Sistemas Automáticos de Identificação de Impressões Digitais

Fingerprint Automatic Identification Systems

Raimundo Cláudio da Silva Vasconcelos[1] , FATEC

Resumo

Este trabalho trata do uso das impressões digitais em sistemas de identificação automáticos. Inicialmente é apresentado um resumo histórico e os conceitos principais da biometria e suas aplicações. Também aborda a caracterização das impressões digitais, incluindo algumas técnicas utilizadas para melhoramento de imagens e as etapas envolvidas na classificação e identificação de uma impressão digital. Por fim, discute a comparação de uma impressão digital com imagens previamente armazenadas.

Palavras-chave. biometria; impressões digitais; sistemas automáticos; identificação.

Abstract

This work considers the using of fingerprints in automatic identification systems. Initially, presents a summary history and key concepts of biometrics and its applications. It also deals with the characterization of fingerprints, including some techniques used for image enhancement and the steps involved in sorting and identification of a fingerprint. Finally, it discusses the comparison of a fingerprint and an image previously stored.

Keywords. biometry; fingerprints; automatic systems; identification.

1.Introdução

Impressões digitais são bastante utilizadas em sistemas de identificação, reconhecimento e autorização, por suas características intrínsecas: imutabilidade, unicidade, universalidade e classificabilidade. A análise manual da impressão digital é uma tarefa tediosa, onde os aspectos para comparação são extremamente pequenos necessitando auxílio de lentes de aumento para obter um melhor exame das marcas de uma impressão digital (JAIN *et. al.*, 1997).

Reconhecimento biométrico, ou apenas biometria, consiste em reconhecer de forma automática indivíduos baseado nas suas características fisiológicas e ou comportamentais. Este reconhecimento é melhor do que aquele estabelecido em algo que o indivíduo deva lembrar (ex.: senhas) ou do que ele deva carregar (ex.: cartões de identificação) (JAIN, ROSS & PRABHAKAR, 2004) (ver Figura 1).

[1]Mestre. Docente da Faculdade de Tecnologia de Americana-FATEC (Americana-SP).

Figura 1. Evolução das técnicas de autenticação (COSTA, 2001).

Os sistemas automáticos de identificação de impressões digitais (AFIS) são sistemas biométricos e consistem nos módulos de registro e no de identificação. O primeiro módulo, chamado de identificação, consiste nas seguintes etapas: a) aquisição da impressão digital, b) melhoramento da imagem ou pré-processamento, c) extração das minúcias (pontos característicos), d) armazenamento do vetor de características (*template*) dessas minúcias. A partir dessas informações armazenadas em um banco de dados, pode-se comparar uma impressão digital candidata com todas as já armazenadas e analisar os resultados. A aquisição de uma impressão digital pode ser feita através da impressão tintada em papel ou leitor eletrônico (óptico ou capacitivo), mais confiável. Várias técnicas podem ser aplicadas para o melhoramento da imagem: filtros (contraste, Gabor, Wavelets), operações morfológicas (binarização, afinamento), aplicados pontualmente ou por área.

Este trabalho está organizado da seguinte forma: a primeira Seção aborda o histórico, principais conceitos e aplicações envolvidas com biometria. A Seção seguinte aborda técnicas para melhoramento de imagens. A terceira Seção descreve as etapas de classificação e identificação de minúcias em uma impressão digital, e por fim a comparação de uma impressão digital com as armazenadas é discutida.

2.Histórico

Alphonse Bertillon, chefe da divisão de identificação criminal do departamento de polícia francesa em Paris, desenvolveu e praticou a idéia de usar medidas corporais para identificar criminosos no século XIX (JAIN, ROSS & PRABHAKAR, 2004).

Sir Francis Galton, antropólogo e primo de Charles Darwin, provou cientificamente no século XIX que impressões digitais não mudam ao decorrer do tempo de vida humana. De acordo com seus cálculos, a probabilidade de duas impressões serem iguais é de um em um bilhão. Galton identificou as características (minúcias) através das quais impressões digitais podem ser identificadas (GALTON, 2005).

Em 1891, Juan Vucetich, argentino naturalizado apresentou seu sistema de identificação com o nome de *Icnofalangometria*. Em 1894, Dr. Francisco Latzina, sugere que o nome Icnofalangometria fosse substituído por *Dactiloscopia*.

Em 1901 impressões digitais foram introduzidas para identificação criminal na Inglaterra e país de Gales. As observações de Galton e revisões feitas por sir Edward Richard Henry foram utilizadas. Isto deu origem ao chamado Sistema Henry de Classificação, que adotava quatro tipos fundamentais: arcos, presilhas, verticilos e compostos.

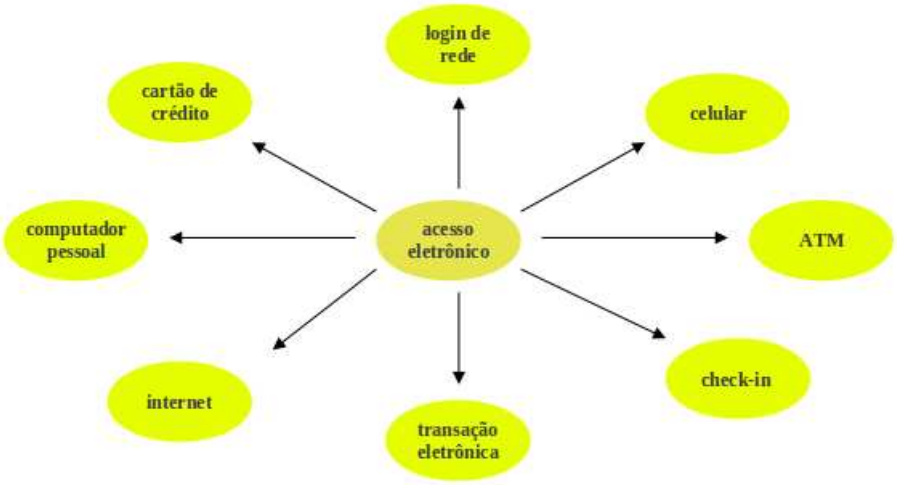
Em 1903, foi regulamentada a lei 947, instituindo o sistema dactiloscópico Vucetich, no Rio de Janeiro.

Em 1918, Edmond Locard escreveu que se 12 pontos (detalhes de Galton) forem os mesmos entre duas impressões digitais, isto seria suficiente para uma identificação positiva. Isto foi intitulado como a *regra dos 12 pontos*.

O uso de impressões digitais ganhou popularidade e, a partir de 1991, a identificação baseada em impressões digitais foi formalmente aceita pela justiça e governo da Inglaterra como método de identificação pessoal. Atualmente, vários departamentos de polícia aderiram à idéia de armazenar impressões digitais de criminosos em um banco de dados para realizar futuras pesquisas a partir de impressões digitais *deixadas* (fragmentos, geralmente) em cenas de crime.

Além dessa aplicação, o reconhecimento de indivíduos através de biometria tem sido utilizado em várias aplicações civis, buscando o aumento de segurança e agilidade em sistemas de controle de acesso, financeiros, eleição, licença para dirigir, cartão de crédito, entre outros (ver Figura 2). Sistemas baseados em impressões digitais se popularizaram de tal forma que se tornaram sinônimo para sistemas biométricos.

Figura 2. Aplicações que requerem autenticação automática (PRABHAKAR, 2001).



3.Características da impressão digital

Uma característica biométrica pode ser:

- característica fisiológica (atributo inato aos indivíduos); ou
- característica comportamental (algo que nós fazemos, podendo sofrer alterações motivadas por doença ou idade. Ex.: assinatura, caminhar).

Em termos de precisão, geralmente características fisiológicas são mais confiáveis do que comportamentais. As principais características em estudo abordam face, impressões digitais, geometria da mão, veias da mão, íris, padrão da retina, voz, e termograma facial.

Impressões digitais são bem aceitas como biometria por apresentarem as seguintes características (OLIVEIRA & LEITE, 2004):

- Universalidade: todas as pessoas possuem;
- Distinguibilidade: é suficientemente distinguível de uma pessoa para outra, mesmo em caso de gêmeos idênticos;
- Permanência: as características não se alteram no decorrer do tempo; e
- Coletabilidade: fáceis de serem coletadas.

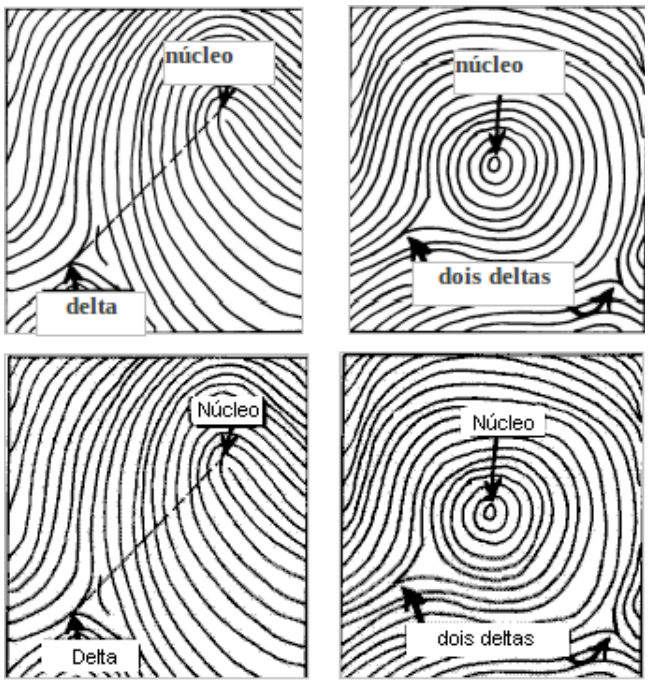
Impressões digitais (ver Figura 3) são feitas de cristas (*ridges*) e vales resultados da fricção dos dedos (linhas papilares) sobre superfícies. Quando uma pessoa toca alguma coisa com seus dedos, geralmente haverá resíduos visíveis ou invisíveis deixados na superfície tocada. O resíduo é cópia da impressão digital e pode ser coletado para posterior estudo e comparação. A formação das papilas é uma combinação de fatores genéticos e ambientais. Mesmo gêmeos possuem impressões digitais diferentes[2].

Figura 3. Um dedo e sua impressão digital (WIKIPEDIA, 2005).

Uma impressão digital pode ser vista em diferentes níveis: global, local e muito fino (SANDSTROM, 2004).

No nível global pode-se observar *pontos de singularidade*, chamados núcleo e delta (ver Figura 4). Esses pontos são muito importantes para classificação de uma impressão digital, mas não são suficientes para um casamento preciso.

Figura 4. Núcleo e delta de uma impressão digital (SANDSTROM, 2004).

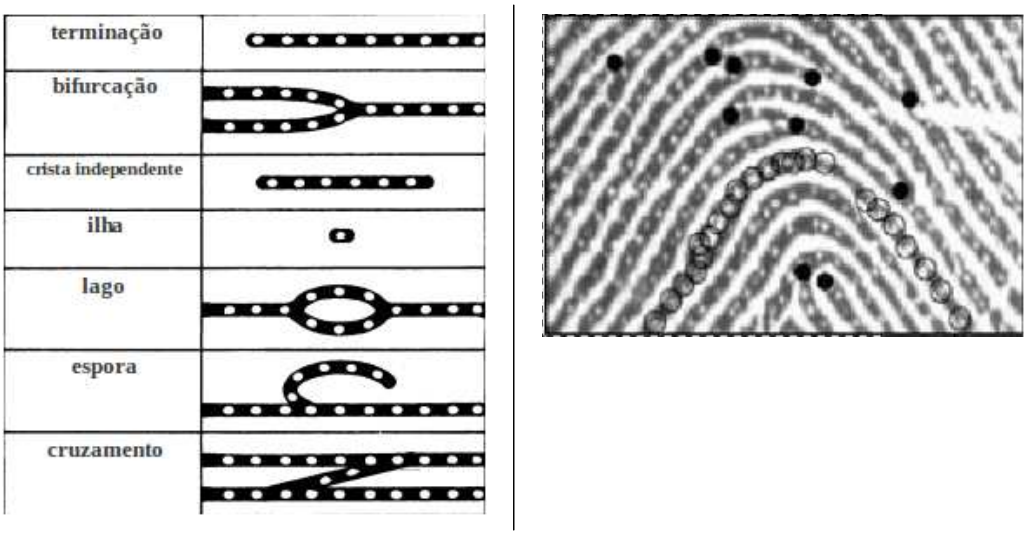


No nível local pode-se observar *minúcias*. As minúcias podem ser: terminação de uma crista, bifurcação, crista independente, ponto ou ilha, lago, espora e cruzamento (Figura 5). As duas minúcias mais importantes são terminação e bifurcação.

[2]http://www.fingerprint.tk

No nível de maior detalhamento há os poros de suor (Figura 5). A posição e a forma dos poros podem ser usadas para ajudar a identificar uma pessoa. Para poder utilizar essa informação, a imagem precisa ser de alta resolução.

Figura 5. À esquerda, minúcias, também conhecidos como detalhes de Galton. À direita, parte de uma impressão digital, onde pode-se observar as linhas pretas correspondem às cristas e as linhas brancas aos vales.



Os pontos brancos são os poros (círculos brancos em uma crista). As minúcias estão marcadas como círculos em preto.

3.1.Classificação

Impressões digitais foram classificadas de várias maneiras através da história. O sistema de classificação de Henry foi a base para os sistemas AFIS modernos. Os novos métodos de classificação usam a distância entre o núcleo e o delta, minúcias e o tipo de impressão digital (através do sistema de Henry).

Impressões digitais podem ser divididas em três grandes classes: arco, laço e verticilo. Essas classes podem sofrer outras subdivisões: arco plano, arco angular, laço à esquerda, laço à direita, espirais e mistos.(Figura 6)

Figura 6. Verticilo, laço à esquerda, laço à direita, arco plano e arco angular (ROSISTEM, 2005).

3.2.Sistema automático de identificação de impressões digitais

Um sistema biométrico é um sistema de reconhecimento de padrões que opera sobre dados biométricos adquiridos de um indivíduo, extrai um conjunto de características e compara essas características com as armazenadas em um banco de dados. Um sistema biométrico pode operar no modo de verificação ou de identificação:

- No modo de verificação, o sistema valida a identidade de uma pessoa comparando a informação biométrica capturada com a informação do próprio usuário previamente armazenada no banco de dados. O sistema realiza uma comparação um-para-um.

- No modo de identificação, o sistema reconhece um indivíduo pesquisando o conjunto de características de todos os cadastrados no banco de dados em busca de um casamento. O sistema realiza uma comparação um-para-muitos para estabelecer a identidade de um indivíduo.

Um sistema automático de identificação de impressões digitais (AFIS) consiste em três estágios fundamentais:

- aquisição da imagem da impressão digital;

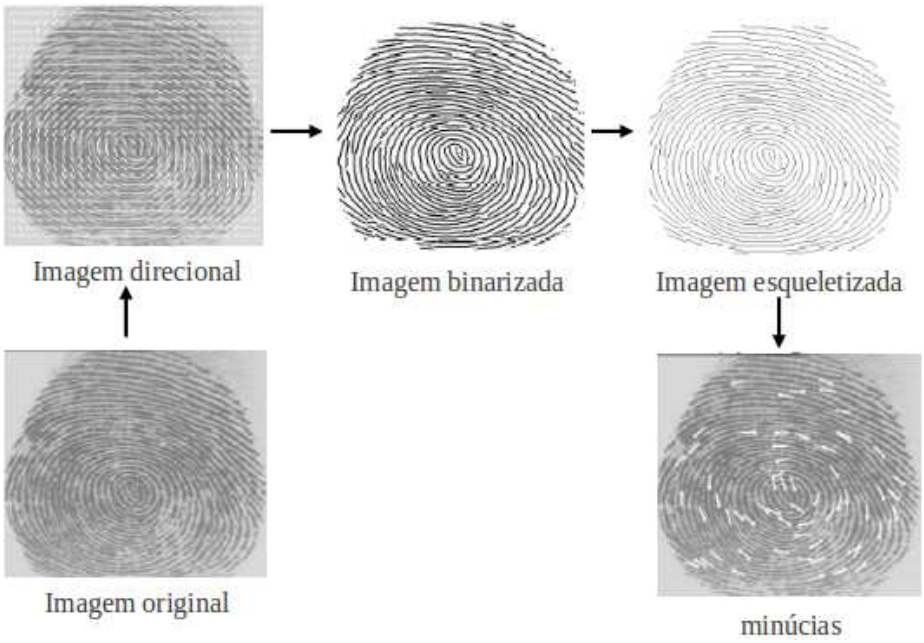
- extração das características;

- tomada de decisão, onde as características da imagem de consulta são comparadas com as características armazenadas no sistema. Esta comparação é quantificada, de forma que se ficar acima de um certo limiar, as imagens são consideradas terem se originado do mesmo dedo.

Freqüentemente, o banco de dados é particionado segundo informações extras (sexo, idade) ou intrínsecas às impressões digitais (classes, por exemplo).

A maioria dos AFIS segue os mesmos estágios básicos para identificação de uma impressão digital.

Figura 7. Sequência de operações para extração de minúcias (JAIN, HONG & BOLLE, 1997).



Existem várias abordagens para tratar uma imagem de impressão digital a fim de obter o vetor de características, visando um futuro casamento com impressões previamente armazenadas em um banco de dados. Os sistemas clássicos (YAGER & AMIN, 2004) de verificação de impressões digitais automáticos efetuam basicamente as seguintes operações (Figura 7):

- Aquisição: o método tradicional para obter impressões digitais é realizado através da rolagem do dedo *tintado* sobre cartões de coleta. Para sistemas automatizados, usa-se scanners, que são mais rápidos e de baixo custo.

- Representação: as impressões devem ser armazenadas de forma eficiente e compacta. O FBI desenvolveu uma forma de compactar as imagens baseada na compressão por *wavelets* (FBI, 1993). Uma outra maneira pode ser armazenar apenas as características extraídas, mais apropriado para

sistemas em tempo real, pois o pré-processamento e a extração de características são executadas apenas uma vez. Também é possível armazenar tanto a imagem quanto as características.

- Pré-processamento: a qualidade de uma impressão digital pode ser um fator decisivo na fase de extração de características. Há muitas pesquisas sendo desenvolvidas coma finalidade de melhorar a imagem de uma impressão digital. Em nível regional, as cristas e vales que compõem uma impressão digital possuem freqüência e orientação bem definidas. Portanto, é natural usar ferramentas de análise de frequência para melhorar a imagem, como (GONZALEZ & WOODS, 2001) transformadas de Fourier, filtros de Gabor e *wavelets*. Outros passos úteis são equalização de histogramas e filtragem laplaciana. Estimação da orientação das cristas, binarização e afinamento são etapas importantes no pré-processamento.

- Extração de características: tais características são as minúcias já discutidas na Seção 3.

- Casamento: o objetivo final de um AFIS é encontrar ou confirmar a identidade de uma pessoa cujas impressões digitais foram submetidas ao sistema. Em última análise, isto significa comparar as características de duas impressões e determinar a probabilidade de que elas tenham partido do mesmo dedo.

3.3.Técnicas para melhoramento da imagem

Para uma boa extração das minúcias de uma impressão digital é importante que a imagem tenha qualidade e confiabilidade. Várias técnicas podem ser aplicadas para o melhoramento da imagem: filtros (contraste, Gabor, *wavelets*), operações morfológicas (binarização, afinamento), aplicados pontualmente ou por área. Considera-se o bloco de extração de minúcias crucial, devendo, portanto, ser imune a qualquer interferência na imagem ou erro de extração.

O filtro de contraste tem como objetivo principal aumentar a discriminação visual entre os objetos contidos em uma imagem. Por exemplo, pode-se considerar uma certa vizinha do *pixel* (5x5). Se o valor do *pixel* for menor do que a média da região considerada, receberá zero, caso contrário manterá o seu valor original (HONG *et. al.*, 1996).

As operações morfológicas são aplicadas quando se tem interesses na resolução das formas (contornos, padrões geométricos, etc.) dos elementos da imagem.

3.4.Extração de características

O método mais popular para extração de minúcias consiste em usar uma representação binarizada e esqueletizada da imagem. Esses algoritmos consistem geralmente em três passos: estimação da orientação, detecção das cristas e afinamento.

A imagem direcional contém informação sobre as direções regionais das cristas de uma impressão direcional. Um exemplo da imagem direcional pode ser vista na Figura 8.

Figura 8. Imagem de uma impressão digital e sua imagem direcional (YAGER & AMIN, 2004).

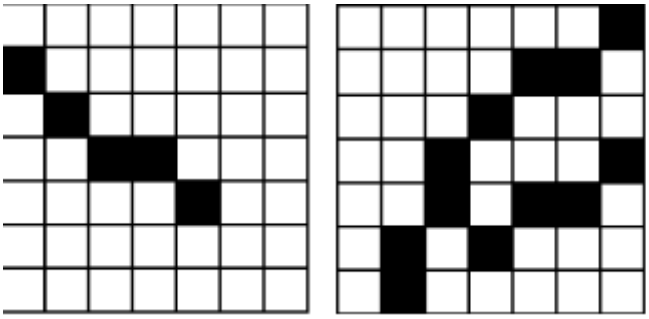
A imagem direcional é largamente utilizada em AFIS e possuem várias aplicações incluindo pré-processamento, classificação de impressões digitais e detecção de cristas. Existem várias técnicas para o seu cálculo. A mais comum baseia-se nos gradientes da imagem (JAIN, HONG & BOLLE, 1997). Outros algoritmos realizam a convolução de máscaras apropriadas para detectar a direção predominante de uma crista. Este último é mais rápido e simples, mas há um limite com relação à quantidade de direções detectadas.

A fim de achar as minúcias é necessário primeiro localizar as cristas. Um mapa de cristas é uma imagem da impressão digital onde os *pixels* pretos correspondem às cristas e os *pixels* brancos correspondem aos vales. Uma solução simples seria aplicar um algoritmo de limiarização (binarização). Como *pixels* dos vales são mais brilhantes do que *pixels* das cristas, qualquer *pixel* acima de um certo valor poderia ser classificado como vale. Contudo, devido à presença de ruídos, o resultado pode ser ruim. Portanto, informação regional do *pixel* deve ser levado em conta para definir deve sele ele pertence a uma crista ou a um vale.

A operação de afinamento (esqueletização) pode ser usada para remover pontos isolados no fundo da imagem e ângulos retos ao longo de borda dos objetos (COSTA, 2001). Um esqueleto (*skeleton*) é uma representação linear de um objeto com largura de um *pixel* e que preserva a topologia do objeto, e dessa forma o esqueleto é criado através do afinamento de uma imagem binarizada.

A extração das minúcias a partir do mapa de cristas afinado é uma tarefa trivial. Qualquer *pixel* preto que possui um único vizinho (8-conexo) é uma terminação e qualquer *pixel* preto com mais do que dois vizinhos é uma bifurcação (ver Figura 9). Infelizmente não é tão simples assim e o processo necessita de filtragem adicional para retirar falsas minúcias.

Figura 9. Terminação e bifurcação (YAGER & AMIN, 2004).



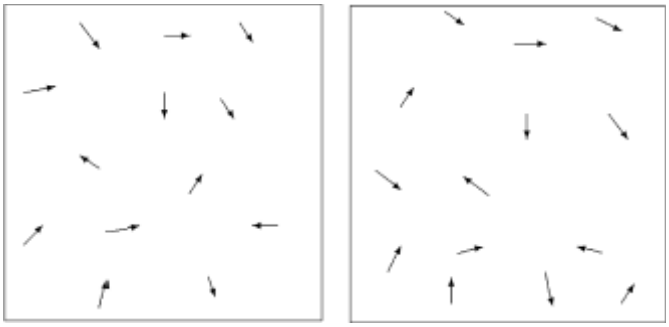
3.5.Casamento de impressões digitais

O resultado do passo de extração de minúcias costuma ser uma lista de locais e orientações, representada pelas coordenadas x e y e o ângulo de orientação #.

É importante observar que a maioria dos sistemas não difere entre terminações e bifurcações quando comparando duas impressões digitais. Uma razão pode ser o ruído ou o excesso de pressão que pode fazer com que uma bifurcação seja vista como uma terminação, ou vice-versa.

Alinhar conjuntos de minúcias é conhecido com registro (ver Figura 10), e é essencialmente um problema de casamento de padrão de pontos (*point pattern problem*). O objetivo é encontrar uma translação, rotação e possivelmente, escala, que alinhe os conjuntos de pontos. Vários algoritmos foram propostos, mas devido ao domínio específico, muitos não são adequados ao problema.

Figura 10. Minúcias de duas impressões digitais que podem ser do mesmo dedo (YAGER & AMIN, 2004).



Após o alinhamento, calcula-se a pontuação do casamento entre duas impressões digitais como na Equação 1 (JAIN, HONG & BOLLE, 1997).

Equação 1. Pontuação do casamento entre digitais

$$pontuação = \frac{100\, N_{correspondentes}}{Max(M, N)}$$

onde $N_{correspondentes}$ é o número de minúcias que casaram, `M` é o número de minúcias de um conjunto e `N`, do outro.

A pontuação requerida para que duas impressões digitais sejam consideradas iguais pode ser um parâmetro ajustável do sistema.

Para os sistemas biométricos comerciais, o desempenho deve ser considerado. Este desempenho pode ser categorizado por duas medidas, a taxa de falsa aceitação (FAR) e a taxa de falsa rejeição (FRR).

- FAR (*False Acceptance Rate*): representa a porcentagem de usuários não autorizados que são incorretamente identificados como usuários válidos e, portanto, aceitos pelo sistema.
- FRR (*False Reject Rate*): representa a porcentagem de usuários autorizados que são incorretamente rejeitados pelo sistema.

4.Conclusões

Reconhecimento de impressões digitais tem sido tema de pesquisa nas áreas de processamento de imagens e de reconhecimento de padrões nos últimos vinte anos, fato que propiciou o surgimento de vários AFIS comerciais bem como seu uso em várias aplicações civis. Mesmo assim, a comunidade científica considera que há muito que melhorar:

- a etapa de extração de minúcias é crucial. Os algoritmos existentes ainda perdem uma quantidade razoável de minúcias ou geram minúcias espúrias. Algumas propostas existentes sobre imagens em tons de cinza têm alcançado resultados similares aos algoritmos baseados em esqueleto, a despeito do menor curso computacional.
- algoritmos de verificação de minúcias podem ter uma etapa de pós-processamento, como por exemplo, confirmar as minúcias extraídas a partir do esqueleto com técnicas de percurso sobre cristas da imagem em tons de cinza.
- soluções híbridas que incorporem, além de impressões digitais, íris, DNA podem aumentar a robustez e confiabilidade nos sistemas.

Agrega-se a isto a crescente preocupação mundial com segurança, o que tem levado países e empresas a investir cada vez mais em sistemas de identificação e verificação de indivíduos.

5.Referências bibliográficas

COSTA, S. M. F. *Classificação e Verificação de Impressões Digitais*. Dissertação (Mestrado em Engenharia Elétrica [SP-Capital]) - Universidade de São Paulo, defendida em 2001. Disponível em http://www.teses.usp.br/teses/disponiveis/3/3140/tde-18032002-102113/publico/dissertacao_Silvia.pdf. Acesso em 09/2005.

FBI (Federal Bureau of Investigation). *WSQ gray-scale fingerprint image compression specification*. Document IAFISIC-0110v2. Disponível em: ftp://ftp.c3.lanl.gov/pub/misc/WSQ/documents/wsqSpec2.ps. Acesso em 09/2005.

GALTON. *Sir Francis Galton F. R. S.*. Disponível em: http://galton.org/. Acesso em 09/2005.

GONZALEZ, R. & WOODS, R. *Digital Image Processing*. Second Edition, Upper Saddle River: Prentice-Hall Inc., 2001.

HONG, L.; JAIN, A.; PANKANTI, S. & BOLLE, R. *Fingerprint Enhancement*. Proceedings of Third IEEE Workshop on Applications of Computer Vision, pp. 202-207, Sarasota, FL, 1996.

JAIN, A.; HONG, L. & BOLLE, R.. *On–Line Fingerprint Verification.*. In: IEEE Transactions on Pattern Analysis and Machine Intelligence, vol.19, nº 4, pp. 302-313, 1997.

JAIN, A.; HONG, L.; PANKANTI, S. & BOLLE, R.. *An Identity-Authentication System using Fingerprints*. Proceedings of the IEEE, vol. 85, nº 9, pp. 1365-1388, 1997.

JAIN, A.; ROSS, A. & PRABHAKAR, S. *An Introduction to Biometric Recognition*. In: IEEE Transactions on Circuits and Systems for Video Technology, Special Issue on Image- and Video-Based Biometrics, Vol. 14, No. 1, January 2004.

OLIVEIRA, M. & LEITE N. *Reconnection of Fingerprint Ridges Based on Morphological Operators and Multiscale Directional Information*. SIBGRAPI, pp. 122-129, Computer Graphics and Image Processing, XVII Brazilian Symposium on (SIBGRAPI'04), 2004.

PRABHAKAR, S. *Fingerprint Classification and Matching Using a Filterbank*. Dissertação de doutorado – Michigan State University. 2001. Disponível em: http://citeseer.ist.psu.edu/482312.html. Acesso em 09/2005.

SANDSTROM, M. *Liveness Detection in Fingerprint Recognition Systems*. Dissertação – Linköping University. 2004. Disponível em: http://www.diva-portal.org/liu/undergraduate/abstract.xsql?dbid=2397. Acesso em 09/2005.

ROSISTEM. *Bar Cod – Biometric Education*. Disponível em: http://www.barcode.ro/tutorials/biometrics/fingerprint.html. Acesso em 09/2005.

WIKIPEDIA. *Fingerprint*. Disponível em: http://en.wikipedia.org/wiki/Fingerprint. Acesso em 09/2005.

YAGER, N. & AMIN, A. *Fingerprint verification based on minutiae features: a review*. In: Pattern Analysis and Applications, Ed. Sameer Singh. Springer, Germany, 2004, vol.7 pp. 94 – 113.