UNIVERSIDADE FEDERAL DE SANTA CATARINA

CAMPUS ARARANGUÁ

Pós Graduação de Tecnologias da Informação e Comunicação aplicadas à Segurança Pública e Direitos Humanos

Fernanda Todesco Nunes

TÉCNICAS DE BIOMETRIA BASEADAS EM PADRÕES FACIAIS E SUA UTILIZAÇÃO NA SEGURANÇA PÚBLICA

Araranguá, 09 de julho de 2015

Fernanda Todesco Nunes

TÉCNICAS DE BIOMETRIA BASEADAS EM PADRÕES FACIAIS E SUA UTILIZAÇÃO NA SEGURANÇA PÚBLICA

Monografia submetida ao Programa de Pós Graduação da Universidade Federal de Santa Catarina para a obtenção do Grau de Especialista em Tecnologias da Informação e Comunicação Aplicada a Segurança Pública e Direitos Humanos Orientador: Prof. Dr. Juarez Bento da Silva.

Araranguá, 09 de julho de 2015

Fernanda Todesco Nunes

TÉCNICAS DE BIOMETRIA BASEADAS EM PADRÕES FACIAIS E SUA UTILIZAÇÃO NA SEGURANÇA PÚBLICA

Esta Monografia foi julgada adequada para obtenção do Título de "Especialista em Tecnologias da Informação e Comunicação aplicadas a Segurança Pública e Direitos Humanos", e aprovado em sua forma final pelo Programa de Pós Graduação da Universidade Federal de Santa Catarina.

Araranguá, 09 de julho de 2015.

Prof. Giovani Mendonça Lunardi, Dr.
Coordenador do Curso

Banca Examinadora:

Prof. Juarez Bento da Silva, Dr.
Orientador
Universidade Federal de Santa Catarina

Profª. Simone Meister Somme Bilessimo, Drª.
Avaliadora
Universidade Federal de Santa Catarina

Profª. Marta Adriana da Silva Cristiano, MSc.
Avaliadora
Universidade Federal de Santa Catarina

Dedico a minha família, por serem muito especiais e essenciais para minha vida. E, por terem me incentivado e apoiado no meu percurso acadêmico.

AGRADECIMENTOS

Agradeço a todos os professores que acompanharam a minha jornada acadêmica, em especial, ao professor Dr. Juarez Bento da Silva, por me orientar e incentivar na realização desta pesquisa.

Agradeço, também, a toda a minha família, pela atenção e força, nos momentos bons e nas horas mais difíceis.

“A menos que modifiquemos a nossa maneira de pensar, não seremos capazes de resolver os problemas causados pela forma como nos acostumamos a ver o mundo”.

(Albert Einstein)

RESUMO

Os constantes e contínuos avanços tecnológicos trazem atrelados a si vulnerabilidade, aumentando a necessidade de evoluir também a forma com a qual são protegidas as pessoas, os bens e os recursos pessoais, públicos ou privados. A biometria é uma área tecnológica que permite identificar pessoas e controlar o acesso aos diversos locais e recursos. Mediante o uso da biometria é possível realizar a identificação e reconhecimento de pessoas, permitindo, por exemplo, selecionar quais as pessoas que poderão ter acesso a certos locais ou recursos. Porém, a biometria não somente é aplicável no controle de acesso de pessoas, ela também tem potencial para aportar um grande apoio no campo forense, na vigilância, no reconhecimento e identificação de pessoas desaparecidas, somente para mencionar algumas possíveis aplicações. Neste trabalho monográfico será apresentado de forma geral as diferentes técnicas de biometria, dando ênfase ao reconhecimento de pessoas através de seus padrões faciais. Buscou-se abordar com mais profundidade as técnicas mais utilizadas no reconhecimento facial com a finalidade de prover informações que possam futuramente dar suporte para o desenvolvimento de novos trabalhos a partir deste.

Palavras Chave: biometria, reconhecimento de rostos.

ABSTRACT

The constant and continuous technological advances bring tied to each other vulnerability, increasing the need to evolve the way in which people are protected, property and personal, public or private resources. Biometrics is a technology area that allows people to identify and control access to various sites and resources. Through the use of biometrics is possible to perform the identification and recognition of people, allowing, for example, selecting which persons may have access to certain sites or resources. However, biometrics is not only applicable in the access control of people, it also has the potential to contribute a great support in the forensic field, supervision, recognition and identification of missing persons, just to name a few possible applications. In this monograph will be presented in a general way the different biometrics techniques, emphasizing the recognition of people through their facial patterns. We attempted to address in more depth the techniques most used in facial recognition with the purpose of providing information that may support future for the development of new work from this.

Keywords: biometrics, face recognition.

ÍNDICE DE FIGURAS

ÍNDICE DE TABELAS

SUMÁRIO

1 Introdução

Muito se fala ou se tem escrito a respeito dos possíveis benefícios das TIC na área de Segurança Pública, assim como da eficiência e transparência que estas podem aportar à Administração Pública e ao Governo em todos seus níveis e áreas. Sem dúvida, que para falar da utilização das TIC na Segurança Pública, deve-se levar em conta o contexto, tanto político-administrativo quanto social, no qual se pretende inseri-las, a fim de, não se deixar cair em “soluções mágicas” nem “receitas universais”.

A necessidade crescente de inclusão digital, por parte dos cidadãos, a adoção de novas tecnologias e seu consequente conhecimento e a vertiginosa rapidez com a qual estas modificam as relações entre as pessoas, demandam uma adequação e desenvolvimento evolutivo do Estado nesta temática. O Estado não é somente um ente jurídico e social que regula e condiciona seus cidadãos. Ele também é influenciado pelos processos sociais, o que o obriga a recompor suas estruturas e ações de maneira continua frente às novas realidades. Como mencionam muitos autores o importante não é nem o “Estado” nem a “Sociedade” e o “e” que as vincula e orienta suas complexas relações. (O´DONELL, 1984).

Um dos processos que caracteriza a sociedade atual é a crescente densidade das relações sociais, produto entre outras coisas, da ingerência que possuem as novas tecnologias. Densidade aqui se refere à capacidade de relacionamentos pessoais de uma maneira mais complexa, onde as ações de uma pessoa repercutem direta ou indiretamente em uma maior quantidade de indivíduos, criando relações de interdependência mais dinâmicas. Também está relacionada a capacidade de relacionamentos com uma maior quantidade de pessoas, no mesmo sentido que levantou Emile Durkheim (1987) quando falou de “densidade dinâmica”. Esta maior densidade gera novos desafios para os Estados, já que a maneira de relacionar-se com e entre seus cidadãos se modifica constantemente. Neste contexto, as TIC aplicadas à Segurança Pública devem ser englobadas em um processo mais amplo de mudanças sociais e das maneiras de relacionamentos entre todos os atores.

Ao fazer referência à capacidade ou não que as TIC podem ter na prevenção ou detecção de delitos, ou na sua resolução e controle, devemos fazer-

nos uma série de perguntas a respeito do grau de inclusão digital da sociedade, da transformação das tipologias delitivas, e da capacidade normativa, organizacional e técnica do Estado.

Nesta monografia pretende-se apresentar um breve panorama sobre a utilização por parte do Estado das TIC, as possíveis aplicações na área de Segurança Pública, seus entraves e soluções, os desafios que o Estado enfrenta em acompanhar a evolução tecnológica, entre outros assuntos pertinentes ao tema.

Será um trabalho direcionado principalmente para a discussão da utilização das tecnologias de reconhecimento biométrico, em especial o reconhecimento facial.

1.2. Pertinência do problema

A pouca informação disponível a respeito de sistemas de reconhecimento facial, tem dificultado e limitado a possibilidade de sua implantação de maneira massiva, bem como, o desenvolvimento de projetos que utilizam este tipo de alternativa nos sistemas de segurança privada ou pública demandam um alto valor de investimento, os tornando possíveis de implantação em um pequeno grupo de empresas ou setores da Administração Pública.

Inúmeros projetos buscam a aplicação do reconhecimento facial principalmente para reforçar a segurança orgânica e patrimonial das instalações privadas e públicas, que produzem conhecimento ou guardam informações de segurança institucional.

Seria possível então reunir técnicas que permitam conhecer e desenvolver um sistema de segurança baseado na biometria estática através de padrões faciais para identificação de rostos humanos nos órgãos de Segurança Pública, e aplicá-los na resolução de crimes?

1.3. Justificativa

Devido à importância e o valor que podem obter alguns dos recursos físicos e informáticos (dados) utilizados nas diversas empresas e instituições, se torna uma necessidade a criação de mecanismos de proteção, tanto de acesso

como de integridade destes recursos. As empresas empregam processos para restringir o acesso somente a determinadas pessoas. Estes processos buscam utilizar mecanismos altamente confiáveis e seguros.

A identificação de pessoas utilizando técnicas de reconhecimento de padrões faciais pode tornar-se uma alternativa segura e pouco invasiva que provê a informação biométrica dada as características únicas que possui o rosto de cada pessoa. Devido aos altos níveis de confiabilidade e segurança providos pela identificação de pessoas através de seus padrões faciais, hoje em dia este modelo é utilizado em empresas, aeroportos, terminais de transporte, instituições bancárias, autoridades e outros tantos lugares onde se fazem necessários.

Diante do aumento da criminalidade, todos os setores da sociedade têm discutido soluções para minimizar os prejuízos sofridos. Visualiza-se um maior investimento por parte das pessoas e empresas em tecnologias de segurança, tais como: sistemas de monitoramento, alarmes, escoltas armadas, equipamentos de rastreamento, etc. A Segurança Pública também tem recebido maiores fatias de recursos financeiros para aprimorar seus sistemas tecnológicos, principalmente com a aquisição de equipamentos de vídeo-monitoramento instalados nas áreas urbanas.

Neste viés, o desenvolvimento de tecnologias de reconhecimento facial em conjunto com os sistemas de vídeo-monitoramentos já existentes, poderá ser uma ferramenta eficaz no combate a criminalidade, principalmente na localização e identificação de foragidos, criminosos, desaparecidos, etc.

1.4. Objetivos

Os objetivos deste trabalho estão divididos em objetivo geral e objetivos específicos.

1.4.1 Objetivo geral

Construir uma monografia que relacione as diferentes técnicas existentes para o tratamento de imagens e que permitam fazer identificação ou reconhecimento de padrões faciais em seres humanos.

1.4.2. Objetivos específicos

- Definir os sistemas biométricos.
- Descrever os tipos de sistemas biométricos.
- Definir quais são os padrões faciais que servem para identificar rostos.
- Identificar e descrever técnicas que são utilizadas no reconhecimento de padrões faciais.
- Analisar como é possível aplicar estas técnicas na construção de sistemas de segurança.
- Descrever de forma simplificada a utilização do reconhecimento facial na área de Segurança Pública no Exterior e no Brasil.

1.5. Opções metodológicas

A partir da metodologia, desenvolve-se a forma da pesquisa, permitindo, por meio de estudos, um melhor entendimento e compreensão.

De acordo com Barros e Lehfeld (2000), a pesquisa é um fato natural e necessário a todos, é um ato dinâmico de questionamento e indagação, que busca respostas a um problema. Porém, para que a pesquisa seja de cunho científico, deve-se concretizá-lo por meio da Metodologia Científica.

Segundo estes autores, a metodologia é um conjunto de procedimentos e técnicas a serem utilizados na obtenção do conhecimento, através da coleta e análise de dados. Assim, de acordo com Barros e Lehfeld (2000, p.68), “através da pesquisa, chega-se a um conhecimento novo ou totalmente novo, isto é, o pesquisador pode aprender algo que ignorava anteriormente”.

As pesquisas devem contribuir na formação de uma consciência crítica, onde os pesquisadores apóiam-se em observações, análises e deduções interpretadas por meio da reflexão.

Neste trabalho, a pesquisa, quanto a sua forma de estudo, caracteriza-se como descritiva. Segundo Andrade (2003), na pesquisa descritiva, os fatos são observados, registrados, analisados e interpretados, sem a interferência do pesquisador, que estuda os fenômenos do mundo físico e humano, porém, não os manipula.

De acordo com Barros e Lehfeld (2000), a pesquisa descritiva, quanto ao objeto, engloba dois tipos: a bibliográfica ou documental e a de campo. O presente estudo se fundamenta na pesquisa bibliográfica.

Segundo Andrade (2003), a pesquisa bibliográfica é sustentada pelas informações de teses, dissertações, artigos, livros, jornais e sites na internet, tendo como finalidade desenvolver os objetivos propostos na pesquisa, ou seja, resolver o problema.

Para Barros e Lehfeld (2000), o pesquisador deverá levantar e selecionar conhecimentos já catalogados em bibliotecas, editoras e internet. Sendo que descreve esta pesquisa como vinculada à biblioteconomia. Segundo estes autores, esta pesquisa é de grande eficácia, pois permite obter uma postura científica quanto à elaboração de informações da produção científica já existente.

Portanto, a pesquisa bibliográfica abrange a leitura, análise e interpretação de livros, periódicos, textos legais, documentos virtuais, fotos, manuscritos etc. Esta pesquisa tem por objetivo conhecer as diferentes contribuições científicas disponíveis sobre determinado tema, dando suporte a todas as fases de qualquer tipo de pesquisa, uma vez que auxilia na definição do problema, na determinação dos objetivos, na construção de hipóteses, na fundamentação da justificativa da escolha do tema e na elaboração do relatório final.

1.6. Estrutura do texto

No primeiro capítulo de introdução é apresentado o problema abordado pela pesquisa e o seu contexto, justificativa, os objetivos e as opções metodológicas. No segundo capítulo é desenvolvido um breve referencial teórico no qual se baseia a pesquisa, ou seja, sobre sistemas biométricos.

O terceiro capítulo busca ser mais específico e aborda o tema reconhecimento facial, buscando assim dar mais profundidade e direcionamento ao referencial teórico. Já o capítulo quatro apresenta brevemente o uso do reconhecimento facial em termos de segurança pública no exterior e no Brasil. E finalmente o último capítulo trata das conclusões.

2. Sistemas Biométricos

Nas civilizações antigas as pessoas viviam em comunidades pequenas onde se reconheciam sem dificuldade, sem dúvida com a mobilidade e a rápida expansão da população, a identificação se converteu em um processo complexo de maneira que nas sociedades modernas tem sido necessária a implementação de sofisticados sistemas de gestão de identidade. A identidade se refere ao conjunto de informações associadas a uma pessoa, como seu: nome, sobrenome, data de nascimento, endereço, entre outras.

Os sistemas de gestão de identidade são utilizados em diferentes aplicações, tais como: nas aduanas, na restrição de acesso à instalações, no controle de acesso à recursos informáticos, nas transações financeiras e na abordagem de vôos comerciais, somente para mencionar alguns. Dentro dos sistemas de gestão de identidade são encontrados os que baseiam seu funcionamento na biometria, são os que realizam a análise dos traços característicos do corpo humano.

2.1. O que é biometria

Biometria tem origem no grego onde “bio” (que significa vida) e “metron” (que significa medida) e se refere a todas aquelas técnicas que permitem identificar e autenticar às pessoas através de suas características fisiológicas e de comportamento. A biometria foi utilizada pela primeira vez em meados do século XIV na China, e foi a partir do século XIX que começou a ser utilizada nas culturas ocidentais. O explorador e escritor espanhol João de Barros relatou que os comerciantes chineses usavam papel com tinta para que as pudessem estampar suas impressões digitais com finalidade de poder diferenciá-las. (SAEED; NAGASHIMA, 2012)

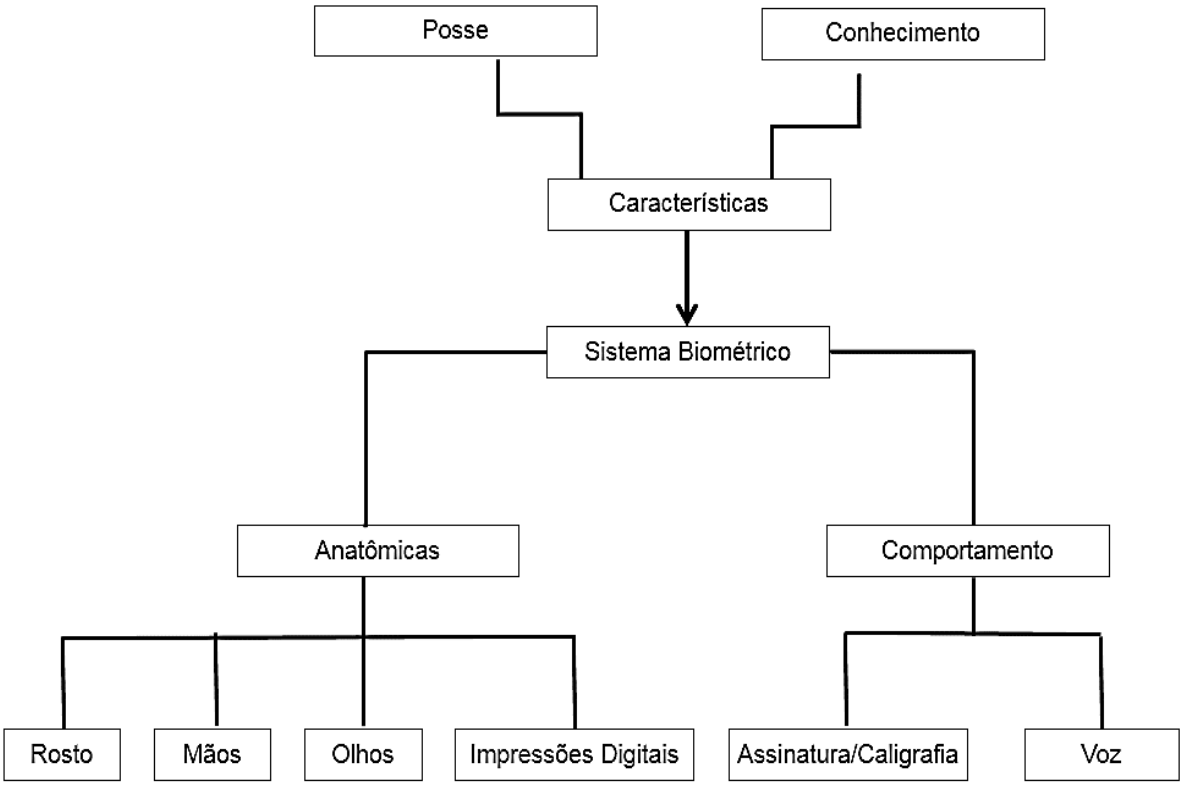
No ocidente, a identificação se baseava simplesmente na “memória fotográfica” até que Alphonse Bertillon, chefe do departamento fotográfico da Polícia de Paris, desenvolveu o antropométrico em 1883. Este foi o primeiro sistema preciso, amplamente utilizado cientificamente para identificação criminal e converteu a biometria em um campo de estudo. Funcionava medindo de forma precisa certos

comprimentos e larguras da cabeça e do corpo, assim como registrar marcas individuais como tatuagens e cicatrizes.

O sistema de Bertillon foi adotado extensamente no ocidente até que se passou a detectar defeitos no sistema, principalmente problemas com os diferentes métodos de medidas e mudanças de medida. (LI; JAIN, 2009)

A figura 1 apresenta um tipo de classificação adotada para sistemas biométricos.

Figura 1: Classificação dos sistemas biométricos



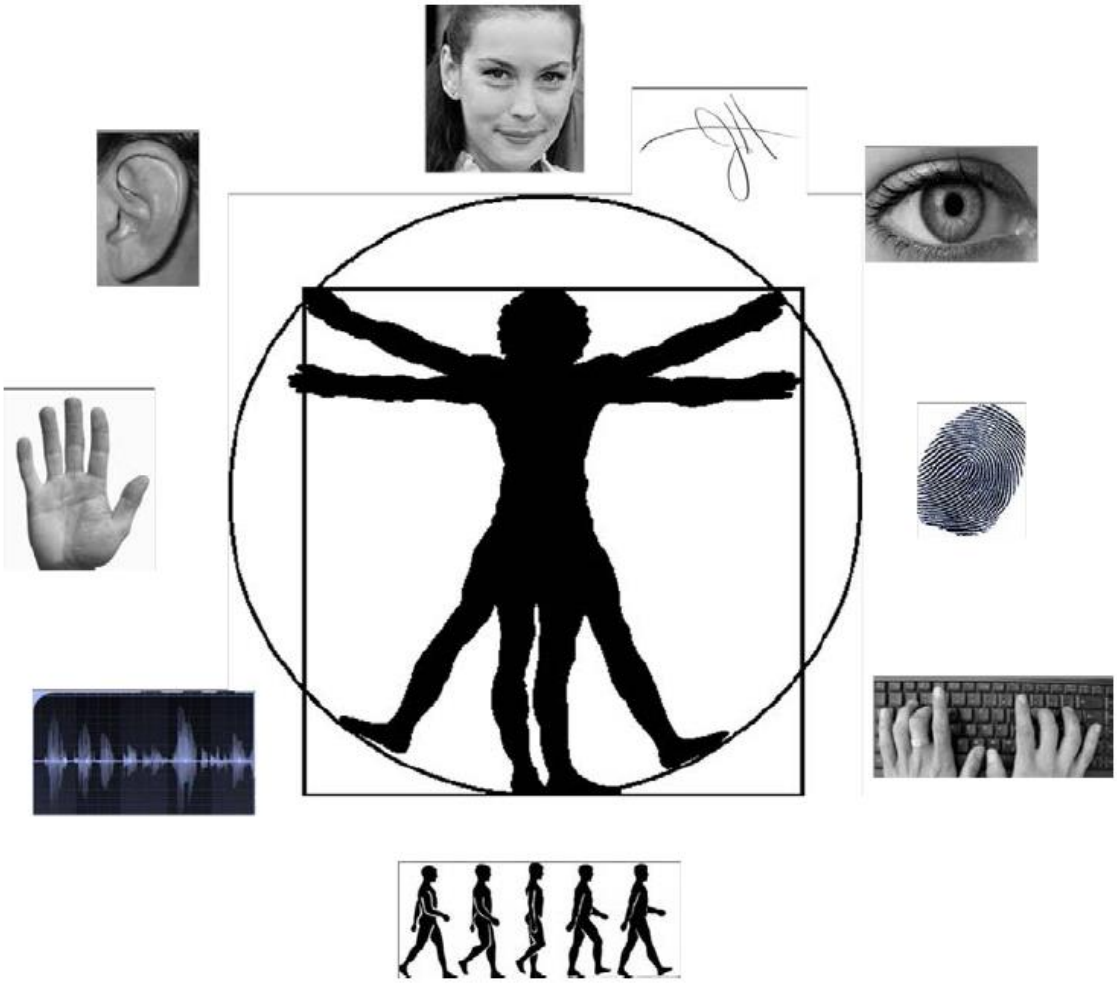
Fonte: Adaptado pela autora de BIOMETRICS-ON, Historia sobre la biometría, Disponível na internet: http://biometrics-on.com/es/historia-sobre-labiometria. asp

Posteriormente, foi colocada em prática a impressão digital como método de reconhecimento por parte das autoridades policiais. Muito parecido com o sistema utilizado pelos chineses há muitos anos. Atualmente a biometria não somente se centra na identificação por meio da impressão digital, mas sim por diversas outras técnicas de reconhecimento que levam em conta várias medidas físicas e também comportamentais.

O reconhecimento biométrico corresponde a um sistema automático baseado na inteligência artificial e no reconhecimento de padrões, que permite a identificação e/ou verificação da identidade de pessoas a partir de características morfológicas ou de comportamento, próprias e únicas de cada indivíduo, conhecidas como identificadores. Atualmente as tecnologias biométricas mais utilizadas são: biometria de impressão digital, geometria da mão e dedos, facial, de íris e de voz. (JAIN; ROSS; NANDAKUMAR, 2011))

A Figura 2 apresenta alguns dos traços característicos do corpo humano.

Figura 2: Exemplos de traços característicos do corpo humano.



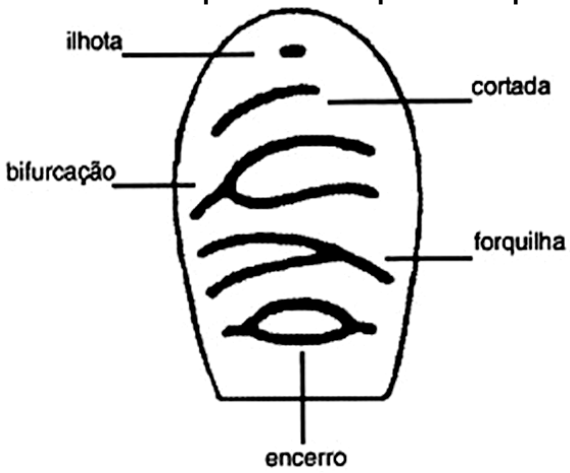
Fonte:

2.1. Impressão Digital

A identificação baseada na impressão digital é a mais antiga das técnicas biométricas e tem sido utilizada em um grande número de aplicações, posto que a maioria da população tem impressão digital única e inalterável. Seu uso foi iniciado no ocidente no final do século XIX no campo forense. Em 1890 o argentino Juan Vucetich foi a primeira pessoa a criar o primeiro método de arquivos de impressão digital, e graças a este método conseguiu esclarecer um crime identificando seu autor mediante as impressões digitais encontradas na cena do crime.

A característica biométrica é a mais utilizada para autenticação e apresenta a maior gama de tecnologias de captura com diversas características de funcionamento. Tem como vantagens sua alta taxa de exatidão e que, habitualmente, os usuários têm conhecimentos suficientes sobre sua utilização. Isto se deve ao padrão único que se forma na ponta do dedo de cada pessoa e mais importante ainda é que se trata de uma característica imutável e que não mudará através dos anos. A única forma para que esta característica se veja alterada reside em fatores genéticos, envelhecimento, meio ambiente, ou por motivos profissionais (pessoas que sofrem cortes ou contusões que fazem com que sua impressão digital se modifique). (LI; JAIN, 2009); (SCHEIDAT; ENGEL; VIELHAUSER, 2006).

Figura 3: Características que formam o padrão na ponta do dedo.



Fonte:

A figura 3 apresenta as principais características biométricas que forma o padrão na ponta de um dedo. Na tabela 1 é possível visualizar brevemente as principais vantagens e desvantagens deste tipo de identificação biométrica.

Tabela 1 - Vantagens e desvantagens da impressão digital

Vantagens	Desvantagens
– Facilidade de uso	– Incidência de erro
– Precisão	– Custo ainda elevado do hardware
– Aceitação do usuário	– Mais fácil de ser fraudado

Fonte: Elaboração da autora, 2015.

O processo de reconhecimento e identificação de pessoas por meio da impressão digital inicia a partir da obtenção de uma imagem detalhada da impressão a ser comparada. Depois de adquirir a imagem esta deve ser ampliada para que se possa capturar os pontos chaves que formam o padrão único na ponta dos dedos. A imagem ampliada posteriormente é convertida em valores binários e submetida a algoritmos que permitem reduzir a espessura das linhas e reduzindo-as a poucos pixels. Com a imagem já processada se procede a identificação do padrão único formados pelas bifurcações da impressão. Finalmente se deve armazenar estes dados em uma base de dados para serem confrontados na hora de realizar um reconhecimento.

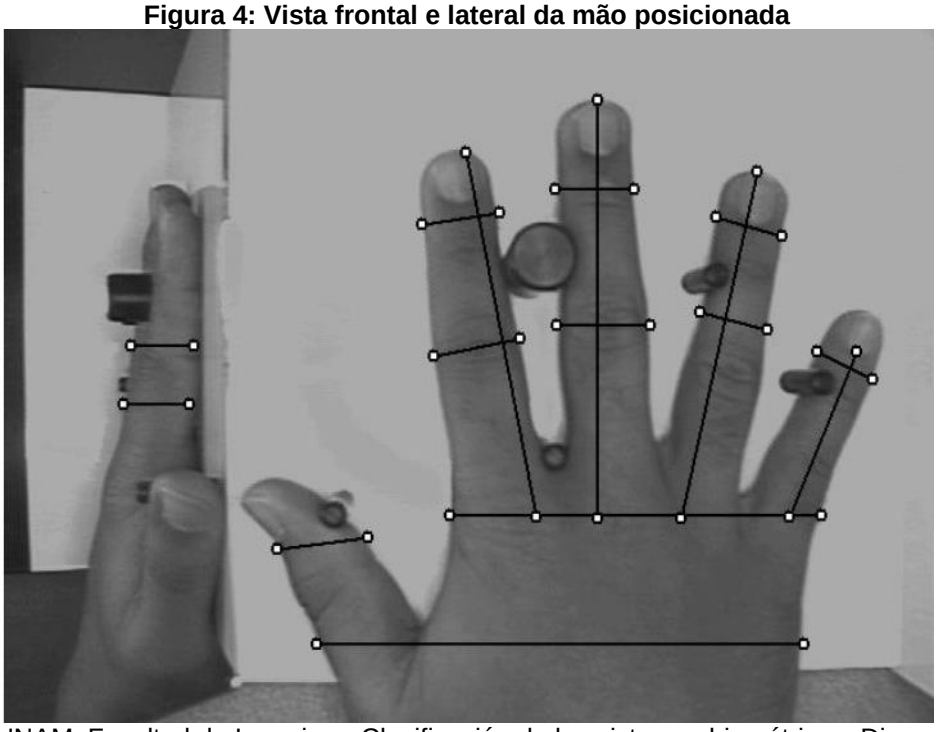
O fato de ser uma técnica pouco intrusiva no ato de aquisição da imagem para a base de dados converte esta em uma técnica altamente aceita pelo público. Aportando a segurança e confiabilidade necessária na hora de reconhecer ou identificar uma pessoa. Graças a estas vantagens, converte na técnica com mais aplicações no mundo real. Esta tecnologia pode ser visualizada em aeroportos na hora de verificar a identidade de um passageiro, nos bancos onde um leitor de impressão verifica a identidade do usuário, em empresas onde o acesso está limitado a certas pessoas, funcionando como um controle de acesso, e para não ir tão longe, nos computadores portáteis que atualmente já vem com este mecanismo para iniciar sessão ou utilizá-los.

2.2. Geometria da mão e dos dedos

O primeiro sistema comercial para reconhecimento de geometria da mão foi disponibilizado no início da década de 70. A Universidade de Geórgia foi uma das primeiras instituições a utilizá-lo, já no ano de 1974 o exército dos Estados Unidos testou o sistema para uso em bancos em 1984, porém o conceito não foi patenteado

até 1985. David Sidlauskas desenvolveu e patenteou o conceito de geometria da mão em 1985 criando ao mesmo tempo a empresa Recognition Systems Inc., cujo primeiro sistema comercial ficou disponível no ano seguinte. Nos Jogos Olímpico de 1996 foi feito uso deste tipo de sistema para controlar e proteger o acesso físico à “Vila Olímpica”. (SHASHIKUMAR; RAJA; CHHOTRAY, 2010).

Figura 4: Vista frontal e lateral da mão posicionada



Fonte: UNAM, Facultad de Ingeniera, Clasificación de los sistemas biométricos, Disponible en internet: http://redyseguridad.fip.
unam.mx/proyectos/biometria/clasificacionsistemas/capturamano.html

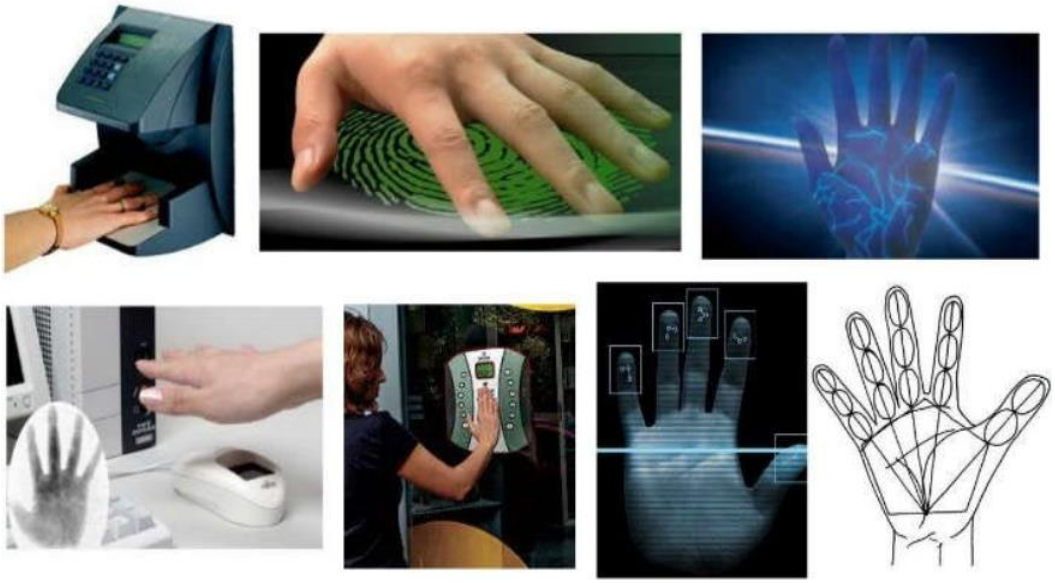
Os sistemas de reconhecimento baseados na geometria da mão se fundamentam em uma série de medidas tomadas da mão, incluindo sua forma, tamanho da palma, comprimento e largura dos dedos.

A técnica é simples, relativamente fácil de usar e de baixo custo. Os fatores ambientais como a umidade ou anomalias individuais como a pele seca, não parecem ter efeitos negativos na validação do reconhecimento destes sistemas. Por outro lado, a geometria da mão não é uma característica completamente exclusiva de um indivíduo. Consequentemente, não podem ser ampliados para sistemas que requeiram a identificação de um indivíduo dentro de uma população grande.

Além disso, a informação geométrica da mão é variável durante o período de crescimento e também por causa do uso de jóias ou certas enfermidades (como a artrite, por exemplo). Outro inconveniente é o tamanho do sistema físico, pois

trata-se de um sistema grande e que não pode ser integrado em determinados dispositivos portáteis. Existem, não obstante, sistemas de verificação que se baseiam em medições de alguns dos dedos (em geral o indicador e o médio), em vez de toda a mão. Estes dispositivos são menores que os utilizados para a geometria da mão, porém ainda assim maiores que os que são utilizam para outras características biométricas (por exemplo: impressão digital, voz, etc.). (LI; JAIN, 2009).

Figura 5: Reconhecimento através de geometria da mão



Fonte: Esteban Saavedra lopez, Ph.D, CEO Opentelematics Internacional Bolivia, biometría y patrones para la identificación humana, Disponible en internet: http://www.slideshare.net/estebansaavedra/biometria-y-patrones-para-laidentificacion-humana

A tabela 2 apresenta brevemente as principais vantagens e desvantagens deste tipo de identificação biométrica.

Tabela 2: Vantagens e desvantagens da geometria da mão e dedos

Vantagens	Desvantagens
– Cômodo para os usuários. – Apropriado para as bases de dados de muitos usuários dado a pouca informação armazenada. – Fácil integração em outros sistemas e processos de controle.	– Custo elevado de hardware. – Ocupa um grande espaço. – Variação da geometria da mão ao longo da vida. – Informação insuficiente para realizar a identificação.

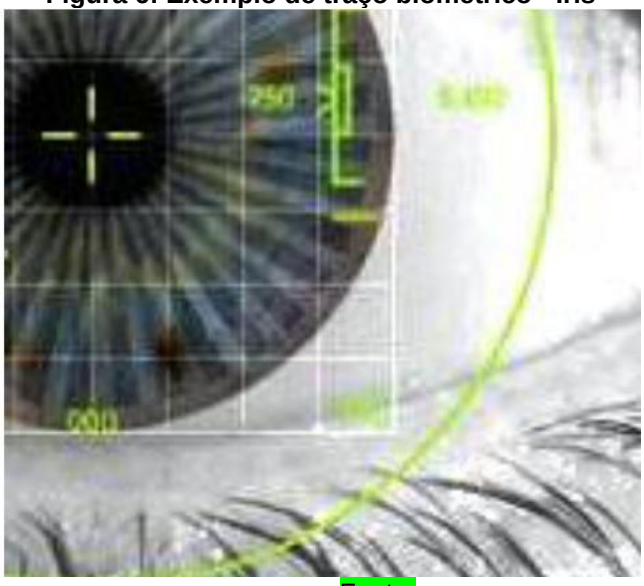
Fonte: Elaboração da autora, 2015.

2.3. Reconhecimento de Iris

A textura da íris se forma durante o desenvolvimento fetal e se estabiliza durante os dois primeiros anos de vida. A complexa textura da íris leva uma informação muito útil como diferenciador de reconhecimento pessoal. A precisão e a velocidade dos atuais sistemas de reconhecimento baseados na íris são promessas e ponto de partida para a viabilidade de sistemas de identificação em grande escala.

Cada íris é diferente, inclusive em gêmeos idênticos. É muito difícil manipular cirurgicamente a íris e relativamente fácil detectar uma artificial (por exemplo: lentes de contato). Dado as características únicas que possui esta técnica de reconhecimento biométrico, brinda uma grande porcentagem de confiabilidade e precisão na hora de reconhecer ou identificar uma pessoa. As primeiras pessoas a tomar conhecimento disso foram os oftalmologistas. (LI; JAIN, 2009) (BERTILLON, 2009).

Figura 6: Exemplo de traço biométrico - Íris



Fonte:

Apesar de que os primeiros sistemas baseados no reconhecimento da íris requeriam uma considerável participação dos usuários e equipamentos caros, os atuais sistemas tem se tornado mais fáceis de usar e econômicos. Como a íris humana é relativamente pequena é necessário contar com o Hardware apropriado para esta técnica e que possa capturar com detalhes a informação da íris. Para isto são necessárias câmeras digitais de alta resolução de forma similar a técnica de reconhecimento facial.

A tabela 3 apresenta as principais vantagens e desvantagens do reconhecimento de íris.

Tabela 3. Vantagens e desvantagens do reconhecimento da íris

Vantagens	Desvantagens
– Alta precisão e baixos níveis de erro. – A característica biométrica é única. – Pouca variação da característica ao longo da vida.	– Alto custo de implementação. – Técnica mais invasiva.

Fonte: Elaboração da autora, 2015.

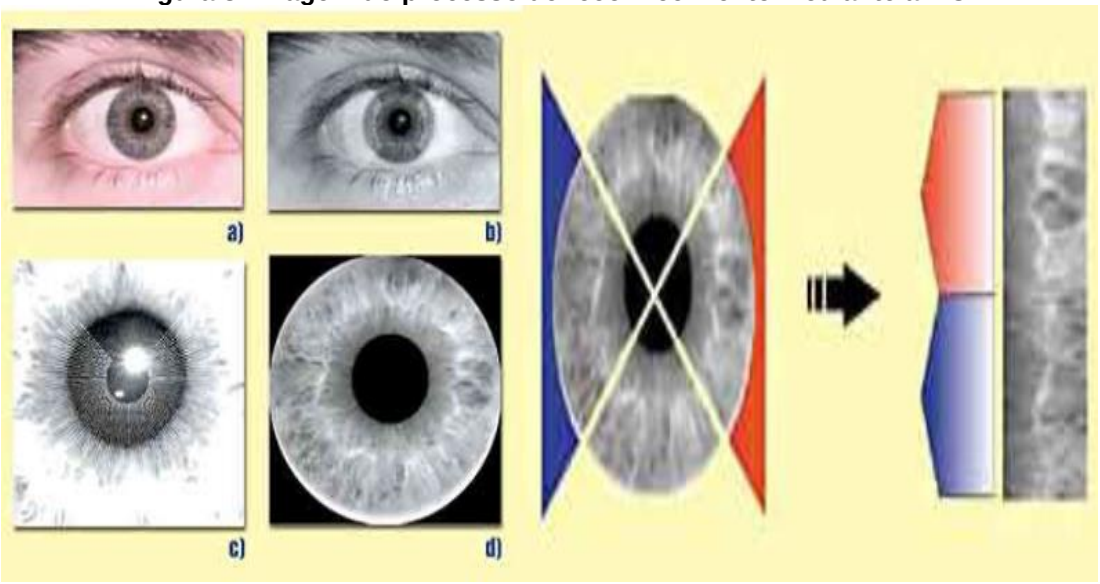
A figura 7 mostra o momento da captura da imagem para um processo de reconhecimento biométrico através da íris.

Figura 7: Momento da captura da íris

Fonte: Blog dedicado a la inteligencia criminal: http://inteligenciacriminal.blogspot.com/

A figura 8 apresenta imagens referentes ao processo de reconhecimento biométrico mediante o uso da íris.

Figura 8: Imagem do processo de reconhecimento mediante a íris



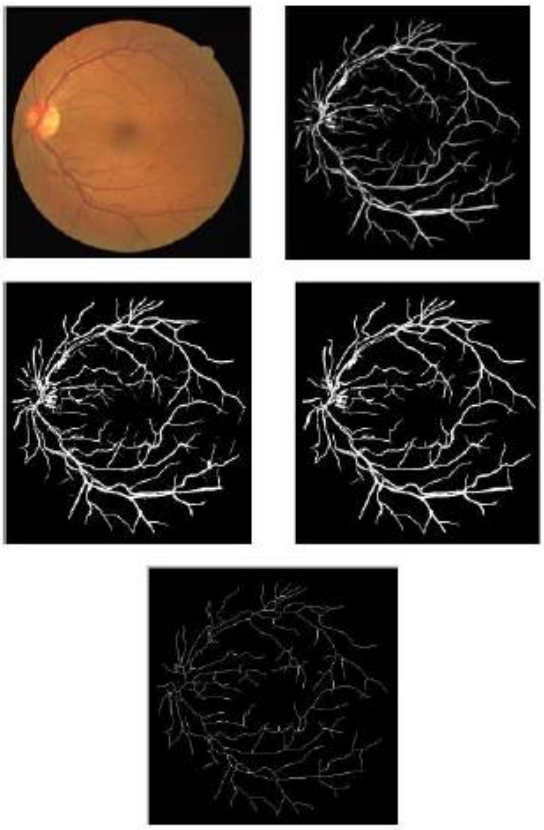
Fonte: UNAM, Facultad de Ingeniera, Clasificación de los sistemas biométricos, Disponible en internet: http://redyseguridad.fip.unam.mx/proyectos/biometria/clasificacionsistemas/capturaretina.html

2.4. Retina

Nos olhos existem características únicas que são utilizadas para identificar pessoas. A parte a íris, o olho abriga outra seção a qual nos permite aplicar biometria informática. A retina possui informação única dentro de sua estrutura a qual permite o reconhecimento e a identificação satisfatória de pessoas.

O reconhecimento biométrico através da retina se baseia na identificação do padrão criado pelos vasos sanguíneos que a formam. Dado que os padrões formados pelos vasos sanguíneos que nascem do nervo óptico e se dispersam através da retina são únicos, estes são ideais para a identificação e reconhecimento de pessoas. Esta informação biométrica é altamente diferenciada já que não existem dois padrões iguais, nem sequer em irmãos gêmeos idênticos. (LI; JAIN, 2009).

Figura 9: Segmentação do padrão vascular



Fonte: M.Z. CheAzemin, Dinesh K. Kumar and Hong Ren Wu, Shape signature for retinal biometrics, School of electrical and computer engineering RMIT University, Australia, 978-0-7695-3866-2 IEEE, 2009.

Esta técnica se destaca entre as demais dado que é uma das mais precisas das atualmente conhecidas no mercado da Biometria Informática. E também porque é uma característica fisiológica estável com baixíssima probabilidade de ser replicada. (UNAM, 2015)

Entre as limitações mais importantes cabe ressaltar que esta resulta ser uma técnica muito invasiva, dado a que se deve aproximar muito o dispositivo de captura a pessoa, resultando muito incomodo e gerando uma grande rejeição por parte dos usuários.

2.5. Reconhecimento de Voz

A voz é uma combinação de dados biométricos fisiológicos e de comportamento. As características da voz de uma pessoa se baseiam na forma e no tamanho do aparelho fonador (boca, fossas nasais e lábios) que se utiliza na criação

do som. Estas características fisiológicas da linguagem humana são invariáveis. Sem dúvida, a parte do comportamento do discurso, esta pode variar com o tempo devido as mudanças causadas pela idade, condições médicas (como o resfriado comum), estado emocional, etc. Também pode ver-se afetada por fatores externos, como o ruído de fundo. Consequentemente, o reconhecimento pela voz pode não ser apropriado para a identificação em grande escala.

Esta técnica biométrica é comumente utilizada em áreas de acesso restrito, e também no campo da criminologia dado a que muitas vezes somente se tem disponíveis gravações da voz dos suspeitos. A figura 10 apresenta exemplo desta característica biométrica.

Figura 10: Exemplo de traço biométrico – Voz

Fonte:

A tabela 4 apresenta algumas vantagens e desvantagens deste tipo de característica biométrica.

Tabela 4: Vantagens e desvantagens do reconhecimento de voz.

Vantagens	Desvantagens
– Ocupa pouco espaço. – Fácil de usar. – Alta aceitação por parte do usuário	– A voz está sujeita a variações. – A voz pode apresentar alterações de volume, velocidade, qualidade e tom.

	– Fácil de enganar com gravações. – O custo de um microfone de alta qualidade é elevado..

Fonte: Elaboração da autora, 2015.

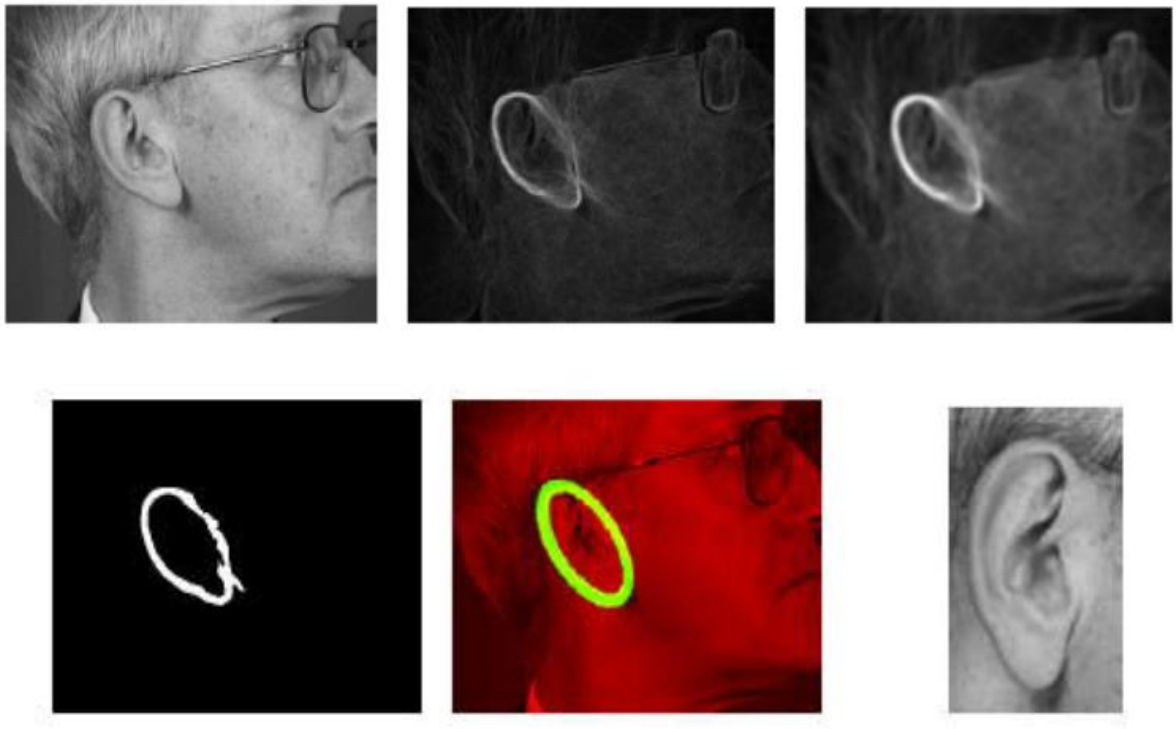
2.6. A orelha

Cientistas da universidade de Southampton descobriram a forma de identificar pessoas através de suas orelhas, os resultados neste tipo de reconhecimento biométrico tem sido quase de 100%. Esta técnica se denomina “a transformação dos raios em imagem”. A transformação dos raios em imagem é uma nova técnica para a extração de características tubulares e circulares que não são encontradas outros métodos.

Esta pesquisa foi realizada pelos professores Mark Nixon, Dr. John Carter e o estudante Alastair Cummings. Se centraram na espiral da orelha e nas armações de óculos. Desta maneira surgiu esta nova biometria. O ouvido é um sistema biométrico com qualidades que lhe conferem superioridade sobre outros tipos de biometria, em particular o ouvido é relativamente imune à variações devidas ao envelhecimento.

O sucesso da biometria do ouvido se baseia em um bom armazenamento dos dados, e que se rege pela posição, escala e rotação. Este método alcançou uma taxa de êxito de 99,6% através de 252 imagens da base de dados XM2VTS. O professor Nixon afirma que a estrutura da orelha não muda desde o nascimento até a morte, somente mudam de tamanho. Outra vantagem é que as orelhas não mudam por expressões faciais, sempre permanecem fixas. (LI; JAIN,2009). (ALSTAIR; CUMMINGS; NIXON, 2010).

Figura 11: Medidas adotadas para a tomada de dados do ouvido



Fonte: Alastair H. Cummings, Mark S. Nixon, John N. Carter, A Novel Ray Analogy for Enrolment of Ear Biometrics, 978-1-4244-7581-0 IEEE, 2010.

2.7. Termogramas

O calor que o corpo humano irradia é uma característica das pessoas a qual é capturada por uma câmera de infravermelho. A identificação do indivíduo é obtida construindo um mapa de valores sobre a forma de cada pessoa. Este sistema não tem nenhum contato físico com o indivíduo e não é invasivo. Porém ao adquirir a imagem por esta técnica pode-se ter problemas devido ao entorno, por exemplo, aparelhos de calefação, escapamentos de veículos, etc. Uma grande vantagem desta técnica é que pode obter imagens em um ambiente com pouca luz ou na ausência da luz.

O reconhecimento por termograma pode depender de uma série de fatores como o estado emocional e a temperatura corporal, além disso, é dependente do ponto de visão que tenha o dispositivo de escaneamento, uma das debilidades que também possui o reconhecimento facial. (GRUPO ATENEA, 2015).

2.8. O “caminhar do indivíduo”

A forma de caminhar das pessoas é um tipo de biometria muito complexo já que pode variar com o passar do tempo devido à lesões que comprometem articulações ou ao cérebro, mudanças de peso, vestimentas, enfermidades ou estados de embriaguez, etc.

Os sistemas baseados no “caminhar” utilizam sequências de vídeo de uma pessoa que caminha para tomar medidas de vários movimentos de cada articulação simultaneamente, pelo que apresenta uma captura intensa e cara computacionalmente. A vantagem deste sistema biométrico é que potencialmente se pode realizar reconhecimento a distância ou com baixa resolução.

Figura 12: Exemplo de traço biométrico – forma de caminhar

Fonte:

2.9. Forma de “digitar”

Não é muito segura, porém existe a possibilidade de que cada pessoa “digite” de forma diferente. Esta técnica se baseia principalmente em reconhecer o padrão da forma de teclar de cada pessoa calculando o tempo que transcorre entre cada pulsação ou o tempo que se mantém pulsada uma tecla.

Para a identificação de uma pessoa através da dinâmica de digitação basta somente o monitoramento do usuário, o que significa que é um sistema não invasivo ou intrusivo. Por ser uma técnica baseada no comportamento pode apresentar alterações na forma de digitação do indivíduo no decorrer do tempo. Uma desvantagem deste tipo de biometria é que não pode ser utilizada em usuários que não sabem escrever em computadores.

Para este tipo são avaliadas características tais como:

- Rapidez;
- Habilidade;
- Efetividade;
- Grau de dificuldade.

Figura 13: Exemplo de traço biométrico – forma de digitar

Fonte:

2.10. Odor

A forma de identificação de um indivíduo através de seu odor corporal é uma técnica utilizada faz muito tempo com cães adestrados. Atualmente são utilizados “narizes eletrônicas” para determinar a existência de agentes químicos no ar, para a identificação de um indivíduo porém ainda não proporcionam a precisão que tem o

nariz humano. Porém, este apresenta grandes problemas já que deve levar em conta o estado de saúde da pessoa, o uso de perfumes, sabonetes, odores ambientais, o contato com outras pessoas, etc. (JAIN; ROSS; NANDAKUMAR, 2011).).

2.11. A “caligrafia”

Uma maneira muito simples, porém não totalmente segura para identificar uma pessoa é por meio do uso de sua caligrafia. A caligrafia de cada pessoa apresenta características únicas, dependendo muito da caligrafia. Para poder diferenciar uma caligrafia de outra são avaliadas propriedades próprias de cada uma, tais como:

- As semelhanças apresentadas na caligrafia;
- A legibilidade na hora de escrever;
- A direção que toma a escrita;
- A velocidade com a qual se escreve;
- O espaçamento entre os caracteres;
- A uniformidade com a qual se escreve;
- Formas distintivas que as pessoas adicionam na hora personalizar sua assinatura.

O processamento no reconhecimento de pessoas usando a caligrafia é composto de três etapas principais:

- Etapa de Pré-processamento: nesta etapa se obtém a caligrafia e se aplica um processo para eliminação de ruído para obtenção dos dados necessários para a verificação.
- Etapa de extração de informação: consta da avaliação da imagem processada avaliando as características da escrita, posteriormente extraindo a informação.
- Etapa de verificação: a informação extraída é comparada com a informação da caligrafia armazenada previamente em uma base de dados dando como resultado se coincide ou não. (JAIN; ROSS; NANDAKUMAR, 2011) (SHASHIKUMAR; RAJA; CHHOTRAY, 2010).

A figura 14 apresenta um método de “captura” da assinatura de uma pessoa.

Figura 14: Exemplo de traço biométrico – “capturando a assinatura”

Fonte:

A tabela 5 apresenta um quadro comparativo entre os diferentes sistemas biométricos apresentados nesta seção.

Tabela 5: Quadro comparativo dos diferentes sistemas de reconhecimento biométrico

Característica	Aceitação pelo usuário	Facilidade de uso	Custo	Estabilidade	Invasiva	Confiabilidade
Impressão digital	Alta	Alta	Médio	Alta	Não	Média
Geometria da mão	Média	Alta	Alto	Média	Não	Média
Íris	Média	Média	Alto	Alta	Média	Alta
Retina	Média	Baixa	Alto	Alta	Média	Alta
Voz	Alta	Alta	Médio	Média	Não	Baixa
Face	Média	Média	Alto	Alta	Não	Alta

Fonte: Elaboração da autora, 2015.

3. RECONHECIMENTO FACIAL

O reconhecimento facial automatizado é um conceito relativamente novo, desenvolvido pela primeira vez na década de 1960. Esta tecnologia chamou muito a atenção do público, quando em 2001, durante o SuperBowl da NFL (Liga Nacional de Futebol Americano), foram capturadas imagens de vigilância e comparadas com uma base de dados de foto-arquivos digitais. Desta demonstração originou-se um importante debate sobre como usar a tecnologia para satisfazer necessidades, principalmente governamentais, porém, levando em consideração as preocupações sociais e de privacidade das pessoas. Atualmente a tecnologia de reconhecimento facial está sendo muito utilizada para combater, por exemplo, as fraudes de passaportes, a identificação de crianças desaparecidas, em minimizar as fraudes nas identificações e controle de acesso, entre outras.

Nos últimos anos têm sido realizados estudos mais detalhados devido a necessidade de encontrar meios para reconhecer às pessoas a partir de seus traços característicos, e no campo da segurança é onde tem sido exigidos os maiores avanços.[1]

Os principais modos de aplicação dos sistemas de reconhecimento facial, podem ser classificados em três grupos:

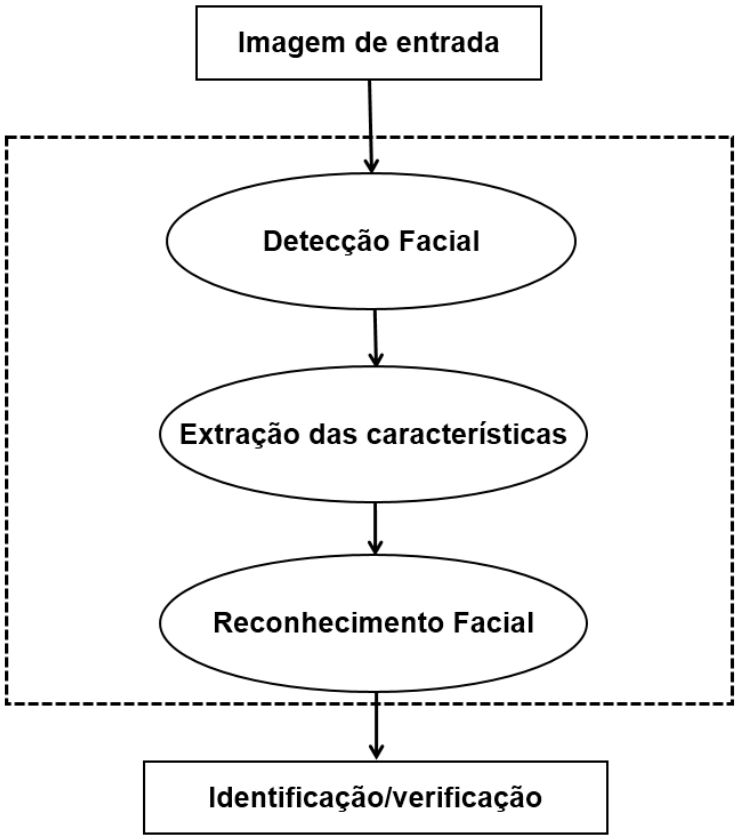
- Verificadores de identidade: servem para autenticar uma identidade de uma pessoa;
- Identificação: uma vez extraídas as características estas são comparadas em uma base de dados e mediante o uso de determinado algoritmo é tomada uma decisão em relação à identidade;
- Buscas: segue o mesmo algoritmo que a identificação, porém, com a diferença, pois, necessita de um padrão de acertos.

3.1. Definição de reconhecimento facial

[1] http://www.cienciaeingenieria.com/2013/09/la-gran-tendencia-reconocimiento-facial.html 27-09-2013. http://bibdigital.epn.edu.ec/bitstream/15000/5504/1/T2481.pdf 17-07-2013

É a capacidade de reconhecer as pessoas por suas características faciais. É uma tecnologia mais avançada e se baseia em algoritmos, por exemplo o Eigenfaces, que mapeia as características do rosto de uma pessoa em um espaço multidimensional. Os computadores podem realizar buscas em bases de dados faciais e/ou efetuarem verificações ao vivo um-a-um ou um-para-muitos, com uma precisão sem precedentes e o processamento em uma fração de segundo. Os usuários podem ter acesso seguro em seu computador, dispositivo móvel, ou para comércio eletrônico on-line, simplesmente olhando para sua câmera web. A figura 15 um fluxograma básico de um sistema automático de verificação facial e suas principais etapas. (LI; JAIN, 2009) (TURK; PENTALAND, 1991).

Figura 15: Diagrama de blocos representativo do problema de reconhecimento automático de rostos.

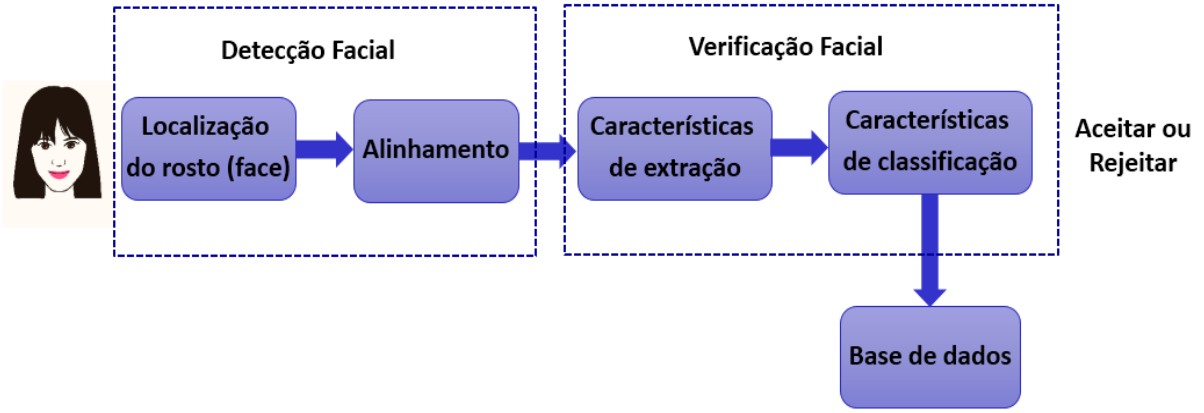


Fonte: Adaptado pale autora de http://iie.fing.edu.uy/investigacion/grupos/biometria/proyectos/aguara/descargas/documenta_aguara_v1.0.pdf

Em geral um sistema automático de verificação facial é composto de duas etapas principais (Figura 16): detecção de rosto (primeira etapa) e verificação do rosto (segunda etapa). Na detecção de rosto, o objetivo é determinar se existe um

ou mais rostos em uma imagem (ou vídeo), e se for o caso, retornar sua posição e escala. O termo localização é empregado quando existe unicamente um rosto na imagem. A detecção do rosto é um aspecto muito importante na pesquisa, porque serve como um primeiro passo necessário para qualquer sistema de processamento facial, como reconhecimento do rosto, acompanhamento e análise de expressões. A maioria das técnicas utilizadas assume, em geral, que a região do rosto tenha sido localizada perfeitamente. Portanto, o rendimento deste sistema depende significativamente da precisão da etapa da detecção facial ou do rosto.

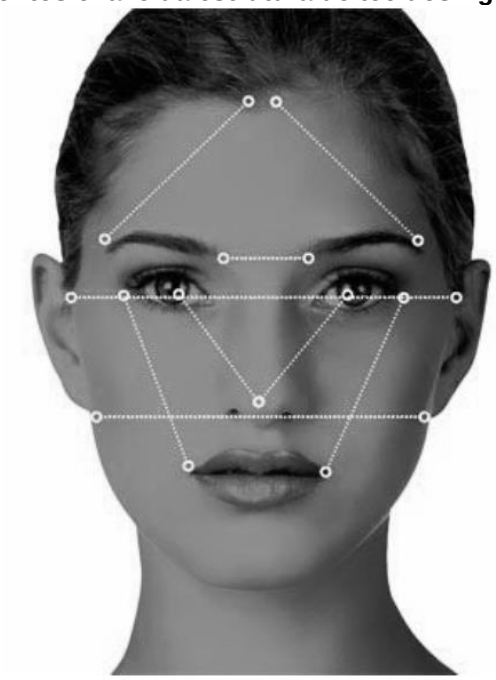
Figura 16: Estrutura de um sistema de verificação composto de dois módulos



Fonte:

A figura 17 apresenta os pontos chave utilizados na verificação e identificação facial.

Figura 17: Pontos chave da estrutura de tecidos rígidos do rosto



Fonte Cesar Tolosa Borja, Álvaro Giz Bueno, “Sistemas Biométricos”, Disponível em: http://www.dsi.uclm.es/asignaturas/42635/web_BIO/Documentacion/Trabajos/Biometria/Trabajo%20Biometria.pdf

3.2. Breve histórico

O conceito de identificação ou reconhecimento facial foi introduzido nos anos 1960. “Durante os anos 1964 e 1965 Woodrow Wilson Bledsoe, Helen Chan Wolf e Charles Bisson trabalharam no reconhecimento facial humano fazendo uso do computador e desenvolveram o primeiro sistema semiautomático de reconhecimento. (GALVIS TRASLAVIÑA, 2015).

Nos anos 70 Goldstein, Harmon, & Lesk, usaram 21 características físicas específicas tais como a cor do cabelo e a espessura dos lábios para automatizar o reconhecimento facial, porém identificar estas características continuava requerendo um processo manual. Ao final dos anos 1980 eles produziram um ponto de referência quando Kirby e Sirovich aplicaram uma técnica padronizada de álgebra linear, a análise dos principais componentes (PCA). (TURK; PENTALAND, 1991).

No início da década de 1990 Turk e Pentland utilizando a técnica de “eigenfaces”, nome que recebeu o método descoberto por Kirby e Sirovich, demostraram que, “o erro residual podia ser utilizado para detectar rostos nas imagens, uma descoberta que permitiu desenvolver sistemas de reconhecimento confiáveis em tempo real. Se bem que a abordagem era um tanto forçada por

fatores ambientais, porém, sem dúvida criou um interesse significativo para posteriores desenvolvimentos destes sistemas. (TURK; PENTALAND, 1991).

Porém foi no ano 2001 que o uso de câmeras de vigilância chamou a atenção de uma grande quantidade de público na partida do Super Bowl, pois nesta ocasião o processo consistiu na captura de imagens através das câmeras de vigilância para depois serem contrastadas e identificadas com uma base de dados que armazenavam imagens digitalizadas de delinquentes. (SUCAR, 2008)

3.3. Aplicações

A técnica de identificação e reconhecimento facial adquire um novo uso em entidades governamentais satisfazendo suas necessidades. Atualmente se pode ver o grande impacto que tem conseguido esta tecnologia, a qual é utilizada em locais onde se deseja levar um controle de acesso e lugares que requerem identificação plena de todas as pessoas como nos aeroportos e terminais de transporte. Inclusive esta tecnologia pode ajudar em atividades tão importantes como a de encontrar pessoas desaparecidas ou em fraudes cometidas muitas vezes ao suplantar a identificação de outra pessoa.

A tabela 7 apresenta algumas áreas e aplicações específicas com reconhecimento facial.

Tabela 7: Aplicações com reconhecimento facial

Área	Aplicações Específicas
Biometria	Carteiras de habilitação, Imigração, Passaportes, Registro Eleitoral, Fraude, Telefones inteligentes, Acesso à instalações restritas.
Segurança da informação	Início de Sessão, Segurança de Aplicações, Segurança em Bases de Dados, Codificação de Informação, Segurança na Internet, Acesso à Internet, Registros Médicos, Terminais de Comércio Seguro, Caixas Automáticos.
Cumprimento da lei e vigilância	Vídeo vigilância Avançada, Controle CCTV, Controle de Portais, Análises Post-event, Furto, Acompanhamento de

	Suspeito, Investigação.
Tarjetas inteligentes	Valor Armazenado, Autenticação de usuários.
Controle de acesso	Acesso à Instalações, Acesso à Veículos.

Fonte: Elaboração da autora, 2015.

3.4. Detecção de rostos

Um dos grandes problemas na identificação de rostos é a detecção dos mesmos por meio de imagens. Para que o algoritmo funcione perfeitamente se deve fazer uma detecção precisa da imagem. O algoritmo não somente deve detectar o rosto para a identificação ou verificação de pessoas, porém, também deve levar em conta outros aspectos os quais poderiam dificultar o processo de detecção do rosto tais como:

- Estado de ânimo da pessoa;
- Posição e orientação do rosto;
- Tamanho do rosto;
- Presença de lentes, barba, gorros, etc.;
- Expressão do rosto;
- Problemas de iluminação;
- Condições da imagem;
- Quantidade desconhecida de rostos na imagem.

Abaixo é mostrada uma imagem com as complicações que se apresentam ao localizar rostos em um cenário real.

Figura 18: Exemplo das complicações a serem levadas em conta ao localizar rostos em um cenário real

Fonte:

Existem outros problemas na localização de rostos relacionados com:

- Localização de características relevantes: olhos, boca, sobrancelhas, queixo, orelhas, etc.;
- Reconhecimento de expressões: triste, alegre, enojado, etc.;
- Estimativa da posição e seguimento.

A figura 19 mostra como pequenas mudanças podem confundir um sistema visual de reconhecimento. (GOLDSTEIN; HARMON; LESK, 1971)

Figura 19: Exemplo das complicações a serem levadas em conta ao identificar rostos

Fonte:

Atualmente existem algoritmos de detecção de rostos dependentes dos cenários a serem considerados. Uma possível classificação dos algoritmos de detecção de rostos pode ser:

- **Métodos Baseados em Características Faciais:** aqueles que buscam encontrar características presentes em qualquer rosto: olhos, sobrancelhas, lábios, boca, queixo, linhas de contorno, etc.
- **Métodos Baseados na Imagem:** aqueles que aplicam ferramentas gerais de reconhecimento de padrões para sintetizar um modelo a partir de um conjunto de imagens de treinamento. Trabalham com a imagem completa ou uma região desta sem buscar características faciais de forma localizada.

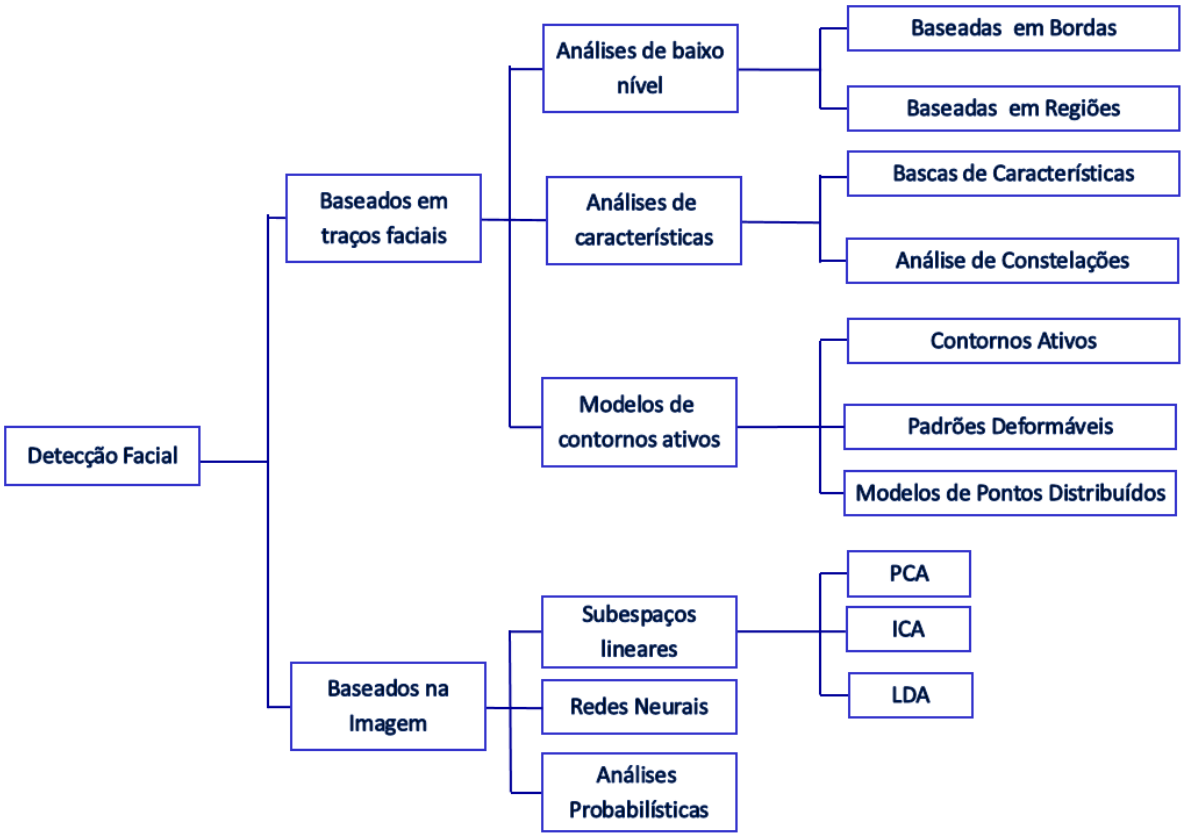
Porém a anterior não é a única classificação possível. Outras classificações possíveis são:

- Métodos baseados em cores VS. Métodos baseados em tons de cinza;
- Métodos holísticos vs. Métodos locais;
- Métodos de localização em tempo real vs. Métodos off-line. (YANG; RIEGMAN; AHUJA, 2002) (HJELMAS; LOW, 2001).

3.5. Métodos baseados em traços faciais

O início do desenvolvimento de projetos nesta área tem seu início nos anos 1970, motivado por idéias intuitivas da representação de um rosto. Os primeiros métodos buscavam resolver o problema de encontrar os traços (características) de um rosto em uma situação totalmente controlada (fundo branco, rosto de frente, expressão neutra). A maioria deles se baseava em buscar relações geométricas entre pontos característicos encontrados mediante heurística. Ao longo dos anos, e em particular na última década cresceu de maneira substancial o interesse para resolver este problema, obtendo assim um desenvolvimento muito importante da área. Podem ser definidos três ramos dentro do conjunto de métodos baseados em traços faciais:

Figura 20: Uma possível classificação dos métodos de detecção facial.



Fonte: Adaptado pela autora de http://iie.fing.edu.uy/investigacion/grupos/biometria/proyectos/aguara/descargas/documenta_aguara_v1.0.pdf

Análises de baixo nível: são técnicas que trabalham diretamente com os pixels, existem duas principais:

- **Baseadas em bordas**: buscam bordas, as afinam, etiquetam e finalmente buscam estruturas similares às de um rosto.
- **Baseadas em regiões**: aproveitam o fato de que existem zonas mais escuras que o restante do rosto (sobrancelhas, pupilas, etc.). A imagem é separada em regiões. O rosto é localizado através da comparação da distribuição das regiões presentes com a distribuição das regiões específicas de um rosto.

Análises de características: Dado que a análise de baixo nível pode ocasionar informação parcialmente correta ou incompleta, este grupo de métodos busca encontrar implicitamente os traços faciais. Baseia-se fortemente nas relações geométricas que apresentam os diferentes traços presentes em um rosto. Existem duas grandes abordagens a respeito:

- **Busca de traços**: tentam realizar uma busca ordenada dos traços característicos de um rosto. Por exemplo, primeiro buscam a testa, logo após os olhos, continuam com o nariz, etc. Baseia-se na hipótese sobre a posição e a orientação do rosto e utilizam heurística.
- **Análise de Constelações**: buscam levantar algumas das hipóteses dos métodos anteriores sobre a posição e orientação do rosto. Baseia-se em uma análise probabilístico da localização certos pontos característicos (constelação) de um rosto.

Análise mediante modelos de contornos ativos: os métodos baseados em modelos de contornos ativos buscam adaptar um modelo genérico de um traço (olho, boca, contorno do rosto) a imagem ou porção da imagem em questão. Para isto, buscam iterar deformando o modelo até adaptá-lo ao traço buscado. Baseia-se fortemente na informação local da imagem (bordas, tons de cinza). Existem três grandes técnicas:

- **Snakes ou contornos ativos**: são comumente utilizados para encontrar o contorno do rosto. Baseia-se na minimização de uma função de energia para adaptar o modelo.
- **Padrões deformáveis**: buscam adaptar modelos paramétricos de cada traço facial. Similar aos Snakes, se baseia em minimizar uma função de energia para a adaptação.
- **Modelos de pontos distribuídos (PDM):** é uma maneira compacta de representar de forma paramétrica as formas buscadas. O ajuste destes modelos se baseia em dividir o contorno PDM em diferentes pontos etiquetados (identificados). As variações possíveis destes pontos são armazenadas em um modelo estatístico realizado cuidadosamente a partir de um conjunto de treinamento. (LI; JAIN, 2005)

3.6. Métodos baseados em imagem

Os métodos anteriormente descritos são muito frágeis para mudanças que possam apresentar as imagens, por exemplo, o surgimento de rostos ou mudanças

no ambiente (iluminação, fundo). Para resolver este problema surgiram as seguintes técnicas: subespaços lineares, redes neurais e análise probabilística.

3.6.1. Subespaços lineares

Estas técnicas se baseiam na representação das imagens dos rostos em espaços lineares buscando a que espaço linear pertence mediante uma análise estatística, entre as quais são destacadas: PCA (análise dos componentes principais), LDA (análise de discriminante linear), ICA (análise de componentes independentes).

- **Análise de Componentes Principais (PCA):** A análise dos componentes principais ou PCA (do inglês Principal Component Analysis) foi introduzida em 1901 por Karl Pearson. Esta ferramenta permite extrair informação, a priori, não visível, capaz de caracterizar um dado fenômeno multidimensional. Além disso, o volume de dados resultantes é menor ou igual à quantidade original, de maneira que em geral, a PCA permite reduzir o volume de dados sem perder informação. (JOLLIFFE, 2002)

  É uma técnica tradicional no reconhecimento de rostos e provavelmente a mais utilizada. Esta técnica consiste em extrair de um conjunto de imagens de treinamento um subespaço que maximize a variância do espaço original. Os vetores que são obtidos destes cálculos são denominados Eigenfaces. Estes são vetores obtidos dos valores próprios maiores da matriz de covariância das imagens originais. Desta maneira se consegue reduzir de forma considerável a dimensão do problema, tomando as características únicas e próprias das imagens originais. Para em seguida fixar as métricas nas quais será efetuado o reconhecimento encontrando a distância do vetor de características de entrada com a distância dos vetores armazenados na base de dados.
- **Análise de Componentes Independentes (ICA)**: A Análise de Componentes Independentes ou ICA (do inglês Independent Component Analysis) é uma particularização da PCA. Esta dita particularização se refere à capacidade da ICA para extrair componentes que são, ao mesmo tempo, estatisticamente independentes e não-gaussianas. Isto é possível pelo fato que existem numerosos campos e problemas para os quais a ICA tem demonstrado ser

uma ferramenta de grande utilidade: economia, medidas da atividade cerebral como EEG e MEG, telecomunicações, etc (HYVÄRIBNEN, 2000). Este método busca representar o espaço de rostos em um subespaço que minimize a dependência de segunda e de maior ordem entre seus componentes. Assume-se que os sinais de entrada são combinações de fontes não observáveis estatisticamente independentes. Se a combinação é linear, pode-se definir uma matriz de combinação cujos coeficientes são os que definem a combinação linear. Então a ICA estima a matriz inversa da matriz de combinação. Cabe salientar que para aplicar ICA se utiliza previamente a PCA para reduzir a dimensionalidade do espaço original de rostos e diminuir o custo computacional.

- **Análise de Discriminante Linear (LDA):** A análise discriminante linear é umas das técnicas mais utilizadas na hora de implementar um sistema de reconhecimento e identificação mediante o uso dos padrões faciais localizados no rosto. Esta técnica consiste em encontrar combinações lineares para poder reduzir a dimensão do problema, de tal maneira que se mantenha a habilidade de separar duas ou mais classes de objetos.

  Este algoritmo busca levar o espaço de caras a um subespaço de baixa dimensionalidade que aumente a separabilidade das classes presentes. A idéia do algoritmo é encontrar a base de vetores em um subespaço que melhor discrimine entre as diferentes classes, no caso do reconhecimento das identidades. Utiliza-se todas as amostras de todas as classes e se calcula a matriz de dispersão entre as diferentes classes (inter-classe) e a matriz de dispersão na mesma classe (intra-classe). Se busca maximizar a relação entre o determinante da matriz inter-classe e o determinante da matriz intra-classe. Aos elementos da base que maximiza a relação anterior, se denomina Fisherfaces em honra a Robert Fisher que em 1936 propôs uma solução baseada no método clássico de reconhecimento de padrões denominado Fisher’s Linear Discriminant (FLD). A diferença principal em relação ao PCA é que a LDA se orienta para a discriminação entre as classes do problema, enquanto que a PCA não leva em conta esta distinção.

3.6.2. Redes neurais

É a técnica de maior uso para o reconhecimento de padrões já que permite verificar se uma imagem contém um rosto. Isto se obtém treinando as redes neurais com imagens que contém rostos e outras imagens que não contém. Além disso, buscam solucionar o problema de saber se um objeto interfere com a imagem do rosto. Existem modelos de redes de diferentes complexidades (quantidade de neurônios, tipos de neurônios, quantidade de camadas de neurônios, conexões entre neurônios) com as quais se obtém distintas performances. Também existem abordagens locais de redes neurais (não holísticas), cujo objetivo é encontrar diferentes estruturas locais e logo com base nelas reconhecer o objeto em questão.

3.6.3. Análise probabilística

É outra série de métodos estatísticos para a detecção de rostos. Muitos deles se baseiam em princípios funcionais de reconhecimento de padrões como podem ser o princípio de máxima plausibilidade ou a distância de Kullback-Leibler. Esta classe de métodos busca estimar distribuições de probabilidade mediante histogramas e logo comparar os mesmos frente a histogramas médios aprendidos estatisticamente de imagens com rostos.

3.7. Reconhecimento de rostos

O reconhecimento de rostos tem sido estudado por várias disciplinas tais como:

- A psicologia;
- Reconhecimento de padrões;
- Redes neurais;
- Visão por computador.

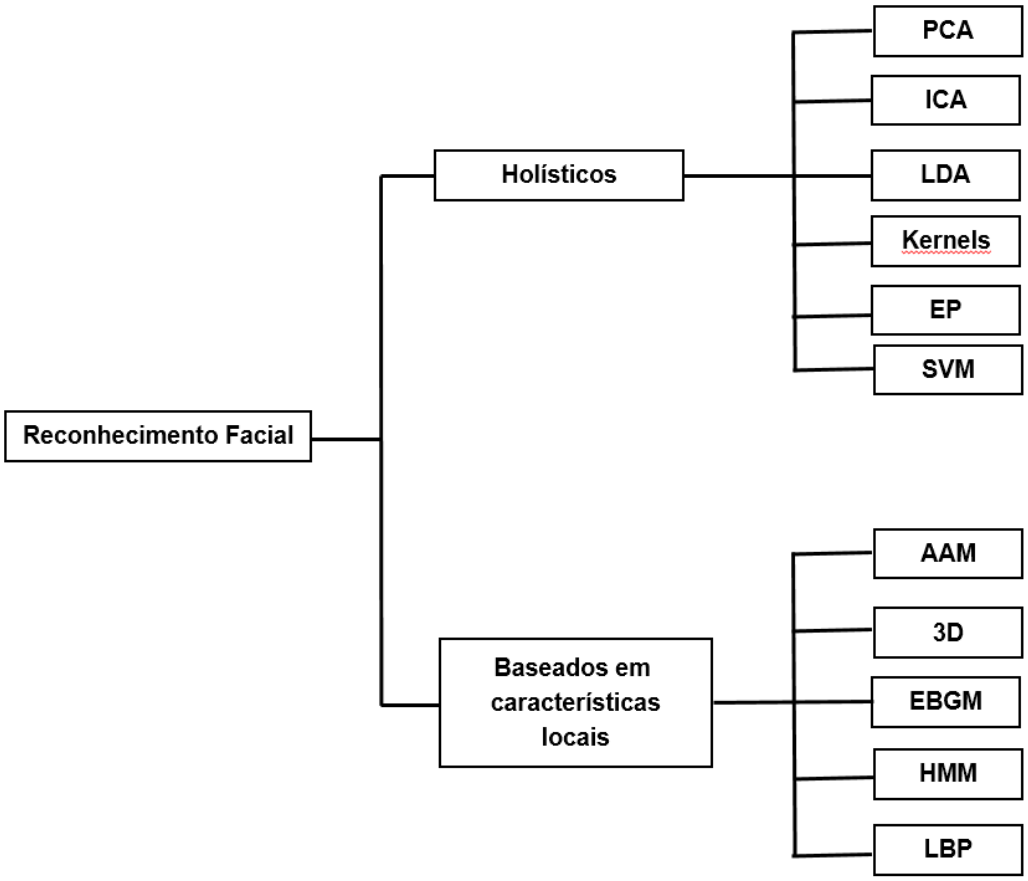
As quais dividem o reconhecimento de rostos em dois grandes métodos:

- **Métodos holísticos:** a imagem do rosto é o dado de entrada, sendo utilizada como a unidade básica de processamento.

- **Métodos baseados em características locais:** são extraídas as características locais do rosto, (olhos, nariz, boca, sobrancelhas, etc.) suas posições formam a entrada do sistema de reconhecimento.

Existe outro método chamado “híbrido” o qual combina os dois métodos anteriores. A figura 21 a seguir mostra a classificação de alguns dos métodos de reconhecimento de rostos.

Figura 21: Classificação de alguns métodos de Reconhecimento de Rostos.



Fonte:

3.7.1. Métodos holísticos

São classificados em: Análise de Componentes (PCA, ICA e IDA), Métodos baseados em Kernels, Evolutionary Pursuit (EP) e Support Vector Machine (SVM).

Os métodos de Análise de componentes podem ser:

- **Análise de Componentes Principais (PCA):** este considera a distribuição de imagens de um rosto e tenta capturar variabilidade destas imagens, buscando a independência de qualquer rosto ou característica particular. É denominado PCA porque busca extrair, de um conjunto de imagens de treinamento, um subespaço cuja base maximize a variância do espaço original. Estes vetores gerados são chamados de Eigenfaces. (TURK; PENTALAND,1991).
- **Análise de Componentes Independentes (ICA)**: Este método tenta representar o espaço das faces em um subespaço que minimize a dependência de segunda e de maior ordem entre seus componentes. Assume que os sinais de entrada são combinações de fontes não observáveis estatisticamente independentes. (HAVRAN at al, 2002).
- **Análise de Discriminante Linear (LDA):** este algoritmo tenta levar o espaço dos rostos para um subespaço de baixa dimensionalidade e que possa aumentar a separabilidade das classes presentes. (ZHAO; CHELLAPPA; KRISHNASWAMY, 1998).

Os Métodos baseados em Kernels são uma generalização dos métodos de análise de componentes (PCA, ICA, LDA). Nos métodos de componentes, é construído um subespaço que cumpre determinadas restrições e a partir disso se escolhe uma base que irá gerar de alguma maneira particular (componentes de maior potência, melhor discriminação, etc.). Os métodos de Kernels tem capacidade para trabalhar com mais dados sem ter um custo computacional muito expressivo, pois, buscam levar o problema de classificação para um espaço de dimensão maior onde as classes possam ser linearmente separadas. (YANF M-H, 2001).

Evolutionary Pursuit (EP) é um método, que de forma similar ao PCA, ICA e lDA se baseia na análise de componentes. O EP propõe uma nova maneira de obtenção de uma base de vetores eficientes para a representação das imagens de rostos. Para encontrar a base, é realizada uma busca de maneira a maximizar uma função fitness que mede ao mesmo tempo a precisão da classificação e a habilidade de generalização do sistema. Como o problema para buscar uma base ótima é um problema de alta dimensão se utiliza para este modelo Algoritmos Genéticos (GA) ao qual são chamados de Evolutionary Pursuit. Esta técnica pode ter mais

vantagens que a PCA sempre e quando o treinamento das imagens seja feito de forma balanceada. (LIU; WECHSLER, 2000).

E finalmente o **Support Vector Machine (SVM)** é uma ferramenta genérica para resolver problemas de reconhecimento de padrões e foi proposta na década de 1990 por Cortes e Vapnik. Dado um conjunto de pontos em um determinado espaço que pertencem a duas classes distintas, o SVM encontra o hiperplano que separa a maior quantidade de pontos da mesma classe do mesmo lado. (CORTES; VAPNIK, 1995).

3.7.2. Métodos Baseados em Características Locais

Os métodos baseados em características locais podem ser do tipo: Active Appearance Model (AAM), Modelagem 3D, Elastic Bunch Graph Matching (EBGM), Modelos Escondidos de Markov (HMM) e Local Binary Patterns (LBP).

Active Appearance Model (AAM) é um modelo estatístico da forma e da aparência em níveis de cinza do objeto de interesse. Pode ser gerada a qualquer tempo. Ajustar o modelo de uma imagem implica em encontrar os parâmetros do modelo para minimizar a diferença entre a imagem e uma síntese do modelo projetado na imagem. (COOTES; WALKER; TAYLOR, 2000).

A ideia central da **modelagem 3D** é de uma técnica para construir um modelo genérico 3D para cada imagem que se deseja analisar. Existem diversas técnicas de aquisição de imagens (ou de reconstrução) 3D, entre elas: câmeras, escâneres, SLS (Structure Light System), sequências de imagens 2D, etc. BLANZ V., VETTER T., (2003).

Elastic bunch graph matching (EBGM): os algoritmos baseados no treinamento com sua exatidão dependem exclusivamente do cenário de treinamento. O algoritmo da EBGM é selecionado graças a robustez da informação na rotação do plano e pela habilidade de classificar rostos demarcando zonas importantes do rosto. Dentro destas zonas distintivas são tomadas mais de 80 características que permitem localizar as semelhanças notáveis e as diferenças das imagens de treinamento. (WISKOTT et al, 1999)Estas zonas estão compostas pelas seis regiões mais predominantes de rosto humano as quais são agrupadas em:

- Duas seções para os olhos.

- Duas seções para as sobrancelhas.
- Uma seção para as fossas nasais.
- Uma seção para a região que rodeia a boca.

O **Modelo Escondido de Markov (HMM)** trata-se de um conjunto de modelos estatísticos utilizados para caracterizar as propriedades estatísticas de um sinal. Estes modelos são de grande utilidade para a representação de dependências estatísticas em problemas que tem uma temporalidade inerente. Este modelo tem alcançado sucesso em aplicações como o reconhecimento de voz e de gestos. (NEFIAN A., 1999).

E finalmente o **Local Binary Patterns (LBP**) que é uma ferramenta interessante como descritor de textura. Este operador recorre a imagem e ao label dos pixels da mesma, estabelecendo uma vizinhança de 3X3 em relação ao valor do pixel no qual se encontra, considerando o resultado como um número binário. Assim o histograma dos labels pode ser utilizado como um descritor de textura. (AHONEN; HADID; PIETIKÄINEN, 2004).

4. Uso do Reconhecimento Facial na Segurança Pública

Embora algumas pesquisas científicas relacionadas ao reconhecimento facial tenham iniciado por volta da década de 1960, um fato relevante, o “ataque de 11 de setembro” nos EUA, alavancou a indústria e a sociedade acadêmica na construção, busca e aprimoramento de sistemas de segurança que utilizassem o reconhecimento facial.

Segundo Almeida (2009) são muitas as áreas de aplicação do reconhecimento facial, dentre elas: ações contra o terrorismo, no controle parlamentar, no controle da circulação, na busca de crianças desaparecidas em meio a multidões, na segurança residencial, na verificação da identidade dos eleitores, nas atividades bancárias, entre outros. Porém é na Segurança Pública que sua implantação é mais requerida.

É preciso salientar que o reconhecimento facial não é algo novo nos órgãos de segurança pública, o que esta surgindo com os novos programas é a automatização do processo. Uma vez que, o processo de reconhecimento facial é análogo ao reconhecimento por fotografia ou mesmo o retrato falado, onde autores ou suspeitos de cometimento de crime têm suas características confrontadas com um banco de dados pré-existente nos órgãos de segurança pública.

Neste sentido, Grue relata que o reconhecimento facial já existia há algum tempo na forma de identificação por foto, que é razoavelmente confiável em nossa sociedade. Até hoje, o processador que decide se uma pessoa é igual a uma foto tem sido o cérebro humano e nunca um computador. No entanto, os computadores introduzidos neste tipo de identificação não servem simplesmente para substituir o raciocínio humano, mas ampliaram a possibilidade de buscas. Já não é mais possível comparar uma pessoa à sua própria identidade, mas com o reconhecimento facial em um computador você pode comparar uma pessoa a um banco de dados de imagens armazenadas, permitindo-lhe identificar uma pessoa que nunca foi vista antes ou procurar por milhares de pessoas simultaneamente e encontrar pelo menos uma delas.

Conforme Azevedo e Faria (2014) as fotos publicadas nas redes sociais, tipo *Facebook e similares,* podem revelar muito sobre uma pessoa, e afirmam que *softwares* de reconhecimento facial, aliados aos imensos bancos de imagens das

redes sociais, podem não só revelar o nome de um usuário, mas informar ainda o endereço, telefone e profissão, colaborando e muito com as forças de segurança pública no combate preventivo da criminalidade.

Diversos centros universitários de pesquisas dedicadas a ciências criminalísticas (Caulkins JP. Mathematical model of drug policy, 1993.) e departamentos policiais mais avançados encontram-se, presentemente, utilizando sistemas de inteligência que empregam redes neurais, hólons e sistemas dinâmicos como modelos de apoio à investigação. Além da biometria, utilizam também características comportamentais para pesquisas científicas em bases criminais e extração de possíveis candidatos que atendam a descritivos específicos registrados em boletins de ocorrências.

4.1. No Exterior

Na área de segurança pública nos EUA, foram implementados alguns monitoramentos utilizando sistemas de reconhecimento facial, porém até o momento não mostraram resultados satisfatórios, ou que levassem a impedir um ataque terrorista, o qual foi a principal causa de sua utilização pelas forças de segurança americana. Mesmo assim, os produtos de reconhecimento facial estão começando a surgir nos aplicativos da vida real e vêm chamando especialmente a atenção da população dos EUA desde a crescente ameaça do terrorismo.

Em 2001, a cidade de Tampa, na Flórida, monitorou cada um dos freqüentadores do Super Bowl usando o “FaceIt”, o aplicativo de reconhecimento facial mais proeminente no mercado, criado pela Visionics Corporation. No entanto, nenhum suspeito foi identificado apesar de um público de 71.000 pessoas (Woodward). Além de Tampa, algumas outras cidades e alguns aeroportos, inclusive o Logan, em Boston, instalaram um software de reconhecimento facial que até hoje tem sido ineficaz na identificação de qualquer suspeito criminal (Bray).

A principal causa da aparente ineficiência dos sistemas esta ligado ao fato que necessariamente existe a necessidade de um banco de dados para confrontar todos os rostos capturados pelo sistema. Um exemplo prático da afirmação anterior é o fato que dos 19 (dezenove) terroristas envolvidos nos ataques de 11 de setembro, apenas 02 (dois) eram conhecidos do sistema de segurança americano,

sendo que apenas 01 (um) possuía fotografia. Evidentemente, poderia o sistema estar em funcionamento naquele dia e não impediria os ataques, pois existe a necessidade de um banco de dados. O sistema por si só não classifica as pessoas em boas ou más, existe a necessidade da informação ser compilada.

Entretanto, a colocação dos sistemas em funcionamento estimulou uma enorme discussão relativa à confiança nos sistemas de reconhecimento facial e se eles interferem ou não na liberdade individual, já que o reconhecimento facial pode ser utilizado de forma passiva ao contrário de muitas outras técnicas de identificação biométrica. Mesmo utilizando um discurso de maior segurança e de um país mais protegido na era do terrorismo, e a recente transição do reconhecimento facial do laboratório para a realidade, ainda necessita de limitações em sua utilização.

Embora exista o argumento que a tecnologia esta em constante aperfeiçoamento, e seu fim seja a identificação precisa de indivíduos que representem ser ameaças a coletividade, a verdade é que tem se despendido muito tempo e recursos para tentar resolver as mazelas da proteção e segurança para o qual o sistema de reconhecimento facial foi idealizado, e não se tem mostrado eficaz, resultando em críticas severas a invasão da privacidade que produz.

O governo está interessado na tecnologia para combater o crime em geral e no mundo, após 11 de setembro, porque o público está se perguntando por que o governo falhou em evitar o ataque. Por essa razão, o governo está se virando para procurar uma solução tecnológica para um problema sério, um problema que não pode ser completamente corrigido através do monitoramento de toda a população americana com sistemas de reconhecimento facial. Não obstante, a DARPA iniciou seu programa de financiamento Identificação Humana à Distância (Human ID at Distance), que propiciou uma verba para a Visionics, entre outras empresas, para continuar suas pesquisas (Woodward). A DARPA está procurando uma tecnologia que consiga identificar pessoas em multidões e em grandes extensões. Eles acreditam que essa tecnologia lhes permitiria identificar melhor os suspeitos em áreas fora do solo americano e dentro dos EUA.

De acordo com a ABDI (2010) o FBI opera atualmente sobre tecnologia de reconhecimento de impressão digital e está em processo de adoção de um sistema de nova geração incluindo outras tecnologias biométricas. A iniciativa mostra uma tendência à utilização de diversas tecnologias biométricas em conjunto

para manutenção de registros de identidade pessoal. Uma aplicação direta de uma base de dados com múltiplas informações é a possibilidade de busca de pessoas a partir de seus registros por diversos meios diferentes, como reconhecimento facial em fotografias e reconhecimento por meio de câmeras de vídeo

4.2. No Brasil

Em nosso País, no ano de 2002 foi desenvolvido de forma experimental um sistema de retrato falado, chamado “fotocrim”, utilizando como base o banco de dados de fotos digitais do sistema de Segurança Pública do Rio de Janeiro, com capacidade de inclusão de características das etnias que formam a população brasileira.

Azevedo e Faria (2014) afirma que o objetivo de um retrato falado é auxiliar uma investigação policial, diminuindo o número de suspeitos e apresentando um rosto com características semelhantes às do indivíduo procurado. A parte principal de um retrato falado é o rosto.

Desta forma, o reconhecimento facial, somado as demais tecnologias já empregadas no dia-a-dia policial, é de suma importância para o aprimoramento das técnicas investigativas, e contribuíra para o aumento de efetividade na resolução de crimes, principalmente no elemento tempo.

Ainda não encontramos registros no Brasil, de integrações entre softwares de produção de retrato-falado e banco de dados criminais. A falta desta interligação, deste elo, entre a composição de um retrato falado e a base de dados comparativa, tem diminuído a efetividade da investigação policial.

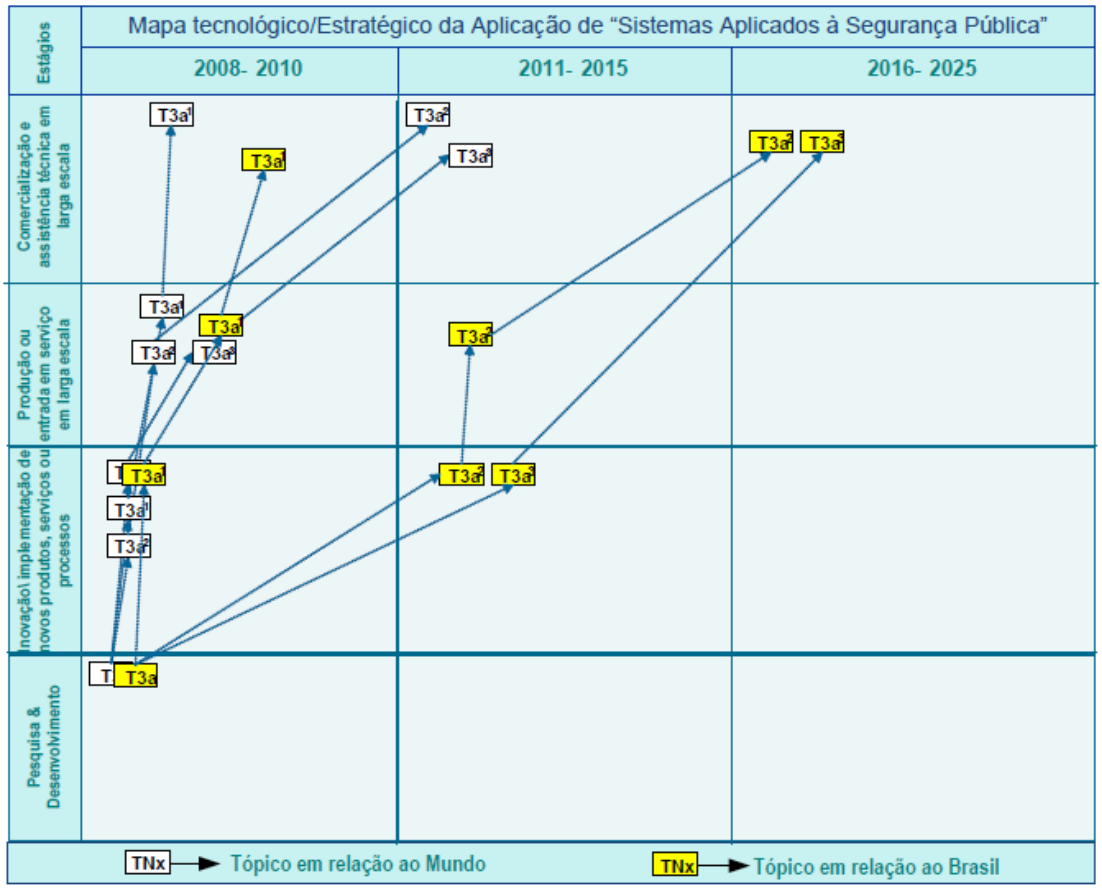
A ABDI (2010) em virtude da variedade de tecnologias classifica os sistemas biométricos em três grupos: Sistemas de Impressão Digital (**T3a1**), Sistemas de Identificação de Íris, DNA e Face (**T3a2**) e Sistemas de Reconhecimento de Voz (**T3a3**). Os dois primeiros baseados em características fisiológicas do ser humano e o último em características comportamentais.

Não existe um consenso quanto à tecnologia biométrica mais adequada para cada tipo de aplicação, mas existem aplicações que só são viáveis com determinada tecnologia. A identificação por impressão digital ainda é a preferida para a maioria das aplicações por ser mais simples e madura e também pela

tradição de uso anterior às tecnologias digitais, principalmente pela polícia. Além disso, é a única tecnologia que permite identificação posterior de pessoas por meio da coleta da impressão digital deixada em objetos. Mas as tecnologias de reconhecimento de voz e face também abrem possibilidades para outras aplicações além da identificação para autenticação da pessoa, que somente elas podem viabilizar.

Segundo a ABDI (2010) o reconhecimento facial possibilita a busca de pessoas desaparecidas ou procuradas a partir de fotografias ou combinando a tecnologia de reconhecimento de face com reconhecimento de padrões em vídeo, sem que a pessoa seja chamada para identificação.

Figura 22: Mapa Comparativo para Biometria



Fonte: ABDI (2010)

Notação: T3a – Biometria; T3a1 – Biometria: impressão digital; T3a2 – Biometria: íris, DNA e face; T3a3 – Biometria: voz.

Segundo a ABDI (2010) e analisando a figura 22, a tecnologia de reconhecimento de impressões digitais (**T3a1**), por estar em um estágio mais

avançado de desenvolvimento, já está saindo da fase de pesquisa e desenvolvimento para ser incorporada a diversos projetos experimentais, devendo atingir as fases de inovação, produção, comercialização e assistência técnica em larga escala ainda no período 2008-2010. As tecnologias de reconhecimento de íris, face e DNA (**T3a2**) e as tecnologias de reconhecimento de voz (**T3a3**), ainda estão em amadurecimento, devendo sair da fase de pesquisa e desenvolvimento e atingir as fases de inovação e produção em larga escala ainda no período 2011-2015. A comercialização e assistência técnica em larga escala devem ocorrer somente no período 2016-2025.

O Brasil encontra-se equiparado ao cenário mundial na utilização de tecnologias de reconhecimento de impressão digital (**T3a1**), embora não como gerador de novas tecnologias e inovações, mas como seguidor na utilização das tecnologias de reconhecimento de íris, face e DNA (**T3a2**) e voz e (**T3a3**).

A utilização de tecnologias de reconhecimento de impressão digital no Brasil está difundida em aplicações de controle de acesso físico, acesso a sistemas de informação e algumas aplicações experimentais. Entre elas estão a Universidade Estadual de Campinas (Unicamp), que utilizou um sistema de reconhecimento de impressões digitais no vestibular, o DETRAN da Bahia, que instituiu um sistema de controle de freqüência em curso de formação de condutores e o Tribunal Superior Eleitoral (TSE), que testou urnas com reconhecimento de impressão digital nas últimas eleições.

O uso das tecnologias de reconhecimento de íris, face e DNA (**T3a2**) e voz (**T3a3**) ainda são incipientes. Um projeto experimental no setor financeiro foi conduzido pelo Unibanco, que realizou um projeto com reconhecimento de íris em caixas eletrônicos. Essas tecnologias devem completar a fase de pesquisa e desenvolvimento no período 2008-2010 e atingir a fase de inovação e produção em larga escala somente no período 2011-2015. A comercialização e assistência técnica em larga escala devem viabilizar-se somente no período 2016-2025. Iniciativas de pesquisa são pontuais e descoordenadas no país.

Além dos *softwares* especializados que a indústria nacional tem condições de produzir, um projeto de envergadura já em andamento, é o projeto de passaportes, que pretende combinar tecnologias RFID, criptográficas e biométricas, como reconhecimento de impressões digitais e o reconhecimento facial. Outro

projeto que pode convergir para a utilização de identificação biométrica é o Registro de Identificação Civil (RIC). Além disso, depois de implantados os projetos que coletam e registram as informações, expande-se o potencial de desenvolvimento de aplicações em segurança pública que utilizarão essas bases de informação.

Existem algumas organizações atuantes em pesquisas biométricas no Brasil, entre elas a Cognitec Brasil é a representante oficial da Cognitec Systems da Alemanha, empresa líder mundial em soluções de biometria de reconhecimento facial.

5. Conclusões e considerações finais

Observando ao nosso redor seguramente encontra-se uma grande quantidade de sistemas biométricos. A necessidade de aumentar a segurança nos diferentes ambientes nos quais o ser humano interage, convertendo a biometria em uma tecnologia de uso cotidiano. A biometria na área de informática é encontrada em muitas aplicações de uso diário, por exemplo, em transações bancárias ou em outros ambientes tão complexos como a identificação de civis por parte de entidades governamentais.

A necessidade de melhorar a segurança tanto de pessoas quanto de bens pode ser beneficiada através do uso da biometria informática, permitindo capturar informações características únicas nas pessoas de forma automatizada, comparando-a posteriormente com dados armazenados em alguma base de dados e fornecendo um parecer confiável sobre a semelhança da amostras analisadas.

Conforme foi apresentado neste trabalho monográfico existe muitas técnicas utilizadas na biometria. Porém na hora de implementar um sistema biométrico algumas técnicas são mais aceitas pelas pessoas, que outras, e isso se deve principalmente ao nível intrusivo que cada técnica biométrica apresenta. Estes normalmente são apontadas em quatro categorias: aquelas que não tem nenhuma interação direta como o usuários; as que apresentam pouca interação; as que requerem alta interação e aquelas que requerem interação muito alta com os usuários, por exemplo, contato físico.

Outro fator que interfere significativamente na decisão sobre qual técnica biométrica pode ser implementada em cada cenário está relacionado, é o ambiente que o rodeia. Ambientes repletos de pessoas são mais difíceis de serem controlados e vigiados, a fim de, manter um nível ótimo de segurança, enquanto que em ambientes controlados onde o tráfego de pessoas é menor, torna-se mais simples e favorável implementar determinadas técnicas.

Ao estudar as diferentes técnicas de reconhecimento biométrico foi possível observar que uma das técnicas que combina, a maior aceitação por parte dos usuários, a confiabilidade na análise e a possibilidade de ser implementada eficazmente em ambientes repletos de pessoas e em ambientes controlados, é o reconhecimento de pessoas por meio do uso de padrões faciais.

Aprofundando mais esta técnica foi possível observar que existe uma grande quantidade de técnicas baseadas no reconhecimento de padrões faciais.

Dado que existe uma ampla variedade o documento se ateve àquelas mais utilizadas no campo da biometria. Os sistemas apresentados em sua maioria trabalham somente com uma técnica na hora de extrair a informação das imagens. Entre as técnicas mais comuns e mais utilizadas estão a PCA e a LDA. Uma conclusão após a realização deste trabalho é que estes tipos de técnicas permitem um melhor desempenho quando trabalham em conjunto, brindando maior eficácia e rapidez na hora de extrair informações.

É possível observar que há muitas áreas de aplicação do reconhecimento facial, porém na área da Segurança Pública, o qual sua implantação é mais requerida e necessária, ainda é pouco empregada. No exterior foram implementados alguns monitoramentos utilizando o sistema de reconhecimento facial, porém não mostraram resultados muito satisfatórios. No Brasil existem poucas referências de aplicação do uso da biometria facial no ambiente da Segurança Pública. Este sistema encontra-se ainda em pesquisa, desenvolvimento e inovações, tendo uma previsão de implantação para 2016-2025. Desta forma, observa-se a aplicação do reconhecimento facial basicamente na iniciativa privada.

Considerando a pesquisa realizada, a utilização da biometria facial na Segurança Pública, em especial no meio investigativo-policial, colaboraria para uma maior resolução de crimes, visto que permitiria ampliar o campo de pesquisa na busca de suspeitos e foragidos da justiça.

Como recomendação fica a proposta de combinar diferentes técnicas na hora de desenvolver algum tipo de sistema biométrico, pois, desta maneira se aproveitaria as diferentes funcionalidades que nos brindam estas técnicas na hora de identificar ou reconhecer uma pessoa.

Recomenda-se também o estudo sobre o uso da biometria por policiais, por meio de dispositivos móveis e como estes podem auxiliar e facilitar a atividade policial; Pesquisa sobre os motivos pelos quais a biometria não alavancou no Brasil; e realizar um estudo de caso sobre o uso do reconhecimento facial nos aeroportos nacional e internacional.

Referências

ABDI. 2010. **Cadernos Temáticos - Tecnologias de Informação e Comunicação - TIC - Serviços Convergentes de Telecomunicações**. Agência Brasileira de Desenvolvimento Industrial. [Online] 2010. Disponível em: < http://www.abdi.com.br/Estudo/Caderno%20Tem%C3%A1tico%20TIC%20-%201%20(Vers%C3%A3o%20Final)%20-%20Servi%C3%A7os%20Convergentes%20de%20Telecomunica%C3%A7%C3%B5es.pdf >. Acesso em: 01 dez. 2014.

AHONEN T., HADID A., PIETIKÄINEN M., (2004). **"Face recognition with local binary patterns".** In Proceedings of the 8th European Conference on Computer Vision, ECCV '04, pages 469–481, Prague, Czech Republic, May 11-14 2004.

ALMEIDA, Alcides Ferreira. **Sistemas e Tecnologias de Informação para Serviços Policiais: O Caso da Polícia Nacional de Cabo Verde. 2009.** Disponível em: <http://bdigital.unipiaget.cv:8080/jspui/bitstream/10964/145/1/sistemas%20e%20tecnologias%20de%20informa%C3%A7ao.pdf >. Acesso em: 01 dez. 2014.

ALSTAIR H. CUMMINGS, M. NIXON, J.N. (2010). **"A Novel Ray Analogy for Enrolment of Ear Biometrics".** 978-1-4244-7581-0 IEEE.

ANDRADE, Maria Margarida de. **Introdução à metodologia do trabalho científico:** elaboração de trabalhos na graduação. 6. ed. São Paulo: Atlas, 2003.

BARROS, Aidil Jesus da Silveira. LEHFELD, Neide Aparecida de Souza. **Fundamentos de metodologia científica.** 2 ed. São Paulo: Pearson Makron Books, 2000.

BERTILLON A. (2009). **"Color of the iris"**. Revue Scientifique, France, IEEE.

BLANZ V., VETTER T., (2003). **"Face recognition based on fitting a 3D morphable model'**. IEEE Transactions on Pattern Analysis and Machine Intelligence, 25(9):1063–1074, 2003.

COOTES F., WALKER K., TAYLOR C. J. (2000). **"View-based active appearance models'.** In Proceedings of the 4th IEEE International Conference on Automatic Face and Gesture Recognition, FG '00, pages 227–232, Grenoble, France, 2000.

CORTES C., VAPNIK V., (1995). **“Support-vector networks”.** Machine Learning, 20(3):273–297, 1995.

DURKHEIM E. (1987). **As Regras do método sociológico.** 3ª ed.. Lisboa: Editorial Presença.

GOLDSTEIN A. J., HARMON L. D., LESK A. B. (1971). **“Identification of human faces”.** Proceedings of the IEEE, 59(5):748–760.

GRUE, ANTONHY RONALD**. Reconhecimento Facial: Aplicação Restrita à Proteção e Segurança.** Disponível em:< http://mit.universia.com.br/STS/STS035/PDF/anthony_final.pdf >. Acesso em: 10 dez. 2014.

GRUPO ATENEA. (2015). **“Biometría informe tecnológico sectorial”.** Disponível em: http://www.ateneadigital.es/revistaatenea/revista/PDF/Documentos/Documento_650.pdf

HAVRAN C., HUPET L., CZYZ J., LEE J., VANDENDORPE L, VERLEYSEN M. (2002). **“Independent component analysis for face authentication”.** In Proceedings of the 6th International Conference on Knowledge-Based Intelligent Information and Engineering Systems, KES ’02, September 2002.

HJELMAS E., LOW B.K. (2001). **“Face detection: A survey”.** Computer Vision and Image Understanding”. 83(3):236–274.
http://www.cienciaeingenieria.com/2013/09/la-gran-tendencia-reconocimiento-facial.html 27-09-2013. http://bibdigital.epn.edu.ec/bitstream/15000/5504/1/T2481.pdf 17-07-2013
HYVÄRIBNEN A. (2000). **“Independent Component Analysis: Algorithms and Applications”.** Neural Networks, 13(4-5): 411-430

JOLLIFFE I.T. (2002), **“Principal Component Analysis”.** 2nd de. Springer Series in Statistics. HYVÄRIBNEN A. (2000). “Independent Component Analysis: Algorithms and Applications”. Neural Networks, 13(4-5): 411-430

LI S.Z. JAIN A.K. (2005). **“Handbook of Face Recognition”.** Springer.

LI S.Z. JAIN A.K. (2009). **“Encyclopedia of Biometrics”.** Springer.

LIU C., WECHSLER H., (2000). **“Evolutionary pursuit and its application to face recognition”.** IEEE Transactions on Pattern Analysis and Machine Intelligence, 22(6):570–582, 2000.

MARTINS, Isnard. **Pesquisa em bases fotográficas, a partir do retrato falado – uma solução para integração através da antropometria de Bertillon.** Disponível em: < http://www.citynet.com.br/retratofalado/Artigo2.htm >. Acesso em: 06 dez. 2014.

NEFIAN A., (1999). **“A hidden Markov model-based approach for face detection and recognition”.** PhD thesis, Georgia Institute of Technology, Atlanta, GA, 1999.
O'DONELL G. (1977). Apuntes para una teoría del Estado. Buenos Aires: Cedes (Documento Cedes, 9, 49p.).

SAEED K., NAGASHIMA T. (2012). **Biometrics and Kansei Engineering**, New York: Springer.

SCHEIDAT T., ENGEL A., VIELHAUSER C. (2006). **“Parameter optimization for biometric fingerprint recognition using genetic algorithms, Advanced Multimedia and Security Lab”.** Magdeburg, Germany. ACM 1-59593-493-6/06/0009.
SHASHIKUMAR D. R, RAJA K.B, CHHOTRAY K. (2010). **“Biometric security system base on signature verification using neural networks”.** 978-1-4244-5965-0 IEEE.

SUCAR L.H. (2010). **“Visión Computacional”.** Instituto Nacional de Astrofísica, Óptica y Electrónica, Puebla, México.

TURK M. PENTALANDA. (1991). **“Eigenfaces for Recognition”.** Jounal of Cognitive Neurosicence, Vol. 3, No. 1, pp. 71-86.

UNAM, Facultad de Ingeniera. **Clasificación de los sistemas biométricos**. Disponível em: http://redysegurança.fip. unam.mx/proyectos/biometria/clasificacionsistemas/capturaretina.html. Acesso em: 15 fev. 2015.

WISKOTT L., FELLOUS J-M., KRÜGER N., MALSBURG C. (1999). **“Face recognition by elastic bunch graph matching”.** In L. C. Jain, U. Halici, I. Hayashi, and S. B. Lee, editors, Intelligent Biometric Techniques in Fingerprint and Face Recognition, chapter 11, pages 355–396. CRC Press, 1999.

YANF M-H. (2001). **“Face recognition using kernel methods”.** In Thomas G. Dietterich, Suzanna Becker, and Zoubin Ghahramani, editors, Proceedings of the Neural Information Processing Systems Conference, NIPS’01, volume 14, pages 1457–1464, Vancouver, British Columbia, Canada, December 3-8 2001. MIT Press.

YANG M-H., KRIEGMAN J. AHUJA N. (2002). **“Detecting faces in images: A survey.** IEEE Transactions on Pattern Analysis and Machine Intelligence, 24(1):34–58, January.

ZHAO W, CHELLAPPA R, KRISHNASWAMY A. (1998). **“Discriminant analysis of principal components for face recognition”.** In Proceedings of the 3rd International Conference on Automatic Face and Gesture Recognition, FG ’98, pages 336–341, Nara, Japan, April 14-16 1998.