henry [Costa, 2001].

```
Divide a imagem em blocos de dimensão Área
Para cada bloco  $B(u, v)$  fazer
Delta[0] recebe  $DirModeValue(B(u, v+1)) - DirModeValue(B(u, v))$ 
Delta[1] recebe  $DirModeValue(B(u, v+1)) - DireModeValue(B(u, v))$ 
Delta[2] recebe  $DirModeValue(B(u, v+1)) - DirModeValue(B(u, v))$ 
Delta[3] recebe  $DirModeValue(B(u, v+1)) - DirModeValue(B(u, v))$ 
Soma recebe 0
para x de 0 até 3 fazer
    Se  $Delta[x] > 90$  então
        Soma recebe  $Soma + Delta[x] - 180$ 
    Senão, Se  $Delta[x] < -90$ , então
        Soma recebe  $Soma + Delta[x] + 180$ 
    Senão
        Soma recebe  $Soma + Delta[x]$ 
Se  $Soma = 180$ , então Desenha círculo verm. centro do bloco  $B(u, v)$ 
Senão, Se  $Soma = -180$ , então
    Desenha círculo verde centro do bloco  $B(u, v)$ 
Algoritmo 3: Distribuição das digitais por classes.
```

Resumindo, o mapa direcional é obtido através de algoritmos que calculam a direção do traçado da digital em uma região específica, reduzindo os ruídos das imagens. Logo após, essa imagem é classificada de acordo com o seu tipo. Essa classificação é usada para separar e agilizar a busca posterior no banco de dados das Ids. A Figura 10 ilustra o fluxograma completo da classificação da ID pelo índice de Poincaré.

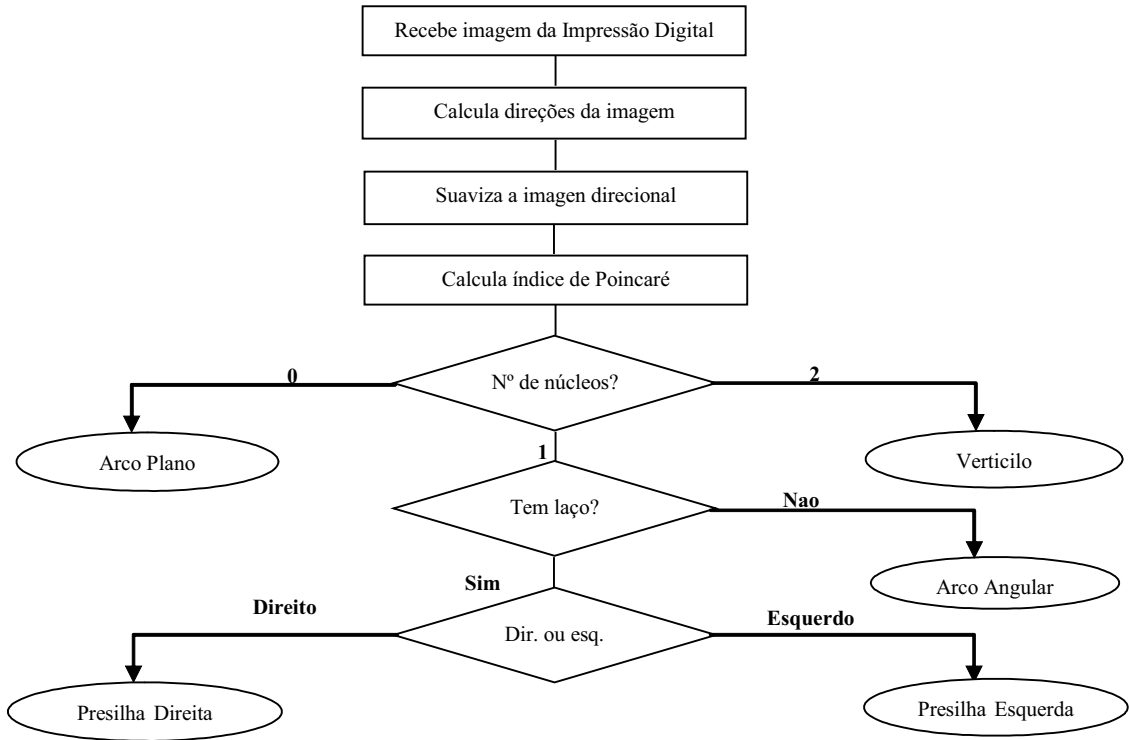


Figura 10: Fluxograma do processo de reconhecimento das digitais.

2.1.4 Afinamento ou esqueletização (Thinning)

O processo de afinamento remove todos os *pixels* redundantes das imagens de impressões digitais produzindo uma nova imagem simplificada com a largura de um único *pixel* [Facon, 2005]. O algoritmo é repetido n vezes, até que não existam mais *pixels* redundantes e apareça somente o esqueleto da imagem. Num primeiro processo, os *pixels* são marcados e, numa segunda varredura, eliminados. A varredura é feita linha a linha, comparando com a vizinhança para saber se o *pixel* pode ser apagado ou não. Para eliminar o efeito escada encontrado na imagem após o afinamento, pode-se aplicar a fórmula de Holt (ibidem). A Figura 11 mostra o processo de afinamento.



Figura 11: (a) fim de linha imagem normal; (b) fim de linha imagem binarizada; (c) bifurcação imagem normal; (d) bifurcação imagem binarizada.

2.1.5 Extração de minúcias

As minúcias são pequenas marcas na imagem do dedo, ou seja, as terminações e bifurcações de sulcos na imagem, como já apresentado. Com base nessas informações, pode-se comparar a imagem recebida no leitor com as informações armazenadas no banco de dados, para verificar se é uma impressão digital válida ou não, liberando o acesso à pessoa em caso de positivo e bloqueando-o, em caso de negativo.

O método mais utilizado atualmente para a extração de minúcias é o de Crossing Number (CN) [Halici, 1999]. Esse método é aplicado à imagens afinadas/esqueletizadas, usando como base uma vizinhança de oito pixels. A extração de minúcias é feita examinando-se a vizinhança do pixel em uma janela de 3 x 3 (matriz). O valor de CN é então computado usando a soma das diferenças entre os pares de pixels adjacentes na vizinhança de oito pixels. O Quadro 1 define as propriedades do Crossing Number resultantes.

Quadro 1: Propriedades do Crossing Number.

CN	PROPRIEDADE
0	Ponto isolado
1	Ponto de final de linha
2	Ponto de uma linha continua
3	Ponto de bifurcação
4	Ponto de cruzamento

Outros autores, como Jain (1996), utilizam um método mais simples para detectar uma minúcia a partir de uma imagem esqueletizada. Com base em uma janela 3 x 3, examina-se a vizinhança local do ponto da linha na imagem. Um *pixel* é classificado como final de linha, se tiver apenas um vizinho na janela, e como bifurcação, se tiver três vizinhos para o ponto da linha.

Deve ser observado se existem ruídos na imagem, pois a sua presença, fará com que se encontrem falsas minúcias ou não se encontrem algumas verdadeiras. Nesse caso, é importante aplicar algum filtro para eliminar os ruídos.

Pós-processamento da imagem

Para testar as minúcias, eliminando as falsas, foi estudado o algoritmo implementado por Thai (2003), que examina os vizinhos de cada ponto. O primeiro passo do algoritmo é criar uma imagem M de tamanho W x W. O ponto central de M corresponde ao ponto de minúcia na imagem esqueletizada e este *pixel* é nomeado com -1. O resto dos *pixels* de M são inicializados com 0 (zero).

O passo seguinte depende de identificar se o ponto candidato à minúcia é um final de linha ou uma bifurcação. O algoritmo a seguir traduz o descrito.

a) Se o ponto é candidato a final de linha:

- nomeia com 1 todos os oito pixels vizinhos do ponto candidato;
- contar o número de transições de 0 para 1 (T01) no sentido horário ao longo da borda da imagem. Se T01 = 1, então o ponto candidato à minúcia é verdadeiramente um final de linha.

b) Se o ponto é candidato à bifurcação:

- examinar os oitos vizinhos no sentido horário. Para os três pontos conectados com a

bifurcação nomear com valores 1, 2 e 3;

- o próximo passo é nomear o resto das linhas dos três pontos conectados. Para cada linha nomear os pixels com 1, 2 e 3;

- em seguida, contar no sentido horário o número de transições de 0 para 1 (T01), 0 para 2 (T02) e 0 para 3 (T03) na borda da imagem M.

Se $T01 = 1$ e $T02 = 1$ e $T03 = 1$, então, o ponto candidato é uma bifurcação válida.

Algoritmo 4: Eliminação de falsas minúcias.

Assim sendo, a extração de minúcias é a enumeração e o mapeamento de pequenas marcas na imagem do dedo, ou seja, a catalogação de terminações e bifurcações na imagem da impressão digital. A qualidade da imagem conseguida é responsável em grande parte pela eficiência de sistemas de impressão digital, que é baseada na taxa de falsas rejeições (False Rejection Rate - FRR) e na taxa de falsas aceitações (False Acceptance Rate - FAR) [Costa, 2001]. Como descrito na Seção 2, FAR representa a percentagem de usuários não autorizados que são incorretamente aceitos pelo sistema, e FRR representa a percentagem de usuários autorizados que são incorretamente rejeitados.

Para o detalhamento da fase de comparação de minúcias, considerada a última etapa para o processo de identificação de ID, é organizada a Seção 4, a qual aborda, com maiores detalhes, os estudos realizados e apresentados até então.

3 Comparação de Minúcias

Para a detecção das minúcias seleciona-se uma região que se considera a mais importante e que possui o maior número de minúcias. Em alguns trabalhos, seleciona-se como região de interesse todos os pixels que se encontram a uma distância inferior a 100 pixels da região central. Com essa seleção, elimina-se a região com pontos que possam ser identificados de forma errônea que se encontram nas bordas da imagem. A Figura 12 exibe minúcias detectadas em área de referência.

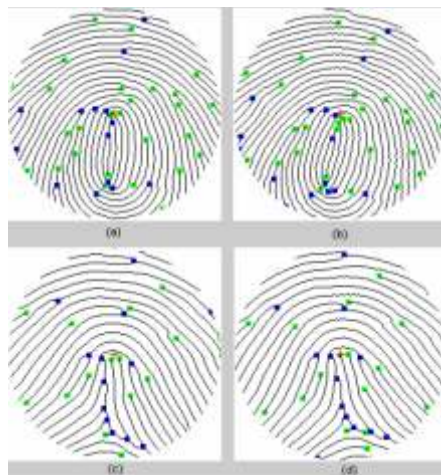


Figura 12: Detecção de minúcias na área de referência [Reis, 2003].

Cada minúcia é definida a partir do seu tipo (terminação ou bifurcação), por sua localização, que é dada pela distância da minúcia com o centro da imagem e pelo seu ângulo em relação a uma linha horizontal imaginária no centro da imagem.

Deve existir uma certa tolerância em relação à posição exata da minúcia, chamada de *threshold*. Se a distância medida for inferior ao *threshold*, é considerada como posição correta. Para as impressões contendo em média 40 minúcias, encontrar 15 a 30 minúcias coincidentes já é possível considerar que são pertencentes a um mesmo dedo. Segundo Kehdy (1968, p. 61) e Tavares Júnior (1991, p. 32) apud [Matias, 2004], “para se confirmar a identidade de uma ID, deverão ser coincidentes no mínimo doze minúcias, as quais devem ser encontradas da mesma forma, localização e mesma quantidade nas duas impressões em comparação”. Também não pode haver minúcias que se encontram na impressão do modelo e não estão presentes na impressão sendo comparada.

O algoritmo de comparação de minúcias deve considerar a posição (x, y) e o tipo de minúcia. Deve receber duas imagens: uma já armazenada no banco de dados (*template*) e outra recebida do leitor. A partir daí, de cada imagem gera-se uma lista de terminações (finais de linha) e bifurcações com suas respectivas posições (x,y).

Deve ser feita uma comparação das duas listas, respeitando um *threshold* e determinando a taxa de distâncias possíveis para que os *pixels* possam ser comparados como coincidentes. As minúcias coincidem com o modelo (*template*), se estiverem localizadas no mesmo bloco e se a distância entre elas não for superior ao *threshold* determinado.

Conforme [Cappelli et. al., 2003] e como descrito na seção anterior, a identificação de uma pessoa com um Sistema Automático de Identificação Digital (Automated Fingerprint Identification System - AFIS) exige a comparação de uma impressão digital com todas as impressões digitais em um banco de dados, que muitas vezes contém milhares de impressões. Adotar, assim, uma abordagem de classificação de ID, segundo Cappelli (ibidem), pode ser uma boa estratégia para reduzir o número de comparações durante a recuperação de impressões digitais e, conseqüentemente, o tempo do processo de identificação.

Atualmente, todos os esquemas de classificação utilizados, principalmente pelas agências de polícia, são variações do esquema proposto por Francis Galton e Edward Henry [Costa, 2001]. Essas classes, relacionadas a seguir, segundo vários autores, agrupam impressões digitais nas seguintes proporções:

- Arch (arco plano) - 3,7% das Ids.
- Tented Arch (arco angular) - 2,9%.
- Left Loop (presilha interna) - 33,8%.
- Right Loop (presilha externa) - 31,7%.
- Whorl (verticilo) - 27,9% das IDs.

A Figura 6, exibida na Seção 2, mostra as classes a partir dos pontos singulares circulosados em vermelho.

Vários estudos têm sido realizados para a classificação de impressões digitais, tais como em Silva, (2002), que utiliza redes neurais, e em Costa, (2001), que usa grafos na classificação daquelas.

A classificação automatizada de impressões digitais nessas 5 classes é considerada um difícil problema de reconhecimento de padrões, devido às variações inter e intraclasses, e aos ruídos que afetam com muita frequência as imagens dessas impressões digitais. Nos últimos 30 anos, muitas abordagens foram e continuam sendo propostas baseadas na variedade de técnicas de classificação, principalmente por sua relevância e sua complexidade intrínseca. Os principais métodos de

classificação e seus autores e/ou pesquisadores são:

- Sintáticos - Moayer et. al. (1976) e Rao et. al. (1980).
- Estruturais - Cappelli et. al. (1999) e Maio et. al. (1996).
- Baseados em regras - Ballan et. al. (1997), Cho et. al. (2000), Chong et. al. (1997), Hong et. al. (1999) e Karu et. al. (1996).
- Redes neurais - Bernard et. al. (2001), Bowen (1992), Halici et. al. (1996), Kamijo (1993), Moscinska et. al (1993).
- Fusão de classificadores (híbridos) - Candela et. al. (1995), Cappelli et. al. (2002), Jain et. al. (1999), Marcialis et. al (2001), Senior (2001) e Yao et. al. (2001).
- Baseados em arquitetura seqüencial de dois estágios - Cappelli, et. al. (2003).

Porém, nem todos os trabalhos utilizam a classificação para a comparação das minúcias. A seguir, outros trabalhos considerados importantes no uso de minúcias para a comparação de ID [Matias, 2004]:

- Hong (1999). Considerado o trabalho mais completo, em que se apresentou um estudo detalhado sobre os passos da construção de um AFIS: aquisição de ID, pré-processamento, mapa direcional, classificação e extração de minúcias.
- Silva (1999). Foi desenvolvido um protótipo para classificação de ID nos tipos fundamentais: arco, presilha interna, presilha externa e verticilo. Para tanto o autor também utilizou a construção de mapa direcional. No protótipo foi utilizada uma Rede Neural Artificial (RNA) - perceptron feedforward - treinada por retropropagação.
- Costa (2001). Foram apresentadas fórmulas para pré-processamento de imagens de IDs, conceitos e algumas técnicas para classificação e extração de minúcias. Ao fim, foram apresentadas conclusões sobre o mapa direcional das cristas papilares.
- Gumz (2002). Foi desenvolvido um protótipo para identificação e classificação das minúcias de uma ID por meio de redes neurais artificiais multicamada.
- Matias (2004). Nesse trabalho é apresentado um protótipo que, através de RNAs feedforward multicamada com treinamento backpropagation, pudesse realizar a identificação de deltas e núcleos em IDs.
- Maniola (2005). No trabalho foi desenvolvido um protótipo de reconhecimento de impressões digitais que utiliza o modelo de Redes Neurais Artificiais Cascade Correlation.

Finalmente, esta seção apresentou os principais estudos sobre Impressões Digitais, no que se refere a melhoramentos de imagem de IDs e ao tratamento de minúcias, como pontos para identificação dessas IDs. Enfim, uma revisão bibliográfica de métodos utilizados no processo de identificação e comparação de impressões digitais para o reconhecimento de indivíduos em sistemas automatizados.

Considerações Finais

Ao final deste trabalho, é possível se ter uma visão completa de todo o processo de reconhecimento de indivíduos pelo uso de impressões digitais, mais precisamente pelo método de detecção de minúcias. Como descrito na introdução, para que uma característica seja utilizada como método biométrico, deve atender os requisitos de universalidade, singularidade, permanência e

mensurabilidade. A impressão digital, além de atender a esses requisitos, apresenta-se como um método com boa aceitação e custo acessível.

As imagens da impressão digital podem ser adquiridas de duas formas: por um scanner digital, procedimento usado atualmente, ou escaneadas a partir de uma imagem do dedo, colocado sobre o papel com carbono tintado. Os estudos recentes têm se preocupado somente com as obtidas de scanners ópticos, devido ao seu baixo custo.

A partir de Galton [Silva, 2002], várias subdivisões foram criadas para a classificação das minúcias e da impressão digital. Essas distribuições foram apresentadas dando-se ênfase à classificação ANSI, com a qual se está trabalhando nesse projeto.

Na Seção 3, foram detalhados os conceitos básicos referentes às impressões digitais, suas características fundamentais, como são definidas, tratadas e empregadas, além de quais e como os principais métodos são usados em sistemas automatizados. Os principais trabalhos na área foram pesquisados e relatados neste estudo.

Os algoritmos apresentados e contextualizados neste texto foram implementados pelo GPTI e testados amplamente (como o propósito deste artigo é apresentar uma revisão detalhada sobre o tema, os resultados dos testes não foram inseridos). Os passos para obter uma imagem, melhorá-la (redução de ruídos) e, a partir dela, detectar e comparar minúcias, foram cuidadosamente descritos e ilustrados.

A comparação de minúcias é parte fundamental do processo, por isso, foi detalhada, apresentando-se os principais métodos e autores que pesquisam o assunto.

Por fim, o propósito do artigo foi mostrar a compilação realizada pelo Grupo de Pesquisa em TI da Feevale até o momento, sobre tema de pesquisa. Aqui, foram esclarecidas as diferentes abordagens, enfatizando pontos de convergência de raciocínio dos principais autores pesquisados.

Referências

BALLAN M., Sakarya F.A. and Evans B.L. (1997) **A Fingerprint Classification Technique Using Directional Images**, Asilomar Conference on Signals, Systems, and Computers.

BERNARD S., Boujemaa N., Vitale D. and Bricot C. (2001) **Fingerprint Classification Using Kohonen Topologic Map**, Proceedings International Conference on Image Processing ICIP'2001, Thessaloniki, Greece.

BOWEN J.D. (1992) **The Home Office Automatic Fingerprint Pattern Classification Project**, in proceedings IEE Coll. On neural network for image processing applications.

CANDELA G.T. et. al. (1995) **PCASYS - A Pattern-Level Classification Automation System for Fingerprints**, NIST tech. report NISTIR 5647.

CAPPELLI R., Lumini A., Maio D. and Maltoni D. (1999) **Fingerprint Classification by Directional Image Partitioning**, IEEE Transactions on Pattern Analysis Machine Intelligence, vol.21, no.5, pp.402-421.

CAPPELLI R., Maio D. and Maltoni D. (2002) **A Multi-Classifer Approach to Fingerprint Classification**, Pattern Analysis and Applications Special Issue on Fusion of Multiple Classifiers, vol.5, no.2, pp.136-144, May 2002.

CAPPELLI, R., Maio D., Maltoni, D. and Nanni, L (2003). **A two-stage fingerprint classification system**, In: WBMA2003, ACM, Berkeley, Califórnia, USA.

CHO B.H., Kim J.S., Bae J.H., Bae I.G. and Yoo K.Y. (2000) **Core-based Fingerprint Image Classification**, Int. Conf. Pattern Recognition (15th), Vol 2, pp. 863-866.

CHONG M.M.S. et. al. (1997) **Geometric Framework for Fingerprint Image Classification**, Pattern Recognition, v. 30, no. 9, pp. 1475-1488, 1997.

COSTA, S. M. F. (2001) '**Classificação e Verificação de Impressões Digitais**', (Dissertação de Mestrado em Engenharia Elétrica). Escola Politécnica de Universidade de São Paulo, São Paulo.

FACON, Jacques. (2005) **Algoritmo de Afinamento de Holt**, Programa de Pós-graduação em Informática Aplicada - Pontifícia Universidade Católica do Paraná. Disponível em: www.ppgia.pucpr.br/~facon/Afinamento/ Acesso em julho de 2005.

GUMZ, Rafael Araújo (2002) **Protótipo de um sistema de identificação de minúcias em impressões digitais utilizando redes neurais artificiais multicamada**. Trabalho de Conclusão de Curso Bacharelado em Ciências da Computação Centro de Ciências Exatas e Naturais, Universidade Regional de Blumenau, Blumenau.

HALICI U. and Ongun G. (1996) **Fingerprint Classification Through SelfOrganizing Feature Maps Modified to Treat Uncertainties**, Proceedings IEEE, Vol. 84, No. 10, pp. 1497-1512.

HALICI, U.; Jain, L. C.; Erol, A. (1999) **An introduction to fingerprint recognition**, In Intelligent Biometric Techniques in Fingerprint and Face Recognition, pp. 3-34, CRC Press, Florida.

HONG L. and Jain A.K. (1999) **Classification of Fingerprint Images**, Scandinavian Conf. (11th) on Image Analysis, June 7-11, Kangerlussuaq, Greenland.

JAIN A.K., Prabhakar S. and Hong L. (1999) **A Multichannel Approach to Fingerprint Classification**, IEEE Transactions on Pattern Analysis Machine Intelligence, Vol.21, No.4, pp. 348-359.

JAIN, Anil; Hong, Ling. (1996) **On-line Fingerprint Verification**, Pattern Recognition and Image Processing Laboratory. Michigan State Univerty.

KAMIJO M. (1993) **Classifying Fingerprint Images using Neural Network: Deriving the Classification State**, in proceedings 3rd Int. Conf. on Neural Network, pp. 1932-1937.

KARU, K.; Jain, A. K. (1996) **Fingerprint classification**, Pattern Recognition, 29(3):389--404.

KAWAGOE, M.; Tojo, A. (1984) **Fingerprint Pattern Classification**, Pattern Recognition, Vol. 17, pp. 295-303.

MAIO D. and Maltoni D. (1996) **A Structural Approach to Fingerprint Classification**, Int. Conf. (23th) on Pattern Recognition, Vienna (Austria), Aug. 1996.

MANIOLA, Ricardo Inácio (2005). **Protótipo de sistema para autenticação de impressões digitais utilizando o modelo de redes neurais artificiais cascade correlation**. Trabalho de Conclusão de Curso Bacharelado em Ciências da Computação Centro de Ciências Exatas e Naturais, Universidade Regional de Blumenau, Blumenau.

MARCIALIS G.L., Roli F. and Frasconi P. (2001) **Fingerprint Classification by Combination of Flat and Structural Approaches**, Int. Conf. (3rd) on Audio-and Video-Based Biometric Person Authentication, pp. 241-246, Sweden.

MATIAS, Caio R. S. (2004) **Protótipo de um sistema de identificação do(s) delta(s) e núcleo em impressões digitais utilizando redes neurais artificiais**. Trabalho de Conclusão de Curso Bacharelado em Ciências da Computação Centro de Ciências Exatas e Naturais, FURB, Blumenau, Santa Catarina.

MOAYER B. and Fu K.S. (1976) **An application of stochastic languages to fingerprint pattern recognition**, Pattern Recognition, vol. 8, pp. 173-179.

MOSCINSKA K. and Tyma G. (1993) **Neural Network based Fingerprint Classification**, in proceedings 3rd Int. Conf. on Neural Network, pp. 229-232.

MUNIZ, Adriano S. (2004) **Reconhecimento da Íris**, DCC IME USP. S.P.: 38p.

PACHECO, C. A. R. A. (2003). **Autenticação com impressão digital**, Instituto Superior de Engenharia de Lisboa, Departamento de Engenharia de Electrónica e Telecomunicações e de Computadores, Portugal.

RAO K. and Balck K. (1980) **Type classification of fingerprints: A syntactic approach**, IEEE Trans. on Pattern Analysis Machine Intelligence, v. 2, no. 3, pp.223-231, 1980.

RATHA, Nalini K.; Chien, Shaoyun; Jain, Anil K. (1995) **Adaptative Flow Orientation Based Feature Extraction in Fingerprint Images** Pattern Recognition, v.28, n.11, pp. 1657-1672.

REIS, Carlos Manuel Silva dos (2003) **Autenticação com impressão digital**, Trabalho de Conclusão de Curso Licenciatura Engenharia de Sistemas de Telecomunicações e Electrónica do Instituto Superior de Engenharia de Lisboa, Portugal.

ROMAGNOLI, G. S. **Biometria: você é sua senha**. Disponível em <http://www.serpro.gov.br/publicacao/tematec/2002/ttec61>. Acesso em 06 de Julho de 2005.

SENIOR A. (2001) **A Combination Fingerprint Classifier**, IEEE Transactions on Pattern Analysis Machine Intelligence, vol. 23, no. 10, pp. 1165-1174.

SILVA, Alex Sandro (1999) **Protótipo de software para classificação de impressão digital**. Trabalho de Conclusão de Curso Bacharelado em Ciências da Computação Centro de Ciências Exatas e Naturais, Universidade Regional de Blumenau, Blumenau.

SILVA, Daniel dos Santos; ABE Narumi. (2002) **Sistema Reconhecedor de IDs Utilizando Redes Neurais**, Universidade Católica Dom Bosco, Campo Grande. Disponível em: <http://www.ec.ucdb.br/engenharia/projetograduacao/projetos2002/monografias/monografia-g7.pdf>. Acesso em novembro 2005.

THAI, Raymond. (2003) **Fingerprint Image enhancement and minutae extraction**, Universidade de Western Australia.

YANG, S., Sakiyama, K. and Verbauwhede, I., A. (2003). **Secure and Efficient Fingerprint Verification System for Embedded Systems**, 37th Asilomar Conference on Signal, Systems, and Computers, Nov. 2003, Pacific Grove, CA.

Yao Y., Frasconi P. and Pontil M. (2001) **Fingerprint Classification with Combination of Support Vector Machines**, Int. Conf. (3rd) on Audio- and Video-Based Biometric Person Authentication, pp. 253-258, Sweden, June 6-8.