DOI: http://dx.doi.org/10.29069/forscience.2015v3n2.e108

ÚLTIMOS CINCO ANOS DE PESQUISA EM BIOMETRIA: UM ESTUDO DAS PRINCIPAIS UNIVERSIDADES NO BRASIL

Magda Vieira da Silva Oliveira[1]
Melina Rossi Santos[2]

RESUMO

Para Nakashiro (2011) e Pinheiro (2008), quando o assunto é integridade de documentos e provas digitais, o desafio está em encontrar tecnologias confiáveis para obter evidências de um computador ou estrutura computacional relacionadas a um incidente e também assegurar sua autenticidade e veracidade. A Biometria é uma tecnologia relativamente nova, útil para identificar pessoas, e funciona como se fosse uma senha. A abordagem aqui tratada não deve ser confundida com a biometria estudada nos ramos da Biologia. A biometria é aplicada para distinguir o ser humano por meio das diferenças entre suas características físicas e biológicas. Ao digitar um nome de usuário e uma senha em um sistema, por exemplo, a pessoa está "diferenciando-se" das outras pessoas e usuários. O objetivo é o mesmo, porém essa diferenciação ocorre por meio de características que são únicas para cada indivíduo. Dentre as técnicas de biometria, temos: impressão digital, reconhecimento de face, de voz, de assinaturas, de íris, de retina etc. Com a pretensão de entender e compreender a importância da biometria e também perceber sua utilização no Brasil realizou-se uma análise bibliográfica dos cinco últimos anos nas principais universidades brasileiras. A partir daí, foram obtidas definições mais precisas do que é biometria, como funciona, quais os tipos, onde é utilizada, em geral, e onde é mais aplicada no Brasil. Espera-se que os resultados tragam mais opções para pesquisas na área, pois faltam pesquisas e literaturas a respeito.

Palavras-chave: Biometria. Autenticidade. Veracidade. Segurança. Sistema biométrico.

LAST FIVE YEARS OF RESEARCH IN BIOMETRICS: A STUDY OF THE MAJOR UNIVERSITIES IN BRAZIL

ABSTRACT

To Nakashiro (2011) and Pinheiro (2008), when it comes to integrity of documents and digital evidence, the challenge is to find reliable technologies in order to obtain evidence from a computer or computational structure, related to an incident and also ensure its authenticity and

[1] Doutorado em Educação pela Universidade Estadual de Campinas (UNICAMP), mestrado em Psicologia Escolar pela Pontifícia Universidade Católica de Campinas (PUC-Campinas) e graduação em Ciências Exatas Licenciatura Plena Em Matemática pela PUC-Campinas. Atualmente professora pesquisadora do Centro Universitário Salesiano de São Paulo - Campinas – SP. E-mail: magda.silva@sj.unisal.br.

[2] Graduando em Engenharia Mecânica, Centro Universitário Salesiano de São Paulo – Campinas - SP. Tem experiência na área de Engenharia Mecânica. Sou membro do grupo de pesquisa Tecnologia, Educação e Inovação. E-mail: melrossi88@yahoo.com.br.

veracity. Biometrics is a relatively new technology, useful to identify people and works like a password. The approach discussed here must not be confused as the biometrics studied in biology fields. Biometrics is applied to distinguish the human being through the differences between their physical and biological characteristics. When you enter a username and password on a system, for example, the person is "individualizing" herself/himself from other people and users. The goal is the same, but this differentiation occurs through features which are unique to each individual. Among the biometric techniques we have: fingerprint, face, voice, signature, iris, retina recognition etc. Aiming to understand and comprehend the importance of Biometrics and also to realize its use in Brazil, it has been performed a bibliographical analysis of the last five years, in the major Brazilian universities.Therefore we have obtained more precise definitions of Biometrics, how it works, what its types are, where in general it is used and applied the most in Brazil. It is expected that the results bring us more options for research in the area, on there is a lack of research and literature on this subject.

Keywords: Biometrics. Authenticity. Veracity. Safety. Biometric system.

1 INTRODUÇÃO

Atualmente é muito comum presenciar a biometria em nosso dia a dia. Ao assistir um filme ou seriado, especialmente quando o tema é policial e investigativo. Muitas vezes, em uma cena, abre-se uma porta ou um cofre onde o personagem precisa colocar a mão ou os olhos em um scanner biométrico.

Praticamente todo mundo já ouviu o termo biometria, mas será que sabem o que é exatamente? Qual a sua real utilidade?

Atualmente, a biometria é considerada um dos métodos mais seguros de identificação e está cada vez mais presente na vida das pessoas, nos aeroportos, agências bancárias, urnas eletrônicas e até mesmo em parques temáticos que utilizam esta técnica de reconhecimento das características únicas de cada pessoa.

Segundo Nakashiro (2011), o termo biometria significa medição biológica, ou seja, é o estudo das características físicas e comportamentais de cada pessoa. O princípio básico desta técnica para identificação é o seu corpo, sua senha.

Conforme Pinheiro (2008), a biometria é a ciência que analisa e compara dados biológicos do corpo humano, podendo ser: impressões digitais, características da voz, características da retina, entre outros. Seu objetivo principal é a identificação de pessoas que foram cadastradas no sistema para serem autorizadas a realizar algum tipo de atividade.

A biometria utiliza características humanas para confirmar a identidade de uma pessoa, tendo como objetivos melhorar a segurança, controlar acessos indevidos, prevenir fraudes, dentre outros.

A maior limitação para o avanço na área se deve aos aparelhos utilizados, afinal não é assim tão simples criar um scanner de retina ou palmar que extraia apenas as informações necessárias.

Considerado um dos métodos mais seguros de identificação, a biometria está cada vez mais presente na vida das pessoas. Aeroportos, agências bancárias, urnas eletrônicas e até parques temáticos fazem uso desta técnica de reconhecimento das características únicas de cada pessoa.

De forma sucinta, a biometria vem do grego *Bios* (vida) e *metron (* medida). Dentre as características biológicas em mecanismos de identificação, destacam-se a íris, a retina, 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 *Deoxyribonucleic Acid* (DNA) e odores do corpo. O uso de características biológicas para identificação apresenta-se como uma ideia viável porque as pessoas possuem características diferentes umas das outras. Por exemplo, não há ninguém com a voz igual, com a mesma impressão digital ou com olhos exatamente idênticos. Até mesmo entre irmãos gêmeos muito parecidos há diferenças. O sistema biométrico busca identificar um indivíduo por meio de suas características físicas (dedo, olho, mão etc.) ou comportamentais, isto é, o modo de assinar uma documentação, entre outros (PINHEIRO, 2008; PINOCHET, 2014; CAIÇARA JUNIOR; PARIS, 2007).

O processo básico do sistema biométrico consiste na aquisição (registro do usuário), exemplar (perfil biométrico armazenado), extração (características biométricas), perfil (modelo biométrico extraído), ccomparação (verifica se os dados apresentados são similares ou não) e limiar (verifica similaridade).

Para o desenvolvimento deste trabalho, primeiramente foram feitos o levantamento e a análise bibliográfica dos últimos cinco anos da Universidade Estadual de Campinas, Universidade de São Paulo, Universidade Estadual de São Paulo e Universidade Federal de São Carlos. Na análise bibliográfica, definiu-se mais a fundo o que é biometria. Além disso, verificou-se como funciona, quais os tipos de biometria, onde é utilizada, em geral, e onde é mais utilizada no Brasil. Com base nos resultados deste estudo e na análise desses levantamentos, obtiveram-se subsídios para pesquisas futuras.

1.1 Breve histórico

A biometria já era conhecida e utilizada há anos atrás, mas sem nenhum auxílio de tecnologia, por meio das características físicas das pessoas (altura, peso, cor dos cabelos, cor

dos olhos, entre outras).

Segundo Pinheiro (2008), os governantes chineses foram os primeiros a usar as impressões digitais grafadas em placas de barro para lacrar documentos e confirmar a identidade da pessoa. Além disso, também carimbavam as mãos e os dedos das crianças em papel, para sua identificação. Um dos primeiros métodos de identificação foi desenvolvido pelo francês Alphonse Bertillon - o método de Bertillon - que era dividido em três partes:

- Medida das partes do corpo: altura, comprimento da cabeça, pé esquerdo, envergadura, largura da cabeça, dedo médio esquerdo, tronco, ouvido direito e antebraço esquerdo;
- Descrição morfológica da aparência e do formato do corpo, por meio de medidas relacionadas ao movimento;
- Descrição de marcas peculiares no corpo, resultantes de deformidades causadas por doenças, acidentes, ou mesmo de nascença, como cicatrizes, tatuagens, deficiências, pintas etc.

Segundo Pinheiro (2008) e Moraes (2006), esse método foi inicialmente utilizado pela polícia de Paris, França, Europa e, posteriormente, Estados Unidos. Devido à dificuldade de armazenamento e visualização das informações coletadas, esse método foi substituído pelo sistema de impressões digitais criado por William James Hersche. Em 1981, Juan Vucetich iniciou o primeiro sistema de arquivamento das impressões digitais, onde a impressão digital marcada pelo sangue da vítima foi utilizada para identificar o criminoso.

Durante anos, o armazenamento dos dados das impressões digitais era em papéis, e, atualmente, esse armazenamento e coleta das informações são digitais.

1.2 Objetivo da pesquisa

Este estudo faz o resgate das pesquisas sobre biometria desenvolvidas nos últimos cinco anos nas principais universidades brasileiras, analisando a tendência dos tipos de biometria, como cada autor define e suas aplicações.

1.3 Métodos e materiais

O material de análise e de referência principal para o estudo está sendo constituído por

dissertações e teses relativas à biometria produzidas nos últimos cinco anos. Metodologicamente, o estudo caracteriza-se como exploratório e bibliográfico. Foram utilizados acervos virtuais de dissertações e teses de algumas universidades, como: UNICAMP, USP (São Paulo e São Carlos), UNESP (Rio Claro), UFSCAR, Universidade de Santa Catarina e Universidade Federal de Minas Gerais (UFMG).

2 TIPOS DE BIOMETRIA CONFORME ALGUNS PESQUISADORES BRASILEIROS

2.1 Biometria como identidade e identificação

Segundo Costa (2001), a biometria pode ser expressa de duas formas:

- **Identificadores fisiológicos:** incluem impressões digitais, geometria de mão, retina, características faciais, formato da unha.
- **Identificadores de procedimento:** destacam-se a voz e a assinatura. Análise do reconhecimento de voz e assinatura geralmente é considerada menos conclusiva porque está sujeita a limitações devido a enfermidades ou imitações (Figura 1).

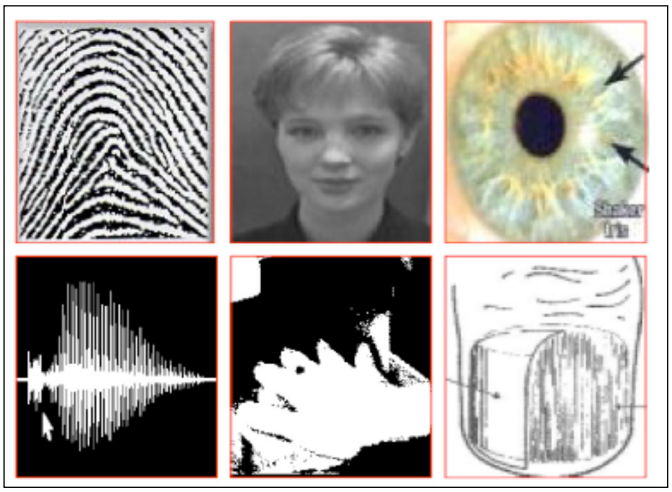

Figura 1 - Tecnologias biométricas - impressão digital, face, íris, voz, geometria da mão, formato da unha
Fonte: Costa (2001).

Segundo Nakashiro (2011), um dos primeiros casos de utilização da biometria no Brasil foi a proposição da criação de uma lei, em 2002, para aumentar a segurança nos presídios por meio de câmeras digitais para a captação de imagens e sistemas de reconhecimento biométricos. Mesmo não tendo sido transformado em lei, esse sistema começou a ser utilizado.

Em 2004, o Ministério da Educação (MEC) iniciou um controle biométrico de alunos de escola pública por meio de suas impressões digitais, visando a uma identidade cidadã e ao melhor planejamento das políticas educacionais. Sendo assim, a frequência escolar de cada aluno era monitorada, auxiliando no controle de alguns tipos de benefícios sociais, como foi o caso do "Bolsa Família" (NAKASHIRO, 2011).

Atualmente, no Brasil, a identificação por meio de impressões digitais está presente na emissão da grande maioria dos documentos de identificação, como, por exemplo, Carteira Nacional de Habilitação (CNH), Registro Geral (RG), Título Eleitoral, Passaporte, dentre outros. Para a CNH, a biometria é utilizada para gerenciar, controlar e fiscalizar todo o processo de habilitação, formação e reciclagem de condutores, mudanças de categorias e de renovação ou expedição da Carteira Nacional de Habilitação.

Nakashiro (2011) comenta que, no caso do Título de Eleitor, está sendo realizado um recadastramento de cada cidadão, através da Justiça Eleitoral, utilizando a biometria por meio de dados coletados, fotografias, assinaturas e impressões digitais. O objetivo é agilizar o processo eleitoral e evitar fraudes e enganos, além de impedir que uma pessoa possa votar no lugar da outra, aumentando a segurança dos votos. **O que hoje já é uma realidade em algumas cidades brasileiras.** (Grifo nosso)

A biometria, na forma de impressão digital, também está sendo adotada em vários segmentos industriais e de serviços, como, por exemplo, no processo de controle de ponto, entrada e saída de funcionários.

2.1.1 Impressões digitais

Existem dois métodos para extração de informações de assinaturas digitais: o coletado via tinta e inserido no papel e aquele realizado por leitores biométricos. O primeiro método quase não é utilizado, devido à falta de clareza, pois apresenta-se como borrões; o segundo é o mais adequado, já que utiliza leitores biométricos, conforme Figura 2 abaixo (COSTA, 2001).

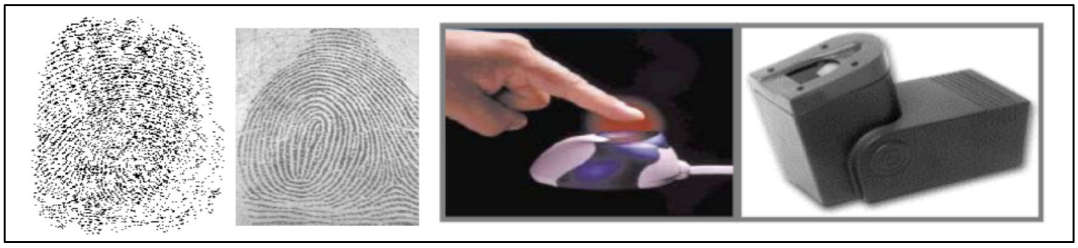

Figura 2 - Impressão tintada em papel e impressão adquirida em um leitor *TouchSafeII* da Identix e exemplos de leitores biométricos
Fonte: Costa (2001).

Segundo Costa (2001), os primeiros leitores biométricos constituíam-se em placas e prismas de vidro, alimentando câmeras ópticas com saída de vídeo analógica. Atualmente existem outros leitores desenvolvidos por meio do uso de câmeras *Charged Coupled Device* (CCD) (Dispositivo de Acoplamento de Carga) e microprismas, leitores capacitivos e outras tecnologias que apresentam características comuns, como, por exemplo, alta resolução.

Na Figura 3 a seguir, são apresentadas as diferenças de tamanho e resolução de amostras DB1, DB2 e DB3.

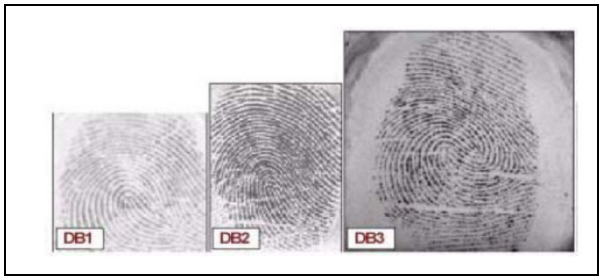

Figura 3 - Amostras DB1, DB2, DB3 - diferenças de tamanho e resolução
Fonte: Costa (2001).

Conforme Costa (2001), os sistemas automáticos ou semiautomáticos biométricos, em sua maioria, são baseados em comparações de minúcias, como mostrado na Figura 4.

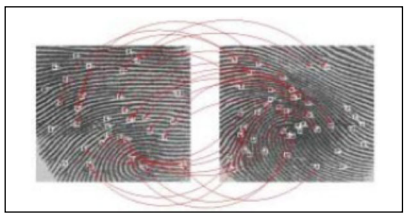

Figura 4 - Comparação de minúcias (cristas finais e cristas bifurcadas)
Fonte: Costa (2001).

As aplicações das impressões digitais destinam-se ao aumento de segurança e agilidade em operações empresariais, governamentais ou institucionais, tais como: Forças Armadas, governo, repartições públicas, transações eletrônicas, controle de ponto, controle de acesso e presença (COSTA, 2001). Na Figura 5, outras aplicações:

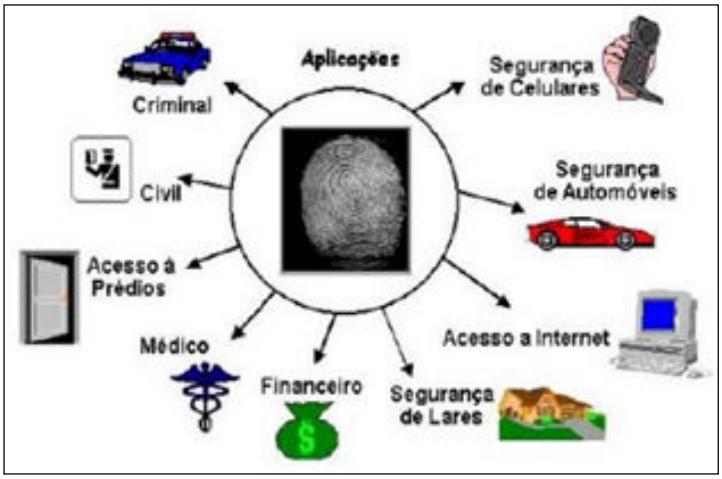

Figura 5 - Aplicação biométrica em diversos segmentos de mercado
Fonte: Costa (2001).

Conforme o mesmo autor, alguns termos técnicos utilizados para o reconhecimento das impressões digitais são de área padrão, que é a parte principal da impressão do dedo e consiste das cristas e todos os seus aspectos, além dos tipos de linhas que são definidos como duas cristas que iniciam paralelamente e divergem sobre toda a área padrão. Estas cristas podem ser contínuas ou não, caso ocorra alguma quebra.

Os pontos singulares, em impressões digitais, são conhecidos como núcleos e deltas (Figura 6), que são usados para classificar os padrões de impressões digitais (COSTA, 2001).

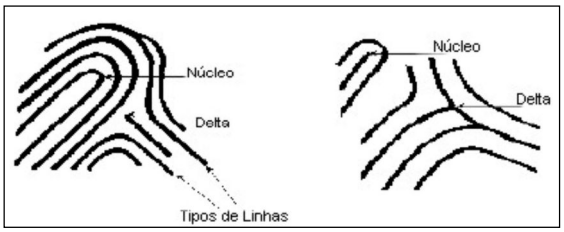

Figura 6 - Ponto delta e ponto núcleo de uma impressão digital
Fonte: Costa (2001).

Para Costa (2001), as técnicas de otimização da imagem podem ser agrupadas dentro de duas principais categorias: melhoria pelo processamento pontual ou pelo processamento de área.

A classificação e verificação (comparação) são duas funções primárias requeridas em um processamento para reconhecimento de impressões digitais. A classificação é feita com base em macroaspectos ou características das cristas. Dessa forma, as impressões digitais são agrupadas de acordo com sua configuração geométrica. A meta da classificação é assegurar que uma dada impressão digital pertença a uma classe específica, de acordo com suas propriedades

geométricas. A classificação pode ser feita em dois níveis: bruto e refinado (COSTA, 2001).

Segundo Casado (2008), os métodos clássicos de extração de minúcias consistem, basicamente, na binarização da imagem, isto é, consistem em converter a imagem para preto e branco, conforme a Figura 7 a seguir.

Figura 7 - Imagem de um fragmento de impressão digital (esquerda) e o resultado obtido após o processo de binarização (direita)
Fonte: Costa (2001).

O processo de afinamento, conforme Gonzalez e Woods (2000), garante que as linhas possuam exatamente um pixel de largura, o que torna a busca pelas terminações e bifurcações relativamente simples, bastando varrer a imagem.

Apesar de simples, a abordagem clássica possui algumas desvantagens: todo processo de binarização provoca perda de informação; se a qualidade da imagem for ruim, a binarização criará muitas minúcias espúrias (falsas minúcias), ou seja, o processo é muito dependente da qualidade da imagem e, por isso, requer um bom pré-processamento.

No trabalho de Sengottuvelan e Wahi (2007, a*pud* CASADO, 2008) é apresentado um método bastante conhecido de extração de minúcias para detecção de fraudes por meio da comparação de impressões digitais de pessoas vivas e até mesmo depois de virem a óbito.

Conforme Casado (2008), a extração de minúcias de imagens de impressão digital é a etapa que antecede a autenticação ou identificação de um indivíduo. O algoritmo desenvolvido é constituído conforme a Figura 8 a seguir:

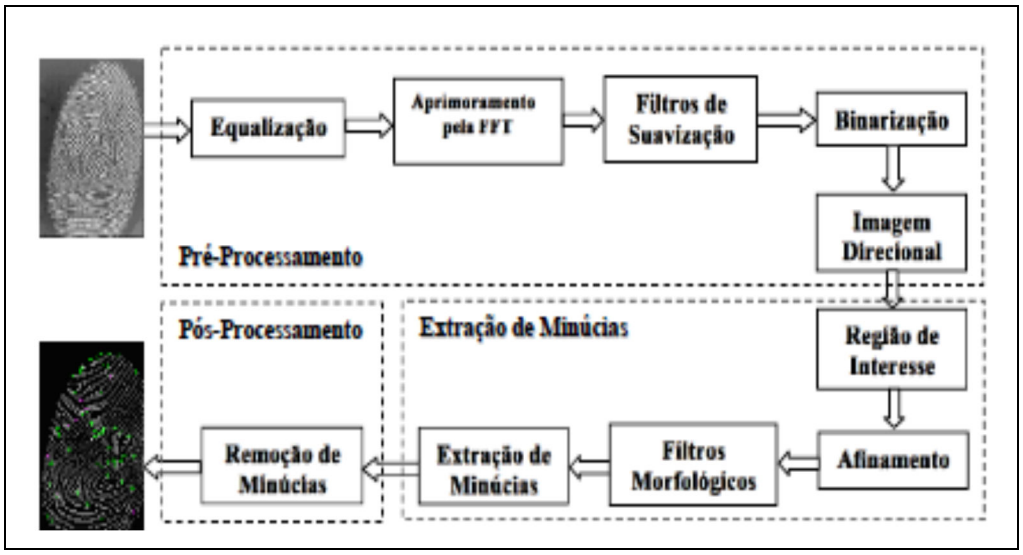

Figura 8 - Módulos do algoritmo de extração de minúcias
Fonte: Casado (2008).

As técnicas utilizadas são o espalhamento de contraste e pontos característicos ou minúcias.

Conforme os estudos de Costa (2001), os aspectos compostos são construídos a partir dos aspectos básicos, que são cristas finais (*ridge ending*) e cristas bifurcadas (*bifurcation*). Para a verificação de impressões digitais, é necessário que haja a coincidência de doze pontos característicos, no mínimo, e que não exista nenhuma discordância entre eles, ou seja, devem ser idênticos e ter a mesma localização. Na maioria dos países, estes critérios são requeridos legalmente para identificação em um caso criminal, sendo que um leitor de impressão digital típico pode registrar mais de 20 pontos característicos (minúcias).

2.2 Reconhecimento da íris

A íris é um órgão interno, que faz parte do globo ocular, protegido pela córnea do olho. É colorida e sua função é controlar os níveis de luz, assim como faz o diafragma de uma câmera fotográfica. A pupila é a abertura para a entrada de luz, que é controlada pela íris, e possui características próprias de cada pessoa (CANUTO, 2010).

2.2.1 Biometria da íris

A biometria da íris sempre está associada à alta segurança, sendo biometricamente muito atrativa, e apresenta os melhores FRR e FAR. A aceitação é baixa, devido principalmente ao

fato de que é invasiva. Provoca certo desconforto de uso, por causa do medo de possíveis danos ao olho. A Figura 9 mostra a pontuação para a biometria da íris (CANUTO, 2010).

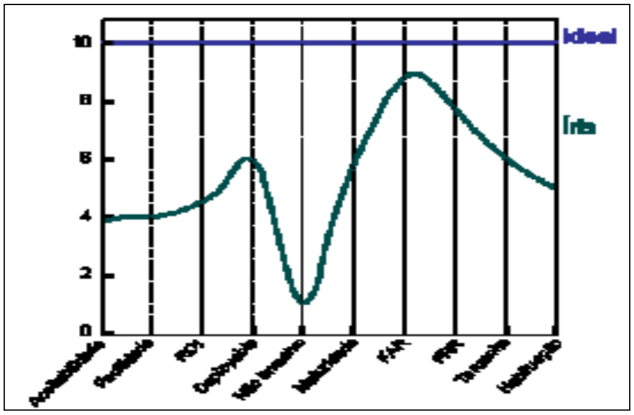

Figura 9 - Pontuação para a biometria da íris
Fonte: Canuto (2010).

Segundo Canuto (2010), os algoritmos básicos de reconhecimento de íris variam de acordo com a classificação dada por diferentes autores na literatura, conforme a Figura 10.

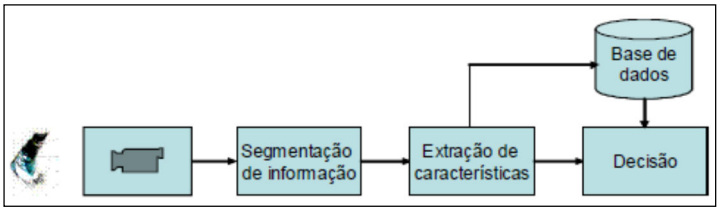

Figura 10 - Descrição de um típico sistema de reconhecimento de íris
Fonte: Chavez (2007).

John Daugman foi pioneiro nessa área, tendo desenvolvido os algoritmos matemáticos que permitiram codificar digitalmente a imagem da íris capturada a partir de um vídeo. Associou-se, então, à empresa *IriScan, Inc*., que se tornou a principal empresa no mundo a oferecer esse tipo de serviço. O método proposto por Daugman pode ser dividido em quatro procedimentos, ou seja, realizar a captura com dispositivos comerciais da empresa *IrisScan*, a localização, a normalização, a extração de características e o casamento (CANUTO, 2010).

Chavez (2007) considera que duas representações correspondem a uma mesma íris ou a íris distinta quando é feita com base num limiar determinado empiricamente. O autor sugere ainda um refinamento que leva em conta as áreas afetadas por oclusão, que consiste em substituir a outra métrica.

O método de Boles representa a estrutura da íris por meio de uma transformada *wavelet*

(Daubechies) diádica contínua, conforme os seguintes passos: localização da íris, normalização da imagem, representação da íris e reconhecimento. Aplica-se, a cada sinal 1D, uma transformação com *wavelets* diádicas. A aplicação da transformada *wavelet* diádica contínua decompõe o sinal em diferentes níveis de resolução. Como a informação na resolução mais fina é extremamente afetada pelo ruído, somente alguns níveis de baixa resolução são utilizados, excluindo-se o nível mais alto e os mais baixos, de um total de oito. Experimentalmente, Boles chegou à conclusão de que somente o quarto, o quinto e o sexto níveis eram relevantes para a representação de uma íris. O passo seguinte consiste em se calcular a energia entre dois pontos de cruzamento de zero consecutivos no sinal da transformada *wavelet.*

Há outros métodos de reconhecimento da íris. MA *et al*. (2003 *apud* CHAVEZ, 2007), em seu trabalho, propuseram um processo baseado na captura de uma sequência de seis imagens da íris. As imagens são divididas em pequenos blocos, e, assim, o processo baseia-se na localização e reconhecimento desses blocos em cada uma das imagens. Nesse processo, é essencial garantir a qualidade da imagem de entrada, o que se obtém através da análise do espectro em frequência da imagem. Posteriormente, MA *et al*. (2003 *apud* CHAVEZ, 2007) publicaram a descrição de outro sistema eficiente de reconhecimento de íris. O sistema fundamenta-se na geração de sinais em 1D, utilizando um esquema semelhante ao de Boles. O objetivo foi tornar o sistema mais eficiente. Utilizaram-se as variações locais do sinal, caracterizando-o em somente dois níveis de resolução. Os resultados obtidos foram bons em termos de precisão, com uma diminuição de complexidade.

De acordo com Chavez (2007), Sanchez-Avila e Sanchez-Reillo deram continuidade ao trabalho de Boles desenvolvendo um sistema que utiliza a representação *zero-crossing* da transformada *wavelet* para construir *templates* da íris. A inovação em relação ao trabalho de Boles foi a introdução de técnicas baseadas em métricas de distância, como a Euclidiana e a distância de Hamming, para os processos de verificação e decisão.

Tissel (2003 *apud* CHAVEZ, 2007) apresentou uma modificação no algoritmo de Daugman ([1993] *apud* CHAVEZ, 2007) com duas grandes diferenças: a primeira relacionada à localização da íris, e a segunda, a etapa de extração de características. O algoritmo de Tissel aplica a transformada de Hough para estimar o centro da pupila e adota um operador semelhante ao proposto por Daugman para determinar as fronteiras da íris. Para as tarefas de extração de características e representação, a transformada de Hilbert 2D é usada, construindo-se a partir daí uma imagem denominada analítica, que é codificada em um vetor que armazena uma informação de frequência e fase.

Chavez (2007) propôs, em em seu trabalho de mestrado, um novo método para se

representar as características da íris, baseado em *Multiresolution Independent Component Analysis* (M-ICA). ICA é um algoritmo não supervisionado usado para redução de dimensionalidade que faz uso de estatísticas de alta ordem, e o M-ICA é um novo método para extração de características, introduzido pelos autores. O autor apresentou comparações com técnicas baseadas em *wavelets* de Gabor, Haar e Daubechies juntamente com o método proposto. O discriminante de Fisher foi adotado como ferramenta de classificação.

2.2.2 Aplicações de reconhecimento da íris

As aplicações da biometria baseada em íris são bem difundidas em ambientes de alta segurança e estão se expandindo no mundo. Pode-se citar sua utilização em fronteiras de países, aeroportos, setores de telecomunicações com vários servidores, em hospitais, campos de refugiados, penitenciárias, caixas automáticos, *Children's Identification and Location Database* (CHILD Project) e verificação da identidade de uma pessoa (CHAVEZ, 2007).

2.3 Reconhecimento da retina

A retina é a túnica mais interna do globo ocular, sendo formada pelas células sensíveis à luz, os fotorreceptores, as células neurais que participam na transmissão do estímulo visual e a neuroglia retiniana, que dá suporte nutricional e estrutural às outras células. Comparando-se o olho a uma câmara fotográfica, a retina corresponderia ao filme fotográfico, ou ao CCD de uma câmera digital. A parte central da retina situa-se no polo posterior, região oposta à porção frontal do bulbo do olho, o segmento anterior. No polo posterior, visualiza-se o disco do nervo óptico, a mácula (ponto central de fixação do olhar, que é a porção mais sensível à luz da retina) e os vasos arteriais e venosos que se distribuem a partir da papila. A retina estende-se do polo posterior até a região do corpo ciliar, terminando em uma região denominada ora serrata. A retina divide-se em duas camadas: a retina neurossensorial e o epitélio pigmentar retiniano (GARCIA, 2009).

2.3.1 Biometria da retina

Levinsohn apresentou um método de identificação pelas estruturas únicas do fundo de olho, registradas em fotografias, que não tinha, na época, possibilidades técnicas de ser aplicado em larga escala. Em 1935, Simons e Goldenstein chamaram a atenção para o caráter único do

padrão vascular de cada olho. Nos anos 50, Tower estudou as retinas de gêmeos idênticos demonstrando a unicidade de seus padrões vasculares retinianos, considerando inclusive que, entre todos os parâmetros, este era o menos semelhante entre gêmeos. Em 1975, Robert B. Hill, retomando os conceitos de Simons, Goldenstein e Tower, estudou um método biométrico de identificação pelos vasos retinianos, utilizando inicialmente equipamento oftalmológico clínico. Posteriormente, o método foi aperfeiçoado com a utilização de equipamentos mais aceitáveis por parte do usuário e foi colocado no mercado. Problemas técnicos e comerciais têm limitado a ampliação do uso dessa técnica. Recentemente, novas empresas retomaram a biometria retiniana com a utilização de novas tecnologias, inclusive em combinação com a biometria da íris (GARCIA, 2009).

Conforme Costa (2001), a exclusividade de cada padrão vascular retiniano é garantida pelo alto grau de aleatoriedade envolvido no processo de vasculogênese embrionária. Esse padrão é muito estável ao longo da vida, alterando-se, no entanto, em casos de graves retinopatias vasculares (por exemplo, retinopatia diabética avançada, oclusões venosas etc.).

A biometria da retina apresenta as seguintes vantagens: é o mais exclusivo caractere biométrico, com taxas de falsa rejeição e positivação próximas a zero; não pode ser fraudada por estrutura sem vida; apresenta modelo biométrico de pequenas dimensões, facilitando sua informatização; é estrutura estável e protegida por ser interna.

As desvantagens são as seguintes: percepção de ameaça à saúde por parte do usuário (que é falsa); requer escaneamento em pequenas distâncias; exige grande cooperação por parte do usuário; lentes de contato e óculos podem atrapalhar a captação do traço biométrico; possui custo muito elevado.

Segundo Garcia (2009), essas desvantagens dificultam a implementação da biometria retiniana na prática, sendo que só se conhece sua utilização por sistemas com alto nível de segurança, como, por exemplo, recursos militares.

Comparando-se as duas técnicas de biometria ocular, é possível apontar, no momento, as vantagens do sistema de biometria da íris, em todos os aspectos, em relação à biometria retiniana, o que explica sua maior presença no mercado. Realmente, é o sistema de identificação pela íris que tem sido utilizado, isoladamente ou em combinação com outros métodos de identificação ou autenticação, em diversos aeroportos e fronteiras no controle de imigração, no controle de acesso físico a determinadas instalações, na autenticação de identidade em caixas eletrônicos, como meio de controle de uso de aparelhos, como celulares, como forma de autenticação de beneficiários a recursos governamentais, como controle da presença física de apenados em sistemas prisionais, como controle de acesso em escolas e universidades, dentre

outros (GARCIA, 2009).

2.3.2 Aplicações de Biometria na retina

Há conhecimento de que a biometria da retina vem sendo utilizada apenas em algumas instalações militares norte-americanas de alto grau de segurança (GARCIA, 2009).

3 DISCUSSÕES E RESULTADOS

Após leitura e análise de algumas dissertações e teses, é notável que haja certa tendência em pesquisa sobre o desenvolvimento de algoritmos, talvez porque boa parte dos pesquisadores é da área de Computação e opta por desenvolver pesquisas envolvendo técnicas e suas práticas (Quadro 1). Acredita-se que, com a necessidade de maior segurança em eventos importantes que ocorreram e ocorrerão no Brasil, tais como Olimpíadas, Copa do Mundo e Eleições, é um grande incentivo para novas pesquisas e aplicações de sistemas biométricos.

Tipos de Biometria	Autor/ano	Aplicação - Segurança
Impressões digitais, geometria de mão, retina, características faciais, voz e assinatura.	COSTA 2001	Segurança em geral
Impressão digital	NAKASHIRO 2011 CASADO 2008	Presídios, eleição, operações empresariais, governamentais ou institucionais. RG, passaporte, controle de imigração, CNH Controle de Ponto, de Acesso e Presença
Reconhecimento da íris	CANUTO 2010 CHAVEZ 2007	**Alta segurança** Passagens alfandegárias, Aeroportos, Campos de refugiados Verificação da identidade de uma pessoa a partir de uma fotografia **No Brasil:** Pesquisas feitas no INPE, UBC, hospitais, clubes e hotéis
Reconhecimento da retina	GARCIA 2009	**Altíssima segurança** Recursos militares

Quadro 1 – Tipos de biometria conforme alguns pesquisadores brasileiros
Fonte: Autores, 2015.

4 CONSIDERAÇÕES PARCIAIS

Conforme já comentado anteriormente, espera-se que os resultados levantados e analisados indiquem novos caminhos para a utilização da biometria em pesquisas nas universidades brasileiras e no mundo e tragam mais opções para pesquisas na área, pois, embora seja um tema de grande importância, muitas áreas são carentes em pesquisas e literatura, como é o caso deste estudo.

REFERÊNCIAS

CAIÇARA JUNIOR, C.; PARIS, W, S. **Informática, Internet e aplicativos**. Curitiba: Ibpex, 2007.

CANUTO, J. C. **Eficiência da análise multifractal na verificação de assinaturas dinâmicas**. 2010. 104f. Dissertação (Mestrado em Engenharia Elétrica e de Computação) – Faculdade de Engenharia Elétrica, Universidade Estadual de Campinas, Campinas, 2010.

CASADO, R. S. **Extração de minúcias em imagens de impressões digitais**. 2008. 102 f. Dissertação (Mestrado em Engenharia Elétrica) – Escola de Engenharia de São Carlos, Universidade de São Carlos, São Carlos, 2008.

CHAVEZ, R. F. L. **Uma proposta para melhoria na eficiência de um sistema de reconhecimento de íris humana.** 2007. 102 f. Dissertação (Mestrado em Engenharia Elétrica, área de concentração Telecomunicações e Telemática) – Faculdade de Engenharia Elétrica e de Computação, Universidade Estadual de Campinas, Campinas, 2007.

COSTA, S. M. F. **Classificação e verificação de impressões digitais**. 2001. 123 f. Dissertação (Mestrado em Engenharia Elétrica) – Escola Politécnica, Universidade de São Paulo, São Paulo, 2001.

GARCIA, I. A. **A segurança na identificação**: a biometria da íris e da retina. 2009. 129 f. Dissertação (Mestrado em Direito Penal) – Faculdade de Direito, Universidade de São Paulo, São Paulo, 2009.

MA, Li et al. Personal identification based on iris texture analysis. **IEEE Transactions on Pattern Analysis and Machine Intelligence**, v. 25, n. 12, p. 1519-1533, dez. 2003.

MARTINS, E. **O que é biometria?** 2009. Disponível em: <http://www.tecmundo.com.br/o-que-e/3121-o-que-e-biometria-.htm>. Acesso em: 10 nov. 2012.

MORAES, A. F. **Método para avaliação da tecnologia biométrica na segurança de aeroportos**. 2006. 203 f. Dissertação (Mestrado em Engenharia Elétrica) – Escola Politécnica, Universidade de São Paulo, São Paulo, 2006.

NAKASHIRO, M. M. **Biometria no Brasil e o registro de identidade civil: novos rumos para identificação**. 2011. 126 f. Tese (Doutorado em Sociologia) – Departamento de Pós-Graduação em Sociologia, Universidade do Estado de São Paulo, São Paulo, 2011.

PINHEIRO, J. M. **Biometria nos sistemas computacionais:** você é a senha. Rio de Janeiro: Ciência Moderna, 2008.

PINOCHET, L. **Tecnologia da informação**. Rio de Janeiro: Elsevier, 2014.

Recebido em: 19/10/2015

Aprovado em: 28/10/2015

Publicado em: 15/01/2016.