

# Um Breve Estudo Sobre Biometria

Cassiana da Silva Bonato, Roberto Mendes Finzi Neto

Departamento de Ciência da Computação – Universidade Federal de Goiás (UFG) –  
Campus Catalão

Avenida Dr. Lamartine Pinto de Avelar – 1120 – Setor Universitário –  
CEP: 75704-020– Catalão – GO – Brasil

kassi.ice@gmail.com, robertofinzi@hotmail.com

***Abstract.** This paper discusses the concept of biometrics, besides some biometrics' types used currently, emphasizing the type fingerprint and also the steps for implementation and use this authentication method.*

***Resumo.** Este artigo discute o conceito de biometria, além de alguns tipos de biometria usados atualmente, enfatizando o tipo por impressão digital e também os passos para implementar e utilizar esse método de autenticação.*

## 1. Introdução

Esse artigo apresenta um sucinto estudo sobre biometria, relatando conceitos importantes e tipos de biometria mais utilizados, dando maior ênfase à impressão digital. Outro tópico apresentado são os passos necessários para tal reconhecimento biométrico.

Biometria é a ciência que procura identificar indivíduos baseando-se em características únicas. Essas características podem ser de caráter físico, químico ou comportamental. Seu principal uso é controlar o acesso de pessoas a um determinado local que exige um alto nível de segurança.

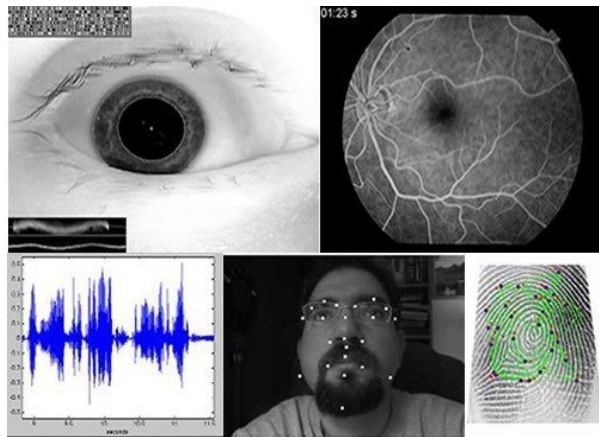
O reconhecimento biométrico é uma alternativa de autenticação que evita perdas de objetos identificadores como cartões ou o esquecimento de senhas, já que a identificação é feita por meio de um atributo do indivíduo, esses atributos são abordados na seção 2 como tipos de biometria, com um aprofundamento na impressão digital. A seção 3 é sobre as etapas para utilização de biometria.

## 2. Tipos de Biometria

Cada atributo que o ser humano possui que é capaz de identificá-lo unicamente gera um tipo biométrico. Alguns destes tipos como o reconhecimento por DNA e facial são apresentados na tabela abaixo, que apresenta suas vantagens, desvantagens, custo e sua conveniência. Após a tabela há exemplos de alguns tipos apresentados na tabela como íris, retina, voz, facial e impressão digital respectivamente na figura 1.

**Tabela 1 - Tipos de Biometria**

<b>Tipos</b>	<b>Vantagens</b>	<b>Desvantagens</b>	<b>Custo</b>	<b>Conveniência</b>
Impressão digital	Simples, barato;	Fácil de ser fraudado;	Baixo;	Boa;
Retina	Precisão;	Caro, difícil de treinar os usuários;	Alto;	Ruim;
Íris	Fácil aquisição, melhor precisão de todos os métodos;	Custo, baixa aceitabilidade;	Médio;	Excelente;
Reconhecimento facial	Similar ao processo humano,	Pode ser difícil de adquirir, baixa precisão;	Baixo a médio;	Excelente;
Reconhecimento por voz	Fácil aquisição;	Fácil de ser fraudado;	Baixo;	Excelente;
DNA	Determinístico e precisão;	Necessita de muito tempo para processar;	Alto;	Ruim;



**Figura 1 - Exemplos de tipos biométricos**

Após observar a tabela, pode-se notar que há questões mais importantes a serem ressaltadas, um exemplo é a precisão. Essa questão se preocupa com autenticação correta, ou seja, é necessário evitar que haja tanto FRR (False Rejection Rate) que é a taxa de rejeição de um usuário verdadeiro quanto FAR (False Acceptance Rate) que é a taxa de aceitação de um usuário não registrado.

### **2.1. Biometria por digitais**

Esse é o tipo biométrico mais utilizado hoje em dia, por ter uma grande aceitação, já que há muito tempo é utilizado no campo forense. Ele consiste em analisar os elementos principais e únicos, conhecidos como minutiae, que podem ser as linhas papilares e suas bifurcações ou mesmo poros no dedo. A figura abaixo mostra alguns desses pontos.



**Figura 2 - Pontos indetificadores das digitais**

Essas características são diferentes até mesmo entre gêmeos idênticos, um ponto vantajoso em relação a outros tipos como o DNA e o reconhecimento facial. Outra vantagem é que esse método já possui uma maturidade, pois existem muitos estudos sobre o assunto. Além disso, é um sistema barato comparado aos outros e simples de ser entendido e aceitado pelos usuários.

Sua principal desvantagem é a maior possibilidade de fraudes, a maioria dos sistemas de reconhecimento por impressão digital não observam se o dedo é um protótipo sintético com as impressões de uma pessoa registrada. As impressões podem ser pegadas de modo fácil em copos por exemplo. Outro problema são cortes no dedo que podem dificultar a autenticação do usuário, escondendo pontos de identificação, podendo gerar uma falsa rejeição.

A biometria por digitais utiliza algoritmos baseados nas características ditas acima como minutiae e poros. Outro tipo de algoritmo apresentado é de correlação que trata as imagens como matrizes e observa o grau de igualdade entre elas. As etapas para a utilização da impressão digital se equiparam aos outros tipos e são apresentadas no próximo tópico.

### **3. As etapas da biometria**

Para implementar qualquer método biométrico, é necessário passar pelas etapas de registro, extração de características e verificação ou identificação do usuário. As subseções a seguir tratam desses assuntos.

#### **3.1. Registro**

O primeiro passo a ser feito é conseguir uma amostra que será utilizada como padrão para a comparação. Essa amostra é chamada de template. O template é obtido através do próprio dispositivo de reconhecimento. A amostra coletada é analisada, com o objetivo de verificar se sua qualidade é aceitável, se for, a amostra é armazenada após um processo de criptografia, para proteger os dados. Caso contrário, é necessário refazer o registro.

#### **3.2. Extração de características**

Existem características que facilitam a comparação entre o template e a imagem coletada pelo dispositivo na hora da autenticação. Assim o template é processado por alguns filtros para separar a imagem importante do plano de fundo e torná-la melhor observável

e armazenável, podendo transformar essa imagem em uma matriz com os dados importantes do template determinados por um algoritmo que faz a extração das características de acordo com o tipo biométrico. A tabela 2 apresenta alguns algoritmos.

**Tabela 2 - Tipos de Algoritmos**

<b>Tipos</b>	<b>Algoritmos</b>
Impressão digital	Baseado em Minutiae, baseado em correlação;
Retina	LCC;
Íris	Daugman, Li Ma, Boles;
Reconhecimento facial	PCA, LDA, ICA, LFA, EBGM;
Reconhecimento por voz	FFT, HMM com Baum-Welch;
DNA	P. Zhang;

### **3.3. Identificação ou verificação do usuário**

Esse é o momento em que o dispositivo coleta uma nova amostra do usuário, extrai suas características e compara com o template. Se as características forem iguais, o usuário é aceito, se não, ele é rejeitado.

Há diferenças entre verificação e identificação, entretanto, a identificação é quando se compara a nova amostra com todos os templates do banco de dados, enquanto na verificação, a comparação é feita apenas com o template do usuário já identificado pelo seu login ou cartão de identificação por exemplo.

## **4. Conclusão**

A autenticação biométrica antigamente era apenas vista como um método que ajudava a identificar criminosos, agora, cada vez mais na segurança de áreas confidenciais e de autenticação de usuário para outros fins. Um exemplo é a urna biométrica que será utilizada em algumas cidades nas eleições brasileiras.

Essas urnas têm um dispositivo para coletar as impressões digitais para identificar o eleitor e diminuir a chance de fraudes. A urna é só um exemplo de como a biometria pode se tornar um dos mais utilizados métodos de segurança no mundo.

## **Referências**

- Boulgouris, N. V., Plataniotis, K. N. e Micheli-Tzanakou, E. (2010), Biometrics: Theory, Methods and Applications, Wiley, IEEE Press, , 1ª edição.
- Gregory, P. e Simon, M. (2008), Biometrics for Dummies, Wiley Publishing, Inc, 1ª edição.
- Jain, A. K., Flynn, P. e Ross A. A. (2008), Handbook of Biometrics, Springer, 1ª edição.
- Tistarelli, M., Bigun, J. e Grosso, E. (2003), Advanced Studies in Biometrics, Springer, 1ª edição.