INTERFACE TECNOLÓGICA
volume 10 - número 1 - 2013

UM ESTUDO SOBRE A BIOMETRIA

A STUDY ON BIOMETRICS

Fábio José Colombo[1]
Brazelino Bertolete Neto[2]
Luciano de Jesus Rodrigues de Barros[3]

RESUMO

Este artigo tem por finalidade apresentar o conceito de biometria. Como é possível distinguir um indivíduo do outro através das suas características físicas é um conceito que existe desde os primórdios. O termo biometria está cada dia mais próximo do cotidiano dos usuários de informática. A biometria vem justamente aproveitar as características únicas das pessoas para garantir segurança e velocidade em muitas atividades diárias.

PALAVRAS-CHAVE: Senha. Segurança. Autenticação. Confiabilidade. Fiscalização.

ABSTRACT

This paper aims to present the concept of biometrics and how it is possible to distinguish one individual from another by their physical characteristics. This is a concept that has existed since the early days. The term biometrics is getting closer to the daily lives of computer users. Biometrics comes precisely take the unique characteristics of the people to ensure safety and speed in many daily activities.

KEYWORDS: *Password. Security. Authentication. Reliability. Supervision.*

[1] Professor do Centro de Educação Tecnológica Paula Souza, Pós Graduado em Análise de Segurança Digital. Endereço: Rua José Mendes F. Júnior, 63 Parque Residencial Laranjeiras Taquaritinga-SP. E-mail: fabio.colombo@fatectq.edu.br
[2] Professor do Centro de Educação Tecnológica Paula Souza, Pós Graduado em Análise de Segurança Digital. Endereço: Rua General Osório, 517 Centro Taquaritinga-SP. E-mail: brasa_tq@yahoo.com.br
[3] Professor do Centro de Educação Tecnológica Paula Souza, Pós Graduado em Gestão em Sistemas de Informação. Endereço: Rua Dr. Alderico Previdelli, nº 188 - Jardim Bela Vista Taquaritinga-SP. E-mail: lennontaqua@hotmail.com

INTRODUÇÃO

Concordando com Alecrim (2005), a informática, ao longo dos anos, vem adquirindo mais relevância na vida das pessoas e empresas, sua utilização traz um grande ferramental para o desempenho das ações das organizações. A biometria traz facilidade, rapidez e confiabilidade nos processos de identificação de pessoas nos vários segmentos informatizados da sociedade.

A identificação de pessoas não pode ser comprovadamente verídica apenas com papéis facilmente falsificáveis. A constante evolução ajuda na busca de métodos automatizados para reconhecer pessoas com base em características fisiológicas, sendo chamada de biometria.

A identidade (*id* do latim isto, este; entidade de ente, ser, o que existe) biométrica é a forma mais precisa para se provar quem somos, trata-se de um estudo estatístico das qualidades comportamentais e físicas do ser humano. Segundo o dicionário Michaelis, biometria é a ciência da aplicação de métodos de estatística quantitativa a fatos biológicos.

Biometria, derivado do grego, *bio* (vida) e *metric* (medir), faz referência a um sistema automatizado que pode identificar uma pessoa mediante características físicas e/ou comportamentais, comparando-as com aquelas que estão registradas.

Sistemas biométricos verdadeiros começaram a surgir na última metade do século XX, coincidindo com o surgimento de sistemas de computador.

Entre os recursos medidos estão eles: face, impressões digitais, geometria da mão, assinatura, retina, íris, voz e outras características que poderão ser mensuradas com a evolução da tecnologia.

FUNCIONAMENTO BÁSICO DO SISTEMA BIOMÉTRICO

De acordo com Costa (2001), como método alternativo ao uso das senhas, surge a utilização de cartões magnéticos que são facilmente fraudáveis e o problema de usuários mal intencionados conseguirem roubar esses artefatos e se passarem por outro se mantém.

Na Ilustração 1, temos um quadro que resume os três tipos básicos de autenticação:

Tipo de Solução	Resumo	Exemplo
Soluções de Autenticação Baseadas no Conhecimento	O que se sabe	Senhas
Soluções de Autenticação Baseadas na Propriedade	O que se tem	Tokens, cartões, chips
Soluções de Autenticação Baseadas em Características	O que se é	Biometria

Ilustração 1. Resumo dos tipos básicos de autenticação

Fonte: Elaboração Própria

Concordando com Costa (2001), os diversos métodos biométricos tem um processo de funcionamento similar, dividido em quatro etapas: captura, extração, comparação e combinação/não-combinação.

A captura consiste no armazenamento de uma característica biológica do indivíduo, física ou comportamental (coleta da impressão digital, da imagem da íris ou da face, gravação da voz, entre outras), extraindo atributos únicos que são então convertidos pelo sistema biométrico em um código matemático que então é armazenado como um *template* biométrico do indivíduo.

Uma vez que o usuário está registrado e necessita ser autenticado, sua característica física é capturada pelo sensor e a informação analógica do sensor é então convertida para sua representação digital *template*. A seguir, esta representação digital é comparada com o modelo biométrico armazenado. Tipicamente o *template* não confere exatamente com o modelo armazenado, como geralmente há alguma variação na medida, estes sistemas não podem exigir uma comparação exata entre o modelo original armazenado e a amostra corrente. Ao invés disso, a amostra corrente é considerada válida se estiver dentro de certo intervalo estatístico de valores. Um algoritmo de comparação é usado para determinar se um usuário verificado é o mesmo que foi registrado.

O algoritmo produz um resultado e demonstra o quanto a amostra se parece com o modelo original. Se o resultado for aceitável, uma resposta afirmativa é dada. É possível configurar o nível do valor de aceitação. Se este nível for baixo o dispositivo biométrico pode falhar e autorizar uma amostra inválida. Se este nível for muito alto, os usuários podem ter problemas na autenticação.

CARACTERÍSTICAS GERAIS DOS SISTEMAS BIOMÉTRICOS

Segundo Mounina (1999), para que as características do ser humano possam ser usadas como forma de reconhecimento digital, devem possuir os seguintes requisitos:

- **Universalidade:** deve existir em todas as pessoas;
- **Singularidade:** deve ser distinta em cada pessoa;
- **Permanência:** não pode variar com o tempo;
- **Mensurabilidade:** pode ser medida.

Na teoria todos os quesitos citados acima bastam, mas na prática, para que o sistema seja adotado funcionalmente, devem ser observados outros pontos importantes:

- **Desempenho:** os fatores ambientais que afetam a precisão da identificação;
- **Aceitabilidade:** refere-se a aceitação do sistema pelos usuários;
- **Proteção:** técnicas de segurança.

Além dos equipamentos, o sistema biométrico possui um software de operação, que inclui o algoritmo

matemático que irá checar a amostra coletada, contra um modelo (*template*) previamente cadastrado.

A Ilustração 2 demonstra o relacionamento dos sistemas biométricos e as suas características gerais.

Sistema	Universalidade	Singularidade	Permanência	Mensurabilidade	Desempenho	Aceitabilidade	Proteção
Face	Alto	Baixo	Médio	Alto	Baixo	Alto	Baixo
Impressão Digital	Médio	Alto	Alto	Médio	Alto	Médio	Alto
Geometria da Mão	Médio	Médio	Médio	Alto	Médio	Médio	Médio
Veias da Mão	Médio	Médio	Médio	Médio	Médio	Médio	Alto
Íris	Alto	Alto	Alto	Médio	Alto	Baixo	Alto
Retina	Alto	Alto	Médio	Baixo	Alto	Baixo	Alto
Assinatura	Baixo	Baixo	Baixo	Alto	Baixo	Alto	Baixo
Voz	Médio	Baixo	Baixo	Médio	Baixo	Alto	Baixo

Ilustração 2. Relacionamento dos sistemas biométricos e as suas características gerais

Fonte: http://penta.ufrgs.br/pesquisa/fiorese/autenticacaoeadcap2.htm (2005)

FORMAS DE IDENTIFICAÇÃO BIOMÉTRICAS

Para Costa (2001), a identificação de uma pessoa nos mais variados sistemas biométricos pode ser feita utilizando-se os métodos de verificação ou identificação, diferenciando-se entre sí apenas na forma de busca. A Ilustração 3 mostra de forma gráfica como funcionam estas etapas.

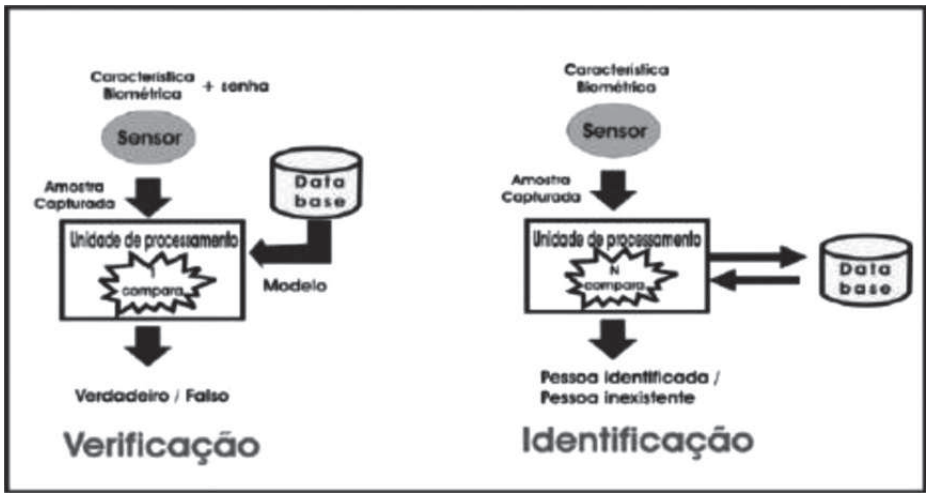

Ilustração 3. Etapas da Verificação e da Autenticação

Fonte: Institute Biometric Group, 2006

Concordando com Costa (2001), a verificação (ou autenticação), que pode ser entendida como comparação **1 para 1**. Este método funciona quando o indivíduo fornece ao software biométrico

sua característica biométrica e um elemento de identificação que pode ser um código ou um cartão identificador, então o software biométrico transforma a característica em *template* e busca um registro no banco de dados através do código identificador. E, por último, faz a comparação com um único elemento do banco de dados, tornando assim o processo de identificação muito rápido.

Já no método identificação conhecido como comparação **1 para N**, é fornecida somente a característica biométrica do usuário ao sistema biométrico que faz a transformação em *template* e em seguida posiciona-se no primeiro elemento do banco de dados e começa a fazer a comparação do *template* fornecido com cada um dos elementos do banco. Somente quando a busca tem sucesso o sistema fornece como verdadeira a identificação. Este método é bastante utilizado em sistemas de identificação de usuários de locadoras, academias e identificação de criminosos. Porém, este método é bastante demorado, dependendo da quantidade de elementos para a comparação.

PROCESSO DE COMPARAÇÃO EM BIOMETRIA

Concordando com Vigliazzi (2006), independente do método, identificação ou verificação, a formula para se dizer se uma amostra da característica biométrica fornecida e comparada à outra armazenada no banco de dados se dá pelo *score* mínio de comparação, ou seja, quando comparadas as amostras, existe um valor de configuração padrão mínimo para determinar o quanto elas são parecidas. Se o *score* for abaixo do valor determinado a comparação resulta como falsa e se for maior ou igual verdadeira.

Este *score* deve ser configurável nos sistemas biométricos, pois fatores externos como cansaço, posição e stress, dependendo do tipo de característica, podem influenciar na extração da amostra a ser comparada. Sendo assim o software do sistema biométrico deve determinar o quanto a amostra se parece com a armazenada e só assim com o auxílio do *score* determinar se a comparação é verdadeira ou falsa.

ANÁLISES ESTATÍSTICAS EM BIOMETRIA

De acordo com o Biometric Institute Group (2006), um aspecto importante que deve ser considerado na escolha de um sistema biométrico é a taxa de erros. Ela é organizada em:

- **Taxa de falsa aceitação** (FAR – *False Acceptance Rate*): essa taxa considera a fração de usuários não-autorizados que foram incorretamente identificados como autorizados.
- **Taxa de falsa rejeição** (FRR – *False Rejection Rate*): representa a percentagem de usuários que deveriam ser autorizados, mas que são incorretamente rejeitados.

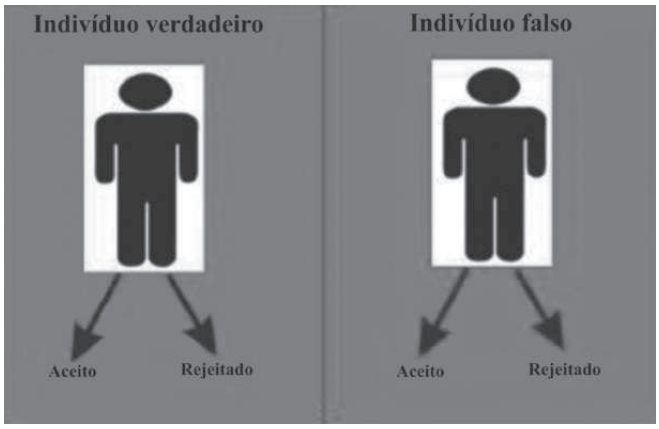

Ilustração 4. Possibilidades na Identificação
Fonte: Biometric Institute Group, 2006

Concordando com o Biometric Institute Group (2006), é possível configurar taxas de falsa aceitação, como também taxas de falsa rejeição para se chegar a um nível de precisão que se considere apropriado a solução biométrica. Porém cada tecnologia, isso inclui *hardware* e *software*, ou seja, se você precisa de uma taxa de falso-positivo de 0,40% e uma taxa de falso-negativo de 8,20%, é preciso achar uma solução que trabalhe com essas taxas. Podendo ser facilmente configurado utilizando-se do padrão mínio chamado *score* visto anteriormente.

TIPOS DE SISTEMAS BIOMÉTRICOS

Segundo Vigliazzi (2006), atualmente existem vários tipos de sistemas biométricos e a cada dia que passa por causa do avanço da tecnologia novos tipos são criados e vão tornando-se presentes no dia-a-dia dos indivíduos ao redor do mundo.

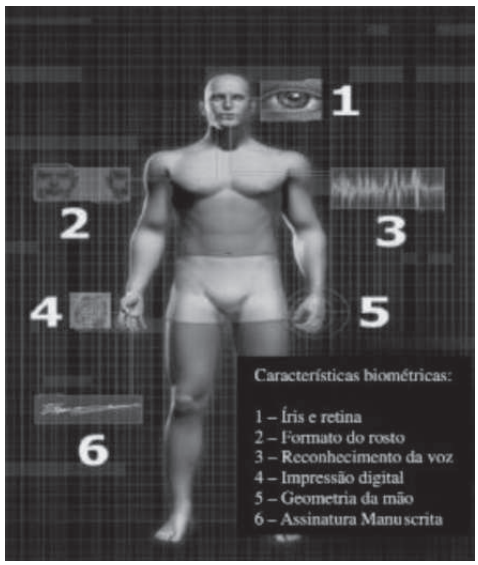

Figura 3. Características biométricas
Fonte - REVISTA GALILEU. (2004).

Dentre os sistemas mais conhecidos estão: Impressão digital, Reconhecimento Facial, Identificação da Retina, Identificação da Íris, Reconhecimento da Voz, Geometria da Mão, Veias da Palma da Mão e Reconhecimento da Assinatura. A Ilustração 5 demostra a porcentagem de utilização das tecnologias biométricas em 2006. Porém com o avanço da tecnologia, novas tecnologias biométricas estão surgindo: Odor, Arquitetura da orelha, Comparação de DNA, Ondas cerebrais, Brilho da Pela, Caminhada, Padrão Vascular, Dinâmica da Digitação, Matriz da Unha e muitos outros que estão por vir.

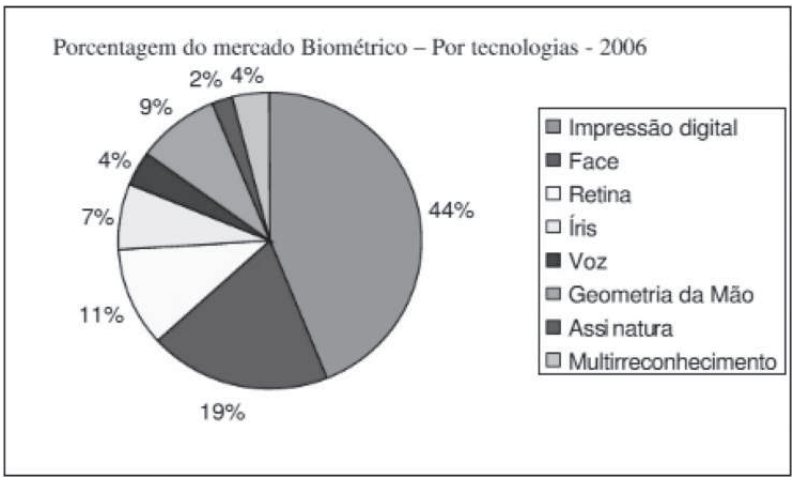

Ilustração 5. Tecnologias Utilizadas no Mercado
Fonte: Institute Biometric Group, 2006

CONCLUSÃO

Atualmente, vivendo na sociedade da segurança da informação, a biometria traz a possibilidade de identificar as pessoas e, com isso, permitir acesso a informações e locais específicos.

As formas tradicionais de identificação são as senhas, cartões magnéticos ou documentação, porém o ser humano possui características corporais únicas, perfeitas para sua identificação. A biometria está crescendo e ganhando mercado a cada dia, num mundo de informações digitais onde todos estão conectados na rede, trazendo muitas vantagens diante da forma tradicional, não mais sendo necessário ter que recordar senhas ou transportar chaves e crachás, permitindo assim um extraordinário controle e confiança nas informações.

REFERÊNCIAS

Alecrim, E. InfoWester - Introdução à Biometria. Dez. 2005. Disponível em: <www.infowester.com/biometria.php>. Acesso feito em: 11 Dez. 2011.
Biometric Institute Limited. Disponível em: <www.biometricsinstitute.org>. Acesso feito em: 5 Jan.

2012.
CBA - Consultores Biométricos Associados Ltda., Uma introdução à biometria e sua história geral. Disponível em: <www.consultoresbiometricos.com.br/05_Bintroducao_definicao.php>. Acesso feito em: 5 Jan. 2013.
Ciência Hoje, Autenticação das Veias da Palma da Mão vence prémio de The Wall Street Journal. Nov. 2005. Disponível em <www.cienciahoje.pt/1589>. Acesso feito em: 15 Jan. 2012.
COSTA, S. M. F. Classificação e verificação das impressões digitais. 2001. 123 f.Dissertação (Mestrado em Engenharia Elétrica). Escola Politécnica da Universidade de SãoPaulo, São Paulo, 2001.
G1 – Tecnologia, Japoneses lançam celular que faz tradução para o inglês. Nov. 2007. Disponível em: <www.g1.globo.com/Noticias/Tecnologia/0,,MUL198919-6174,00.html>. Acesso feito em: 21 Jan. 2013.
IDGNOW!, Biometria. Disponível em: <www.idgnow.uol.com.br/especiais/biometria>. Acesso feito em 21 Jan. 2013.
Malima/Artigos, Biometria: Problemas e Respostas. Abr. 2005. Disponível em: <www.malima.com.br/article_read.asp?id=162>. Acesso feito em: 21 Jan. 2012.
MOUNINA, G. Bocoum. **Acceptance Threshold's Adaptability in Fingerprint-Based Authentication Methods.** 1999. Dissertação (Mestrado em Ciências da Computação). Universidade McGill, Montreal, 1999.
VIGLIAZZI, D. **Biometria Medidas de segurança.** Florianópolis: Visual Books, 2006.