O USO DA BIOMETRIA EM SISTEMAS DE SEGURANÇA

Theylor Moreira Barbosa[1]
theylor-86@bol.com.br

João Paulo G. de Souza[2]
joaopaulogsouza@gmail.com

Marcos Aurélio Carvalho[3]
marcos_carvalho.car@hotmail.com

Leonardo de Carvalho Vidal[4]
leonardo.carvalho.vidal@hotmail.com

Associação Educacional Dom Bosco (AEDB), Faculdade de Engenharia de Resende - Resende, RJ, Brasil.

RESUMO

O conceito de biometria está cada vez mais sendo implantado, quando se trata de segurança. Afinal de contas, fica muito mais seguro e cômodo ao usuário ter acesso a certos tipos de serviço que necessitam sigilo de informações, utilizando apenas alguma característica do individuo e sem se preocupar com o acesso não autorizado. A Biometria é a medida de características físicas ou comportamentais como formas de identificá-las unicamente. As formas mais conhecidas de identificação por um sistema biométrico são pelo reconhecimento de impressão digital, geometria de mãos, íris, retina, voz, face e assinatura. A biometria vem crescendo e ganhando mercado mediante as inseguranças que a vida moderna demonstra, havendo a necessidade de manter sigilo em certas informações de modo profissional e eficaz.
Palavras-chave: Biometria, Sistema biométrico, Impressão digital, Identificação.

ABSTRACT

The concept of biometrics is increasingly being deployed, when it comes to security. After all, it is much safer and comfortable to the user to access certain services that require confidentiality of information, using only some characteristic of the individual and no worrying about unauthorized access. Biometrics is the measurement of physical or behavioral characteristics as ways to identify them uniquely. The best known forms of identification for a biometric system is the fingerprint recognition, hand geometry, iris, retina, voice, face and signature. Biometrics is growing and gaining market by the insecurities of modern life shows, there is a need to keep certain information confidential in a professional and effective manner.
Key words: Biometrics, Biometric System, Digital Printing identification.

---

[1] Theylor Moreira Barbosa – Aluno da Faculdade de Engenharia de Resende – AEDB
[2] João Paulo G. de Souza - Aluno da Faculdade de Engenharia de Resende – AEDB
[3] Marcos Aurélio Carvalho - Aluno da Faculdade de Engenharia de Resende – AEDB
[4] Leonardo de Carvalho Vidal (Professor da Faculdade de Engenharia de Resende – AEDB)

1 INTRODUÇÃO

O termo biometria está cada dia mais próximo do cotidiano. Só resta agora saber como implementar ou utilizar sistemas de identificação com a tecnologia. Vale lembrar que toda a idéia da biometria é conhecida pelo homem desde os primórdios. Afinal de contas, distinguir um indivíduo do outro através das suas características físicas é um conceito que existe há muito tempo. A única diferença é que a interação agora se dá com o computador e não com outro ser humano. Pois bem, a biometria vem justamente a aproveitar essas características únicas das pessoas.

2 CONCEITO DE BIOMETRIA

A Biometria (do grego bios=vida e metron=medida) é o uso de características biológicas em mecanismos de identificação. Entre essas características tem-se a íris (parte colorida do olho), a retina (membrana interna do globo ocular), a impressão digital, a voz, o formato do rosto e a geometria da mão. Há ainda algumas características físicas que poderão ser usadas no futuro, como DNA e odores do corpo.

O uso de características biológicas para identificação se torna bastante viável, pois cada indivíduo possui características exclusivas. Por exemplo, não há ninguém com voz igual, mesma impressão digital, olhos exatamente idênticos. Até mesmo irmãos gêmeos idênticos possuem algumas características diferentes.

2.1 BIOMETRIA X SENHA

O acesso por biometria não é tão diferente do tradicional acesso via senhas. A biometria somente possui uma cadeia de caracteres mais longa que a senha, sendo que as principais vantagens sobre o sistema de senhas são a exatidão em relação a comparação algorítmica, não há necessidade de ser lembrada, portabilidade sem dificuldades, difícil de compartilhar e roubar e irreversibilidade.

2.2 COMO FUNCIONA A BIOMETRIA

O método de identificação de um sistema biométrico usam as seguintes etapas:

- *Registro*: Na primeira vez que se usa um sistema biométrico, ele insere informações básicas como nome ou um número de identificação. Em seguida, captura uma imagem ou registro de uma característica específica do indivíduo;
- *Armazenamento*: Analisa a imagem obtida e traduzem num tipo de código ou gráfico;
- *Comparação*: Compara a imagem capturada com a imagem do registro. Se for igual, ele aceita a identificação do indivíduo, caso contrário, é rejeitado.

2.3 CARACTERÍSTICAS NECESSÁRIAS DE BIOMETRIA

- Universalidade: Todos tem a biometria
- Exclusividade: A biometria é exclusiva o suficiente
- Permanência: A biometria é invariante
- Coletabilidade: A biometria pode ser medida
- Circunvênção: A biometria é difícil de ser falsificada
- Aceitabilidade: Estigma social / Privacidade

OBS: Nenhuma biometria realmente oferece todas estas características

2.4 POR QUE BIOMETRIA?

Nos tempos atuais em alguns tipos de aplicações necessitamos de uma identificação rápida, positiva e confiável , que não possa ser transferida, esquecida ou perdida, com alto grau de dificuldade em copiar e adulterar e que seja possível ser utilizado com ou sem o conhecimento da pessoa analisada.

Muitas industrias, setores médicos, financeiros, comércio, viagens e repartições do governo se mostram interessados nesta tecnologia pela necessidade atual de identificação automatizada.

2.5 TIPOS DE IDENTIFICAÇÃO BIOMÉTRICA

Existem várias formas de realizar a identificação pela biometria que são classificadas em duas classes principais.

- *Fisiológicas*: são relacionadas a forma do corpo. Onde temos como exemplo a impressão digital, reconhecimento facial, geometria da mão e palma e de reconhecimento da íris.
- *Comportamentais:* são relacionadas ao comportamental de uma pessoa. Onde temos como exemplo a verificação de assinatura, dinâmica de digitação e voz.

Seguem-se, assim, os principais exemplos (WILSON, 2010), seja das classificações fisiológicas ou comportamentais, no entanto, aplicados atualmente:

Impressão digital: o uso de impressão digital é uma das formas de identificação mais usadas. Consiste na captura da formação de sulcos na pele dos dedos e das palmas das mãos de uma pessoa.

Esses sulcos possuem determinadas terminações e divisões que diferem de pessoa para pessoa. Para esse tipo de identificação existem, basicamente, três tipos de tecnologia: óptica, que faz uso de um feixe de luz para ler a impressão digital; capacitiva, que mede a temperatura que sai da impressão; e ultrassônica, que mapeia a impressão digital através de sinais sonoros.

Um exemplo de aplicação de identificação por impressão digital é seu uso em catracas, onde o usuário deve colocar seu dedo em um leitor que, ao confirmar a identificação, liberará seu acesso. Como exemplo de scanner utilizado para identificação de impressões digitais (Figura 1).

Figura 1: Scanner usado para identificação de impressão digital

Retina: a identificação por retina é um dos métodos mais seguros, pois analisa a formação de vasos sanguíneos no fundo do olho. Para isso, o indivíduo deve olhar para um dispositivo que, através de um feixe de luz de baixa intensidade, é capaz de "escanear" sua retina. A confiabilidade desse método se deve ao fato da estrutura dos vasos sanguíneos estarem relacionadas com os sinais vitais da pessoa. Sendo mais direto, o dispositivo leitor não conseguirá definir o padrão da retina de uma pessoa se esta estiver sem vida.

Íris: a identificação por meio da íris é uma forma menos incômoda, pois se baseia na leitura dos anéis coloridos existentes em torno da pupila (o orifício preto do olho). Por essa combinação formar uma "imagem" muito complexa, a leitura da íris é um formato equivalente ou mais preciso que a impressão digital. Por nem sempre necessitar da checagem do fundo do olho, é um método mais rápido de identificação. A preferência por identificação da íris também se baseia no fato desta praticamente não mudar durante a vida da pessoa. Apresenta-se o exemplo de equipamento utilizado para identificação de íris (Figura 2).

Figura 2: Scanner usado para identificação de Íris

Geometria de Mãos: este também é um método bastante usado. Consiste na medição do formato da mão do indivíduo. Para utilizá-lo, a pessoa deve posicionar sua mão no dispositivo leitor sempre da mesma maneira, do contrário às informações de medidas poderão ter diferenças. Por esse motivo, os dispositivos leitores contêm pinos que indicam onde cada dedo deve ficar posicionado. Esse é um dos métodos mais antigos que existe, porém não é tão preciso. Em contrapartida, é um dos meios de identificação mais rápidos, motivo pelo qual sua utilização é comum em lugares com muita movimentação, como universidades, por exemplo. Apresenta-se (Figura 3) um exemplo de equipamento utilizado para identificação de geometria das mãos.

Figura 3: Mecanismo de identificação por geometria de mãos

Face: neste método a definição dos traços do rosto de uma pessoa é usada como identificação. É um processo que se assemelha em parte com a leitura de geometria das mãos, mas considera o formato do nariz, do queixo, das orelhas, etc.

Voz: a identificação por voz funciona através da dicção de uma frase que atua como senha. O usuário deverá informar a um reconhecedor a tal frase sempre que for necessária sua identificação. O entrave dessa tecnologia é que ela deve ser usada em ambientes sem ruídos, pois estes podem influenciar no processo. Além disso, se o indivíduo estiver rouco ou gripado sua voz sairá diferente e poderá atrapalhar sua validação. Por esta razão, a identificação por voz ainda é pouco aplicada.

Assinatura: esse tipo de identificação consiste na comparação da assinatura com uma versão gravada em um banco de dados. Além disso, é feita a verificação da velocidade da escrita, a força aplicada, entre outros fatores. É um dos mecanismos mais usados em instituições financeiras, embora não se trate completamente de um método biométrico. É importante frisar que todos esses métodos possuem alguns entraves que os fazem necessitar

de aperfeiçoamento ou, dependendo do caso, da aplicação de outra solução. Por exemplo, na identificação por retina, a pessoa que estiver usando óculos deve retirá-lo; na identificação por face, um ferimento ou um inchaço no rosto pode prejudicar o processo; na identificação da geometria da mão, um anel também pode trazer problemas; na identificação por voz, ruídos externos, rouquidão ou até mesmo uma imitação da voz de um indivíduo pode pôr em dúvida o procedimento; na comparação de assinaturas, o estado emocional da pessoa pode atrapalhar e há ainda o fato da escrita mudar com o passar do tempo. Encontra-se, também, o sistema de identificação por assinatura (Figura 4).

Figura 4: Sistema biométrico para identificação por assinatura

Arcada Dentária: Tal procedimento vem se tornando cada vez mais comum na odontologia, tanto para reconhecimento, verificar procedimentos odontológicos e para intervenções intercorrentes. Este tipo é um dos mais confiáveis atualmente devido a multiplicidade de combinações específicas de cada indivíduo em sua arcada dentária. A verificação pode ser feita através da quantidade de dentes, posicionamento, formato, quantidade de restaurações, faces restauradas envolvidas, dimensões e perdas ósseas.

Figura 5: Geometria das veias

Como a mais recente das tecnologias biométricas encontra-se a Geometria das veias (Figura 5) com maior grau de segurança e reconhecimento sendo praticamente imutável.

2.6 URNAS BIOMÉTRICAS

A maior evolução tecnológica nas urnas eletrônica até este momento é representada pela biometria. (ALECRIN, 2005). Este avanço tecnológico tem como principal objetivo aumentar o nível de segurança das eleições, cruzando os dados biométricos cadastrados, fazendo com que os eleitores fantasmas sejam identificados.(Figura 6)

Figura 6: Kitbio completo com laptop, sensor de digitais, mini-estúdio fotográfico e caixa de transporte

O cadastramento dos dados biométricos são realizados por computadores especiais que são chamados de Kitbio. Cada computados deste custa em média R$ 13.500,00. E ainda é necessário adaptar leitores de impressão digital. Além destes equipamentos é preciso de um sistema de conferência on-line das impressões digitais dos eleitores cadastrados, que evita a duplicidade dos eleitores.

As urnas biométricas foram testadas pela primeira vez nas eleições municipais de 2008. E este novo sistema foi testado somente em algumas cidades como São João Batista (Santa Catarina), Fátima do Sul (Mato Grosso do Sul) e Colorado D ´Oeste (Rondônia). Foram implementas cerca de 100 urnas naquela época. Como a aquisição dos equipamentos são elevadas, este novo sistema esta sendo implementado de forma gradativa (BRUNAZO FILHO, 2009)

Toda essa tecnologia que foi criada recentemente é considerada a mais segura no momento de se autenticar a identificação dos eleitores, mas todos nós sabemos que nenhum sistema é imune a falhas.

3 CONSIDERAÇÕES FINAIS

Em outras palavras podemos dizer que a Biometria pode ser pensada como uma chave bem segura, mas uma chave que não pode ser entregue a outra pessoa, uma ciência de identificação baseada na medição precisa de traços biológicos. A tecnologia biométrica serve como uma barreira ou uma porta de entrada, entre dados das organizações e o acesso não autorizado. Hoje em dia, há vários aparelhos biométricos sendo utilizados por empresas para o conhecimento de características humanas. Estas tecnologias permitem um extraordinário controle sobre as transações e confiança nas informações. Apesar de a tecnologia biométrica poder ser utilizada para uma infinidade de aplicações relacionadas com a identificação, que proporciona uma segurança de dados e proteção de privacidade.

A Biometria está crescendo e ganhando mercado a cada dia com o crescimento das inseguranças, principalmente quando você se pergunta “Quão importante é a proteção das minhas informações?”, deste modo passa-se a pensar de modo amador e começa-se a pensar de maneira profissional e eficaz.

REFERÊNCIAS

BRUNAZO FILHO, Amilcar. **Urnas eletrônicas com biometria:** fraudes e garantias. (Disponível em: <http://www.brunazo.eng.br/voto-e/textos/urnas-b1.htm> Acesso em: 13/05/2014)

ALECRIN, Emerson. **Introdução à biometria.** 2005 (Disponível em: <http://www.infowester.com/biometria.php> Acesso em: 14/05/2014)

WILSON, Tracy. **Como funciona a biometria.** 2010 (Disponível em: <http://ciencia.hsw.uol.com.br/bometrica.htm> Acesso em: 14/05/2014)