Vulnerabilidades em Sistemas Biométricos Baseados em Impressões Digitais

Mario T. Shimanuki
Instituto Tecnológico de Aeronáutica
Divisão de Engenharia Eletrônica
e-mail: explorer@ita.br

Angelo S. Zanini
Instituto Tecnológico de Aeronáutica
Divisão de Engenharia Eletrônica
e-mail: azanini@ita.br

***Abstract*— Fingerprint, which have been used for about 100 years, are the oldest and is known to be the most representative biometric signs of identity. Fingerprint serves the purpose of recognizing individual in applications including law enforcement, banking, and security. Potential threats caused by something like real fingers, which are called fake or artificial fingers, should be crucial for authentication based on fingerprint system. The aim of this paper is to discuss some relevant points concerned with the security of a biometric system that is not discussed by many researchers but it is far too much important.**

I. Introdução

Todos nós temos características biométricas, tais como impressões digitais, íris/retina, voz, face, entre outros.

Qualquer característica fisiológica ou comportamental pode ser utilizado para identificar indivíduos desde que satisfaça os seguintes requisitos [1], [2], [3]:

1) **Universalidade**: todas os indivíduos tem que ter estas características.
2) **Unicidade**: cada individuo tem que ter a sua própria característica, ou seja, não deve haver dois indivíduos com as mesmas características.
3) **Permanência**: as características devem ser invariantes no tempo.
4) **Coletabilidade**: as características podem ser mensuradas quantitativamente.

Os sistemas de biometria tiveram um grande destaque nas últimas décadas [1], [2]. Basicamente os sistemas biométricos são utilizados para a autentificação ou identificação.

Existem aplicações que necessitam um grau de confiabilidade e segurança muito grandes. Com o intuito de aumentar o grau de confiabilidade e segurança de sistemas biométricos baseados em impressões digitais, são analisados alguns tipos de ataques nestes tipos de sistemas.

II. Sistemas Baseados em Impressões Digitais

Uma das características biométricas mais antigas é a impressão digital [4]. Este teve o seu estudo iniciado no século XVI [3], no entanto os fundamentos modernos para a identificação de impressões digitais foram estabelecidas pelos estudos de Sir F. Galton [5] e E. Henry [6] no final do século XIX.

Os estudos de Henry estabeleceram o "Sistema Henry", através do qual foi possível classificar as impressões digitais. No início do século XX, as impressões foram formalmente aceitas como sinais de identificação [3].

A identificação manual das impressões digitais exigiam muito trabalho e deveria ser executado por um profissional experiente. Em 1960 o *FBI Home Office* (UK)e o "Paris Police Departament" iniciaram um estudo sobre um sistema de identificação automático [7].

Dentre os tipos de sistemas biométricos, a impressão digital é o sistema que possui menor Custo x Confiabilidade, fato pelo qual tornou-se popular.

Os tipos mais comuns de sensores biométricos para impressões digitais são os ópticos e capacitivos. Na primeira as minúcias são adquiridos por meio da digitalização da impressão e o outro através da diferença da capacitância entre os vales (planos) e cumes (elevações) das impressões.

A. Características das Impressões Digitais

As minúcias são características das impressões digitais, identificadas nos estudos de Galton. As minúcias de um indivíduo são permanentes, ou seja, são preservadas desde do nascimento até a morte [5]. Foi também provado que duas pessoas não possuem a mesma impressão digital. Os estudos de Galton satisfazem os requisitos dos sistemas biométricos. Galton classificou as minúcias em 8 tipos, conforme mostrado na 1.

Feature	Dot	Ridge End	Island	Bifrucation
Sample				

Feature	Short Ridge	Crossover	Bridge	Spur
Sample				

Fig. 1. Minúcias das impressões digitais

Henry, em suas pesquisas, classificou as impressões digitais e as dividiu em 5 grupos:

1) *Right Loop* (R)
2) *Left Loop* (L)
3) *Whorl* (W)
4) *Arch* (A)
5) *Tented Arch* (T)

Fig. 2. *Right loop*

Fig. 3. *Left loop*

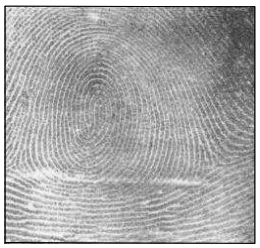

Fig. 4. *Whorl*

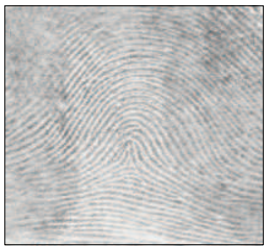

Fig. 5. *Arch*

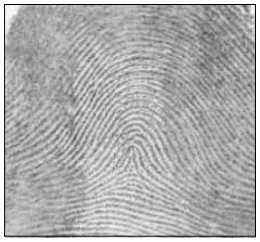

Fig. 6. *Tented Arch*

Existem outras características das impressões digitais além das estudadas por Galton e Henry, como por exemplo o *core* e *os deltas*. O *core* é o ponto central das impressões digitais juntamente com os *deltas*, que são os centros de regiões triangulares, utilizados como referencial para ajuste das imagens.

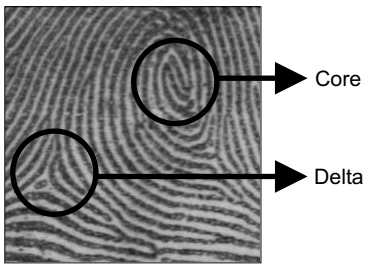

Fig. 7. Características *Core* e *Delta*

A imagem da impressão digital capturada e cadastrada no sistema, poderá não estar em uma mesma posição, sendo necessário transladar e/ou rotacionar a imagem tendo como referência os pontos *core* e *deltas*.

A maneira mais antiga de coletar impressões digitais é passar um rolete de tinta nos dedos e pressiona-los contra uma folha de papel. Atualmente, existem meios mais sofisticados de se obter as impressões digitais, tais como utilizar os sensores CCD (*Charge-Couple Device*) [8]. Uma maneira mais simples de se obter as impressões digitais é digitalizando as impressões em papel através de um *scanner*. No entanto, este método aumenta a probabilidade de se ter imagens distorcidas.

As imagens de uma mesma impressão digital possuem diferenças devido as causas relacionadas abaixo [9], [8]:

1) Translação: devido a diferentes posições do polegar no dispositivo de aquisição de impressão digitais.
2) Rotação: devido a diferentes posições do polegar no dispositivo de aquisição de impressão digitais.
3) Pressão: pela pressão em que o polegar exerce no sensor.
4) Contraste: devido a pressão dos dedos e densidade da tinta nos métodos baseados em tinta.
5) Diferentes regiões: durante a aquisição da imagem alguns pontos podem não ser coletados corretamente, ou seja, a aquisição da imagem é parcial.
6) Distorções: durante a aquisição das imagens, alguns pontos podem estar levemente distorcidos.
7) Perturbações locais: devido a não uniformidade (pressão, rotação, transação, etc), na aquisição.
8) Interrompimentos da minúcias: causada pela não uniformidade do polegar no sensor.
9) Distorção semi-permanentes: por problemas de cicatrizes, suor, doenças de pele, etc.

B. Identificação e Autentificação

Em sistemas automáticos de autentificação e identificação, as minúcias são restritas a dois tipos: "*ridge ending*" e "*bifurcation*". Os outros tipos de minúcias podem ser expressas a partir destes dois tipos [7].

Existem cerca de 50 a 150 minúcias em uma impressão digital. Nos sistemas automáticos 10 coincidências são o suficientes para se estabelecer a identidade [10].

As formas de se classificar uma impressão digital por um sistema automático são:

1) Método sintático [11], [12], [13]: os padrões e minúcias são aproximados a uma *string* de primitivas, a partir disto são modeladas a produção de regras para a classificação.
2) Método estrutural [14], [15]: os traços baseados nas minúcias são extraídos e então representados por uma estrutura de dados gráficos.
3) Redes neurais [16], [17]: é gerado um vetor a partir das minúcias e classificadas por uma rede neural.
4) Classificador estatístico: é utilizado a transformada de Fourier hexagonal sobre a imagem e então classificada.

C. Extração de minúcias

A partir de uma imagem de uma impressão digital é possível extrair as minúcias da mesma, conforme fig. 8.

A extração é feita localizando-se as minúcias e armazenado a sua posição através de coordenadas cartesianas (X e Y) e ângulo em que esta se encontra.

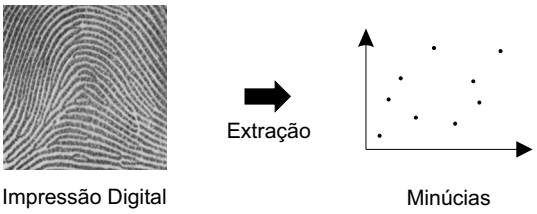

Fig. 8. Extração das minúcias

O sistema automático realiza um pré-processamento para extrair as minúcias de uma impressão digital. O pré-processamento inclui filtragem para eliminar ruídos, binarização da imagem e coleta de informações essenciais. Após o pré-processamento é utilizado um algoritmo para extração e classificação das minúcias.

Feito o pré-processamento da imagem é possível utilizar um algoritmo para a extração e classificação das minúcias.

Uma fonte causadora de erros no reconhecimento de impressões digitais é a falsa minúcia. Falsas minúcias são inevitáveis devido à distorções nas imagens provocadas por cicatrizes, suores, doenças na pele, etc [4]. Para evitar estes tipos de erros alguns algoritmos trabalham com sistemas de eliminação de falsas minúcias.

III. Tipos de Ataques

Geralmente, sistemas biométricos baseados em impressões digitais possuem as seguintes fases:

1) Capturar a imagem;
2) Extrair as minúcias da imagem;
3) Criptografar as minúcias;
4) Transmitir por um canal de comunicação;
5) Armazenar os dados da impressão digital em um banco de dados.

Os ataques em sistemas biométricos podem ocorrer em diversos pontos do processamento e são divididos em 3 grupos [18]:

1) Ataques por meio de impressões digitais artificiais: existem vários métodos que permitem a construção de uma impressão digital artificial;
2) Ataques no banco de dados: os dados armazenados podem ser alterados e ou modificados;
3) Ataques na interface: durante a formação da imagem da impressão digital pode existir um sistema que intercepta e modifica os dados da imagem.

IV. Metodologia Utilizada

Para montagem do experimento foi utilizado um mouse da Siemens (*Siemens Id Mouse*), que possui um sensor capacitivo, e a API (*Application Program Interface*) ID Device SDK 1.9 [19].

O diagrama de blocos simplificado dos processos de autentificação e identificação são mostrados nas Fig. 9 e 10.

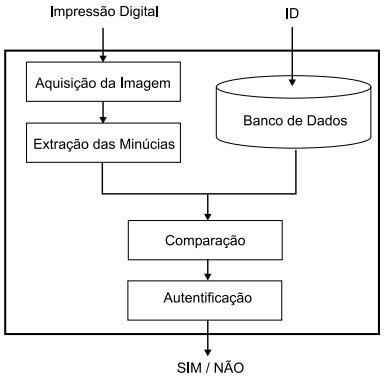

Fig. 9. Diagrama de blocos de um sistema de autentificação

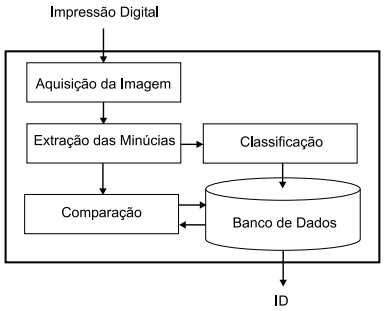

Fig. 10. Diagrama de blocos de um sistema de identificação

Foram simulados ataques por meio de impressões digitais artificiais e os ataque à base de dados.

A. Impressões Digitais Artificiais

Para construção das impressões digitais artificiais foram criados moldes de silicone e goma de mascar. Os moldes representam uma imagem negativa da impressão digital. Para formar o positivo foi preparado uma gelatina em pó incolor sem sabor. Após a preparação da gelatina este foi colocado no molde. Devido ao rápido processo de gelatinação foi possível obter uma impressão digital artificial em poucos minutos.

Com as impressões digitais artificiais criadas existem duas formas de ataques ao sistema. A primeira forma é o ataque ao cadastro da impressão digital original, onde é realizado uma atentificação utilizando-se a impressão digital artifical.

A segunda forma é executar o processo inverso, ou seja, o cadastramento é realizado com a impressão digital artificial e realizada uma autentificação utilizando a impressão digital original. Com a gelatina é possível gerar uma imagem positiva da impressão digital perfeita, mas devido a sua temperatura baixa, o sensor não consegue realizar a aquisição da imagem da impressão digital em alguns momentos.

Outros materiais podem ser utilizados para conseguir construir um dedo artificial [20].

B. Ataque à base de dados

No sistema utilizado, as minúcias são armazenadas em um banco de dados. Um programa em paralelo que extrai as

minúcias de uma impressão (impressão real ou imagem), e substitui um item do banco de dados, conseguimos burlar o sistema, como mostra a Fig. 11.

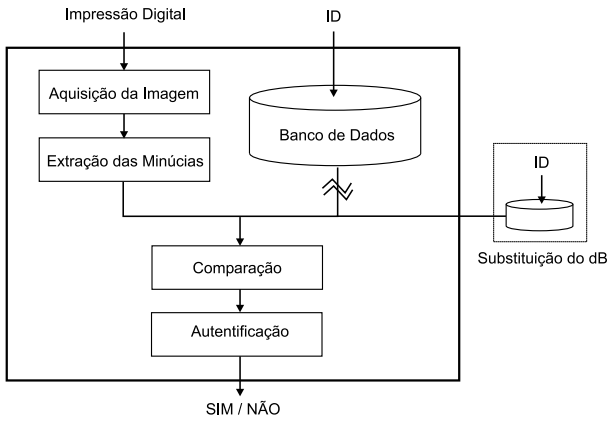

Fig. 11. Ataque à base de dados

Neste tipo de ataque é necessário que haja acesso ao banco de dados.

V. Análise de Resultados

A acurácia da autentificação de um sistema de impressões digitais é medido através das taxas de falsa rejeição (FRR - *False Rejection Rate*) e falso aceite (FAR - *False Acceptance Rate*). A FAR é um importante indicador para a segurança contra usuários não autorizados [21].

Na Fig. 12 são mostrados as taxas de falso aceite, falsa rejeição e Id indefinidos em 3 níveis de segurança (quanto menor o número do nível mais seguro é o sistema).

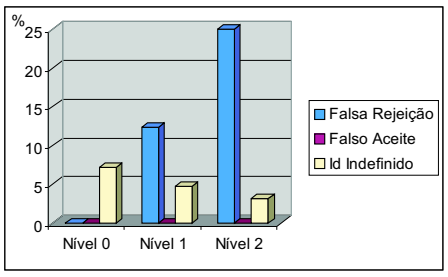

Fig. 12. Eficiência X Segurança

Estes dados foram coletados em um grupo de 150 amostras em cada teste, sob condições de uso habituais (sem a limpeza do sensor após cada amostra e pressionando-se o dedo em posições distintas).

Nos 3 níveis testados (nível 1, nível 2 e nível 3) o FAR foi igual à zero. No entanto, para uma melhor estatística, tornam-se necessários:

1) Utilizar um banco de dados com um número maior de impressões cadastradas;
2) Aumentar o frequência de repetições dos testes.

O maior risco em sistemas biométricos baseados em impressões digitais está em uma pessoa maliciosa por intimidação ou coação à um usuário legítimo forçá-lo a pressionar o seu próprio dedo no sensor fazendo com que o sistema autentifique-o. Isto pode ser evitado com a combinação de outras técnicas de autentificação como PIN, *passwords* e *ID cards*. No entanto vale ressaltar que temos que mediar Eficiência X Segurança, um sistema com alto grau de segurança pode não ser o mais eficiente.

A. Burlando o sistema com um dedo artificial

Foi conseguido autentificar/identificar uma impressão digital que consta no banco de dados do sistema com uma cópia desta impressão por meio de um dedo artificial. Desta forma fica evidenciado a possibilidade de se burlar o sistema.

Um meio preventivo para este tipo de ataque seria a utilização de outros sensores em paralelo medindo outras funções da pele humana, a identificação/validação somente se daria com dedos verdadeiros.

B. Burlando o sistema por ataques ao bando de dados

Tendo-se acesso ao banco de dados, torna-se possível a substituição de minúcias no mesmo.

Um meio preventivo para este tipo de ataque seria a utilização de funções *hash* [22], [23], [24] juntamente com as minúcias, impossibilitando assim que o arquivo seja modificado.

As funções *hash* são funções que produzem uma saída fixa independente do tamanho do texto de entrada e são computacionalmente inviáveis de calcular a inversa desta função.

VI. Conclusão

Fica evidenciado que a segurança da informação em sistemas biométricos merecem uma atenção em especial durante a fase de projeto.

Métodos biométricos utilizando a impressão digital para autentificação/identificação não devem ser utilizados para ambientes que requeiram alta prioridade de segurança.

References

[1] CLARKE, R. Human identification in information systems: Management challenges and public policy issues. *Info Technology People*, p. 6–37, 1994.
[2] MILLER, B. Vital signs of identity. *IEEE Spectrum*, IEEE Spectrum, p. 22–30, 1994.
[3] LEE, H. C.; GAENSSLEY, R. E. *Advances in Fingerprint Technology*. [S.l.]: Elsevier, 1991.
[4] HALICI, U.; JAIN, L. C.; EROL, A. *Introduction to fingerprint recognition*. [S.l.]: CRC Press, 1999.
[5] GALTON, F. Finger prints. *Macmillan*, 1892.
[6] HENRY, E. R. Classification and uses of finger prints. *Routledge*, 1900.
[7] FBI. The science of fingerprints: classification and uses. *Federal Bureau of Investigation*, 1984.
[8] JAIN, A. K. et al. An identity-authentication system using fingerprints. *Proceding of the IEEE*, p. 1365–1388, 1997.
[9] EROL, A. *Automated fingerprint recognition*. Tese (Doutorado) — Middle East Technical University, Ankara, 1998.
[10] BALDI, P.; CHAUVIN, Y. Neural networks for fingerprint recognition. *Neural Computation*, p. 402–418, 1993.
[11] BLUE, J. L. et al. Evaluation of pattern classifiers for fingerprint and ocr applications. *Pattern recognition*, p. 485–501, 1994.

[12] MOAVER, B.; FU, K. S. An application of stochastic languages to fingerprint pattern recognition. *Pattern recognition*, p. 173–179, 1976.
[13] MOAYER, B.; FU, K. S. A tree system approach for fingerprint recognition. *IEEE Transactions on pattern analysis and machine intelligence*, p. 376–387, 1986.
[14] HRECHAK, A. K.; A. MCHUGH j. Automated fingerprint recognition using structural matching. *Pattern recognition*, p. 893–904, 1990.
[15] RAO, T. C. Feature extraction for fingerprint classification. *Pattern recognition*, p. 181–192, 1976.
[16] FREEMAN, J. A.; SKAPURA, D. M. *Neural Networks: Algorithms, applications, and programming techniques*. [S.l.]: Addison-Wesley, 1991.
[17] HALICI, U.; GELENBE, E. *Lecture notes on neurocomputers*. [S.l.], 1998.
[18] THALHEIM, L.; KRISSLER, J.; ZIEGLER, P. M. Body check: Biometrics defeated. *Germany's c't blows through 11 biometric systems*. Disponível em: <http://www.extremetech.com/article2/0,3973,13919,00.asp>.
[19] SIEMENS AG. Information security: Id device software development kit (sdk). 2002.
[20] MATSUMOTO, T. et al. Impact of artificial "gummy" fingers on fingerprint systems. Disponível em: <http://www.totse.com/en/bad_ideas/locks_and_security/164704.html>.
[21] SIEMENS AG. Biometric performance of id device sdk 1.9: Application hints. 2002.
[22] SCHNEIER, B. *Applied cryptography: protocols, algorithms, and source code in C*. Second edition. New York: John Wiley & Sons, Inc., 1996.
[23] MENEZES, A.; OORSCHOT, P. van; VANSTONE, S. *Handbook of applied cryptography*. Boca Raton: CRC Press, 1997.
[24] STALLINGS, W. *Cryptography and network security: Principles and practice*. Second edition. New Jersey: Prentice Hall, 1999.