CAPÍTULO 8

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

Fernanda Todesco Nunes
Juarez Bento da Silva
Priscila Cadorin Nicolete
Josiel Pereira
Marta Adriana da Silva Cristiano

1 INTRODUÇÃO

Muito se fala a respeito dos possíveis benefícios das TIC na área de Segurança Pública, assim como da eficiência e da transparência que estas podem aportar à Administração Pública e ao governo em todos os níveis e áreas. Sem dúvida que, para falar sobre a 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" ou "receitas universais".

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. Aqui, densidade refere-se à capacidade de relacionamentos pessoais de uma maneira mais complexa, em que as ações de uma pessoa repercutem direta ou indiretamente em uma maior quantidade de indivíduos, criando relações de interdependência mais dinâmicas. Também está ligada à capacidade de

relacionamentos com maior número de pessoas, no mesmo sentido que levantou Durkheim (1987) quando falou sobre "densidade dinâmica". Essa maior densidade gera novos desafios aos estados, pois a maneira de relacionar-se com e entre seus cidadãos modifica-se 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.

Devido à importância e ao valor que podem obter alguns dos recursos físicos e informáticos (dados) utilizados em diferentes áreas da sociedade, torna-se necessária a criação de mecanismos de proteção, tanto de acesso como de integridade desses recursos. Por exemplo, são empregados processos para restringir o acesso somente a determinadas pessoas. Esses processos buscam utilizar mecanismos altamente confiáveis e seguros.

Diante do aumento da criminalidade, todos os setores da sociedade têm discutido soluções para minimizar os prejuízos sofridos. Visualiza-se mais investimentos por parte das pessoas e das empresas em tecnologias de segurança, 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 vídeomonitoramento instalados nas áreas urbanas (RIBEIRO, 2013).

Diante disso, a identificação de pessoas a partir do emprego de 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. O desenvolvimento de tecnologias de reconhecimento facial, em conjunto com os sistemas de vídeomonitoramentos já existentes, poderá ser uma ferramenta eficaz no combate à criminalidade, principalmente na localização e na identificação de foragidos, criminosos, desaparecidos etc.

Entretanto, a pouca informação disponível a respeito de sistemas de reconhecimento facial tem dificultado e limitado a possibilidade de sua implantação de maneira massiva (PEREZ; AGUDELO, 2012), bem como o desenvolvimento de projetos que utilizam esse tipo de alternativa nos sistemas de segurança privada ou pública. O que se encontra são projetos que buscam a aplicação do reconhecimento facial para reforçar a segurança orgânica e patrimonial das instalações em geral privadas, que produzem conhecimento ou guardam informações de segurança institucional.

Nesse sentido, seria possível, então, reunir técnicas que permitam conhecer e desenvolver um sistema de segurança baseado na biometria estática por meio de padrões faciais para identificação de rostos humanos nos órgãos de Segurança Pública, e aplicá-los na resolução de crimes de forma massiva?

Desse modo, este estudo pretendeu relacionar as diferentes técnicas existentes para o tratamento de imagens e que permitam a identificação ou reconhecimento de padrões faciais em seres humanos. Para isso, o estudo apresenta um breve panorama sobre a utilização das TIC por parte do Estado, suas possíveis aplicações na área de Segurança Pública, seus entraves e soluções, e os desafios que o Estado enfrenta para acompanhar a evolução tecnológica, bem como discutir a utilização das tecnologias de reconhecimento biométrico, em especial o reconhecimento facial.

2 SISTEMAS BIOMÉTRICOS

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

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

A biometria tem origem no idioma grego – *bio* (vida) e *metron* (medida) – e refere-se a todas aquelas técnicas que permitem identificar e autenticar as pessoas por meio de suas características fisiológicas e de comportamento (GUGLINSKI, 2013). A biometria foi utilizada pela primeira vez na China, em meados do século XIV, 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 baseava-se apenas na "memória fotográfica", até que Alphonse Bertillon, chefe do departamento fotográfico da Polícia de Paris, desenvolveu o sistema antropométrico, em 1883. Esse foi o primeiro sistema preciso, amplamente utilizado cientificamente para identificação criminal e que converteu a biometria em um campo de estudo. Funcionava medindo, de forma precisa, certos comprimentos e larguras da cabeça e do corpo, assim como registrava marcas individuais como tatuagens e cicatrizes (MAERSA, 2010).

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). Posteriormente, foi colocada em prática a impressão digital como método de reconhecimento por parte das autoridades policiais (LI; JAIN, 2009), muito parecido com o sistema utilizado pelos chineses há muitos anos. Atualmente, a biometria não está somente centrada na identificação por meio da impressão digital, mas 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).

3 RECONHECIMENTO FACIAL

O conceito de identificação ou reconhecimento facial automatizado 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" (TRASLAVIÑA, 2015).

Nos anos 1970, Goldstein, Harmon e Lesk (2013) usaram 21 características físicas específicas, 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 (1991), utilizando a técnica de *eigenfaces*, nome que recebeu o método descoberto por Kirby e Sirovich, demonstraram que "o erro residual podia ser utilizado para detectar rostos nas imagens, uma descoberta que permitiu desenvolver sistemas de reconhecimento confiáveis em tempo real".

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 da NFL (Liga Nacional de Futebol Americano), pois naquela ocasião o processo consistiu na captura de imagens por meio das câmeras de vigilância para depois serem

contrastadas e identificadas com uma base de dados que armazenavam imagens digitalizadas de delinquentes. (SUCAR, 2010; MACEDO, 2013).

A partir 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, por exemplo, a tecnologia de reconhecimento facial vem sendo muito utilizada para evitar fraudes de identificação, realizar buscas por pessoas desaparecidas, controle de acesso de funcionários em empresas entre outras aplicações. (DE PAULO; PEREIRA, 2015; MONTIBELER; FERNANDES, 2012). Nos últimos anos, foram realizados estudos mais detalhados devido à necessidade de encontrar meios para reconhecer as pessoas a partir de seus traços característicos, sendo o campo da segurança o que tem exigido os maiores avanços (VALLEJO; NEIRA, 2005).

Nesse sentido, o reconhecimento facial é a capacidade de identificar as pessoas por suas características faciais. É uma tecnologia mais avançada e baseada em algoritmos. Por exemplo. o Eigenfaces 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. (LI; JAIN, 2009; TURK; PENTALAND, 1991).

Em geral, um sistema automático de verificação facial é composto de duas etapas principais: detecção de rosto e verificação do rosto. 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 (OLIVEIRA, 2006). 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 que a região do rosto tenha sido localizada perfeitamente. Portanto, o rendimento desse sistema depende significativamente da precisão da etapa da detecção facial (OMAIA, 2009).

Uma fator importante para sistemas de detecção de rostos é a capacidade para separar o rosto do restante da imagem. Para isso, o sistema faz o reconhecimentos dos pontos altos, pontos baixo e contornos presentes no rosto, e trata esses nós para medir (Figura 8.1) e comparar com aqueles armazenados no sistema de banco de dados (BORJA; BUENO, [20??]).

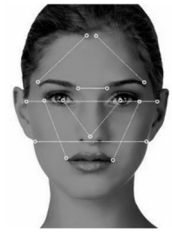

Figura 8.1 Pontos-chave da estrutura de tecidos rígidos do rosto.
Fonte: https://www.dsi.uclm.es/personal/MiguelFGraciani/mikicurri/Docencia/Bioinformatica/web_BIO/Documentacion/Trabajos/Biometria/Trabajo%20Biometria.pdf.

Entretanto, algumas dificuldades são encontradas na detecção de rostos. O algoritmo não somente deve detectar o rosto para a identificação ou verificação de pessoas, como também deve levar em conta outros aspectos que poderiam dificultar o processo de detecção do rosto (OTEGUI et al., 2006), como:

- estado de ânimo da pessoa/reconhecimento de expressões (triste, alegre, enojado etc.);
- localização de características relevantes: olhos, boca, sobrancelhas, queixo, orelhas etc.;
- tamanho do rosto;
- presença de lentes, barba, gorros etc.;
- expressão do rosto;
- problemas de iluminação;
- condições da imagem;
- quantidade desconhecida de rostos na imagem (OTEGUI et al., 2006 ; GOLDSTEIN; HARMON; LESK, 1971).

3.1 Métodos de reconhecimento de rostos

O reconhecimento de rostos tem sido estudado por várias disciplinas, como a Psicologia, assim como se estuda o reconhecimento de padrões e redes neurais, as quais dividem o reconhecimento de rostos duas abordagens para extração de características das imagens da face: "Abordagem global – Aparência da face" e "Abordagem local – geometria da face" (COSTA; OBELHEIRO; FRAGA, 2006; OTEGUI et al., 2006).

Na abordagem global, a ideia básica é reduzir uma imagem de milhares de pixels para um conjunto de número (COSTA; OBELHEIRO; FRAGA, 2006). A vantagem dessa abordagem é que as características podem ser identificadas independentemente dos "ruídos" que uma imagem pode ter, como luminosidade, textura da pele, reflexos etc. (COSTA; OBELHEIRO; FRAGA, 2006). Os métodos

para tratamento utilizando essa abordagem é chamado de Métodos Holísticos (COSTA; OBELHEIRO; FRAGA, 2006; OTEGUI et al., 2006).

Já na abordagem local são extraídas as características locais do rosto (olhos, nariz, boca, sobrancelhas etc.) a partir da sua localização geométrica, ou seja, suas posições, que formam a entrada do sistema de reconhecimento (OTEGUI et al.; 2006). Dessa forma, o reconhecimento de face é feito a partir da comparação dos sistemas geométricos obtidos (COSTA; OBELHEIRO; FRAGA, 2006). Para a utilização dessa abordagem, são empregados Métodos Estruturais (COSTA; OBELHEIRO; FRAGA, 2006), também denominados Métodos Baseados em Características Locais (OTEGUI et al., 2006).

Ainda pode-se explorar uma abordagem híbrida, que combina os dois métodos anteriores. Para Costa, Obelheiro e Fraga (2006), os métodos híbridos oferecem o melhor dos dois métodos.

Cada método possui técnicas para o reconhecimento de rostos. Essas técnicas determinam as características a serem extraídas das imagens e as possíveis medidas de similaridade para a etapa de comparação (COSTA; OBELHEIRO; FRAGA, 2006). A Figura 8.2 mostra a classificação de alguns dos métodos de reconhecimento de rostos.

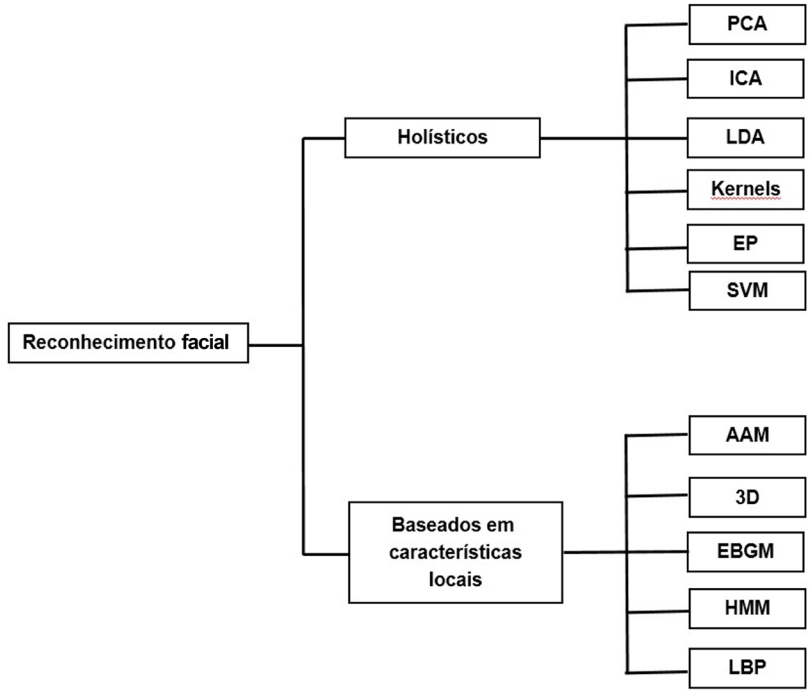

Figura 8.2 Classificação de alguns métodos de reconhecimento de rostos.

A seguir será apresentando de modo geral os métodos e algumas técnicas utilizadas no reconhecimento de rostos.

3.2 Métodos holísticos

Os métodos holísticos são classificados em: Análise de Componentes (PCA, ICA e IDA) e métodos baseados em *Kernels*, *Evolutionary Pursuit* (EP) e *Support Vector Machine* (SVM).

Nos métodos de componentes, é construído um subespaço que cumpre determinadas restrições e, a partir disso, escolhe-se uma base que gerará de alguma maneira particular componentes de maior potência, melhor discriminação etc. (OTEGUI et al., 2006). Os métodos de Análise de Componentes podem ser: Análise de Componentes Principais (PCA), Análise de Componentes Independentes (ICA) e Análise de Discriminante Linear (LDA).

O PCA considera a distribuição de imagens de um rosto e tenta capturar variabilidade destas, 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. Esses vetores gerados são chamados de *Eigenfaces*. (TURK; PENTALAND, 1991). Já os métodos baseados em ICA tentam 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 et al., 2002). E o algoritmo LDA 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).

Existem também os métodos baseados em *Kernels*, que são uma generalização dos métodos de análise de componentes (PCA, ICA, LDA). Esses métodos têm a capacidade de trabalhar com mais dados sem ter um custo computacional muito expressivo, pois buscam levar o problema de classificação para um espaço de dimensão maior, no qual as classes possam ser linearmente separadas (YANF, 2001).

Já os métodos denominados *Evolutionary Pursuit* (EP), de forma similar ao PCA, ICA e lDA, baseiam-se 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 para maximizar uma função *fitness*, que mede ao mesmo tempo a precisão da classificação e a habilidade de generalização do sistema. Como a busca por uma base ótima é um problema de alta dimensão, utiliza-se para o modelo Algoritmos Genéticos (GA), que são chamados de *Evolutionary Pursuit*. Essa técnica pode ter mais vantagens

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

Por fim, 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).

3.3 Métodos estruturais

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).

O *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).

Já na modelagem 3D, a ideia central é a construção um modelo genérico tridimensional para cada imagem que se deseja analisar. Existem diversas técnicas de aquisição de imagens (ou de reconstrução) 3D, entre elas: câmeras, escâneres, *Structure Light System* (SLS), sequências de imagens 2D etc. (BLANZ; VETTER, 2003).

Os algoritmos baseados em *Elastic Bunch Graph Matching* (EBGM) visam extrair uma representação do rosto em forma de grafo e o reconhecimento se realiza comparando os grafos correspondentes a diferentes imagens (OTEGUI et al., 2006). Esse algoritmo é selecionado graças a robustez da informação na rotação do plano e pela habilidade de classificar rostos demarcando zonas importantes do rosto. Dentro dessas 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). Essas zonas estão compostas pelas seis regiões mais predominantes de rosto humano, são agrupadas em: duas seções para os olhos, duas seções para as sobrancelhas, uma seção para as fossas nasais e uma seção para a região que rodeia a boca.

Outro método baseado em características locais é o Modelo Escondido de Markov (HMM), que é um conjunto de modelos estatísticos utilizados para caracterizar as propriedades estatísticas de um sinal. Esses modelos são de grande utilidade para a representação de dependências estatísticas em problemas que tem uma temporalidade inerente. Esse modelo tem alcançado sucesso em aplicações como o reconhecimento de voz e de gestos (NEFIAN, 1999).

Por fim, o *Local Binary Patterns* (LBP) é uma ferramenta interessante como descritor de textura. Esse operador recorre à imagem e ao *label* dos pixels da mesma, estabelecendo uma vizinhança de 3 x 3 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 APLICAÇÕES

A técnica de identificação e reconhecimento facial adquire um novo uso em entidades governamentais, satisfazendo suas necessidades. Atualmente, pode-se ver o grande impacto que essa tecnologia tem conseguido, sendo utilizada em locais em que se deseja levar um controle de acesso e lugares em que seja requerida identificação plena de todas as pessoas, como aeroportos e terminais de transporte. A tecnologia pode, inclusive, ajudar em atividades tão importantes como encontrar pessoas desaparecidas ou em fraudes cometidas muitas vezes ao suplantar a identificação de outra pessoa (DE PAULO RESENDE; PEREIRA, 2015; OMAIA, 2009). A Tabela 8.1 apresenta algumas áreas e aplicações específicas com reconhecimento facial.

Tabela 8.1 Aplicações com reconhecimento facial

Área	Aplicações específicas
Biometria	Carteiras de habilitação, Imigração, passaportes, registro eleitoral, fraude, telefones inteligentes, acesso às 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.
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 às instalações, acesso aos veículos.

A seguir será tratada a utilização de reconhecimento facial especificamente na segurança pública.

5 USO DO RECONHECIMENTO FACIAL NA SEGURANÇA PÚBLICA

Embora as pesquisas científicas relacionadas ao reconhecimento facial tenham iniciado por volta da década de 1960, um fato relevante, o ataque terrorista de 11 de setembro nos Estados Unidos, alavancou a indústria e a sociedade acadêmica na construção, busca e aprimoramento de sistemas de segurança que utilizem o reconhecimento facial (TUCKER, 2014).

Segundo Almeida (2009), são muitas as áreas de aplicação do reconhecimento facial, como: ações contra o terrorismo, no controle parlamentar, no controle da circulação, na busca por 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 está 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, em que 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 (2003) relata que o reconhecimento facial já existia há tempos sob a 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 ampliar 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 podem revelar muito sobre uma pessoa, e afirmam que softwares de reconhecimento facial, aliados aos imensos bancos de imagens dessas redes, 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.

5.1 No exterior

Na área de segurança pública nos Estados Unidos, 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, que 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 norte-americana desde a crescente ameaça do terrorismo.

Na cidade de Tampa, na Flórida, em 2001, foi feito o monitoramento de cada frequentador do Super Bowl a partir do uso de um popular aplicativo de reconhecimento facial, o *FaceIt*, criado pela Visionics Corporation. Entretanto, conforme Grue (2013), nenhum suspeito foi identificado, apesar do público de 71.000 pessoas. Além de Tampa, algumas outras cidades e aeroportos instalaram softwares de reconhecimento facial que se apresentaram ineficazes na identificação de qualquer suspeito criminal até hoje.

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

Entretanto, a colocação em funcionamento dos sistemas 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 focado no aumento da segurança e de um país mais protegido na era do terrorismo, a recente transição do reconhecimento facial do laboratório para a realidade ainda necessita de limitações em sua utilização.

Embora exista o argumento de que a tecnologia está em constante aperfeiçoamento e seu fim seja a identificação precisa de indivíduos que representem ser ameaças à coletividade, a verdade é que tem se despendido muito tempo e recursos para tentar resolver as mazelas da proteção e da 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 vem procurando uma solução tecnológica para um problema sério, que não pode ser completamente corrigido por meio do monitoramento de toda a população americana com sistemas de reconhecimento facial. Não obstante, a Agência de Projetos de

Pesquisa Avançada de Defesa (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. A DARPA está procurando uma tecnologia que consiga identificar pessoas em multidões e em grandes extensões. Eles acreditam que essa tecnologia lhes permitiria identificar mais adequadamente os suspeitos em áreas dentro e fora do solo americano.

De acordo com a ABDI (2010), o FBI opera atualmente sob a 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.

5.2 No Brasil

Em nosso país, em 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) afirmam 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 às demais tecnologias já empregadas no dia a dia policial, é de suma importância para o aprimoramento das técnicas investigativas, e contriburia para o aumento de efetividade na resolução de crimes, principalmente no elemento tempo. Entretanto, não há registros no Brasil de integrações entre softwares de produção de retrato falado e banco de dados criminais. A falta desta interligação, 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 são 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 de-

terminada 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.

Conforme a ABDI (2010) 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 (Figura 8.3).

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 (T3a3).

A utilização de tecnologias de reconhecimento de impressão digital 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 frequência 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.

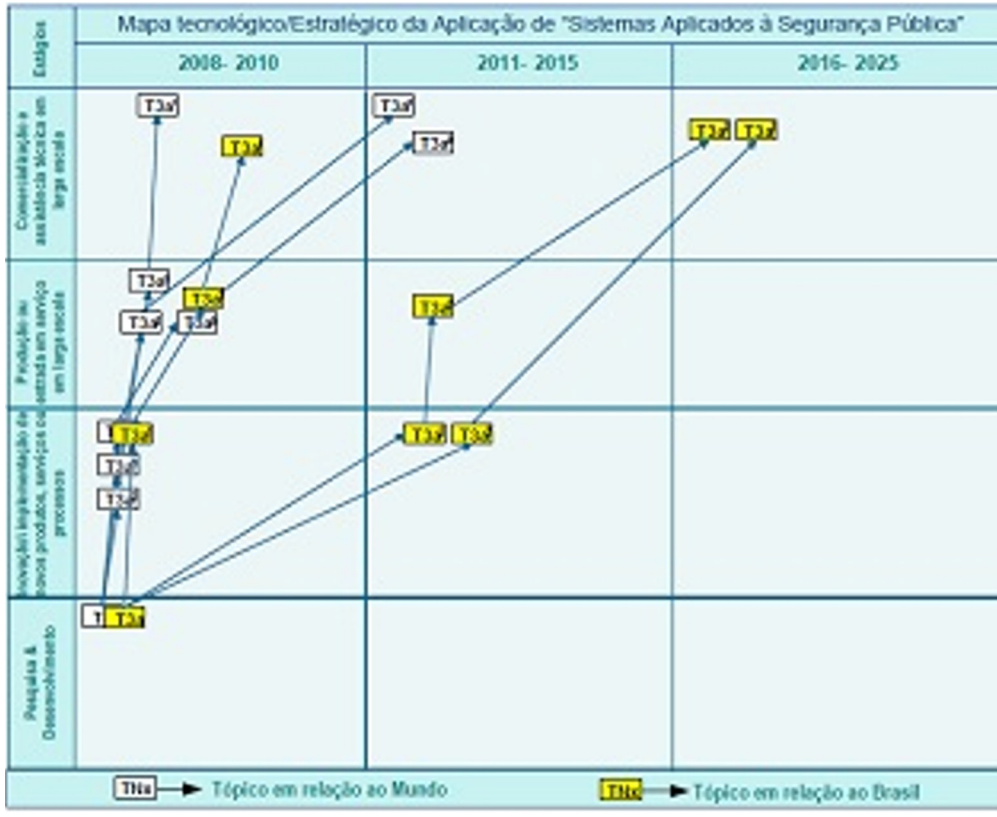

Figura 8.3 Mapa comparativo para biometria.

Fonte: ABDI (2010).

A comercialização e a 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, representante oficial da Cognitec Systems da Alemanha, empresa líder mundial em soluções de biometria de reconhecimento facial.

6 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, como 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 por meio do uso da biometria informática, permitindo capturar informações e 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 estudo, existem muitas técnicas utilizadas na biometria. Porém, na hora de implementar um sistema biométrico, algumas técnicas são mais aceitas pelas pessoas do que outras, e isso se deve principalmente ao nível intrusivo que cada técnica biométrica apresentada. Elas normalmente são apontadas em quatro categorias: as que não têm nenhuma interação direta como os 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 relacionada ao 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, no qual 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 maior aceitação por parte dos usuários, confiabilidade na análise e 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-se mais nesta 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 ateve-se 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

melhor desempenho quando trabalham em conjunto, conferindo mais 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, em que 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 sobre o uso da biometria facial no ambiente da Segurança Pública. Esse 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 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, aproveitar-se-ia 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 realização de estudo de caso sobre o uso do reconhecimento facial nos aeroportos nacional e internacional.

REFERÊNCIAS

AGÊNCIA BRASILEIRA DE DESENVOLVIMENTO INDUSTRIAL – ABDI. **Cadernos Temáticos – Tecnologias de Informação e Comunicação – TIC.** Serviços Convergentes de Telecomunicações. 2010. Disponível em: <http://j.mp/1TfKKri>. Acesso em: 1 dez. 2014.

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

ALMEIDA, A. F. **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: 1 dez. 2014.

AZEVEDO, M. G. D.; FARIA, R. A. D. Retrato falado: a eveolução do método indiciário para reconhecimento facial. In: BRAZILIAN CONGRESS ON BIOMEDICAL ENGINEERING, 24., 2014, Uberlândia. **Proceedings**... Curitiba: UTFPR, 2014. Disponível em: <http://www.canal6.com.br/cbeb/2014/artigos/cbeb2014_submission_757.pdf>. Acesso em: 20 jun. 2016.

BERTILLON, A. Color of the iris. **Revue Scientifique**. France: IEEE, 2009.

BLANZ, V.; VETTER, T. Face recognition based on fitting a 3D morphable model. **IEEE Transactions on Pattern Analysis and Machine Intelligence**, v. 25, n. 9, p. 1063-1074, 2003.

BORJA, C. T.; BUENO, A. G. **Sistemas biométricos**. [S.l.: s.n.], [20??]. Disponível em: <https://www.dsi.uclm.es/personal/MiguelFGraciani/mikicurri/Docencia/Bioinformatica/web_BIO/Documentacion/Trabajos/Biometria/Trabajo Biometria.pdf>. Acesso em: 2 jun. 2016.

CAULKINS, J. P. **Mathematical model of drug policy**. Pittsburgh: Repository Carnegie Mellon University, 1993.

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

CORTES C.; VAPNIK V. Support-vector networks. **Machine Learning**, v. 20, n. 3, p. 273-297, 1995.

COSTA, L. R.; OBELHEIRO, R. R.; FRAGA, J. S. Introdução à biometria. **Minicursos do VI Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais (SBSeg2006)**. Porto Alegre, v. 1, p. 103-151, 2006.

DE PAULO, C. A. R.; PEREIRA, M. H. R. Visão computacional aplicada em reconhecimento facial na busca por pessoas desaparecidas. **e-xacta**, v. 8, n. 2, 2015.

DURKHEIM, E. **As regras do método sociológico**. 3. ed. Lisboa: Editorial Presença, 1987.

GOLDSTEIN A. J.; HARMON L. D.; LESK A. B. Identification of human faces. **Proceedings of the IEEE**, v. 59, n. 5, p. 748-760, 1971.

GRUE, A. R. **Reconhecimento facial:** aplicação restrita à proteção e segurança. 2003. Disponível em: <http://mit.universia.com.br/STS/STS035/PDF/anthony_final.pdf>. Acesso em: 10 dez. 2015.

GUGLINSKI, V. **Leitura sequencial de impressões digitais:** diminuição de fraudes em sistemas biométricos. Teresina: Instituto Brasileiro de Direito da Informática, 2013.

HAVRAN, C.; HUPET, L.; CZYZ, J.; LEE, J.; VANDENDORPE, L.; VERLEYSEN, M. Independent component analysis for face authentication. **Proceedings of the 6th International Conference on Knowledge-Based Intelligent Information and Engineering Systems**, KES '02, Sep. 2002.

JAIN, A. K.; ROSS, A. A.; NANDAKUMAR, K. **Introduction to Biometrics**. New York: Springer, 2011.

LI, S. Z.; JAIN, A. K. **Encyclopedia of Biometrics**. New York: Springer, 2009.

LIU, C.; WECHSLER, H. Evolutionary pursuit and its application to face recognition. **IEEE Transactions on Pattern Analysis and Machine Intelligence**, v. 22, n. 6, p. 570-582, 2000.

MACEDO, R. **La gran tendencia:** reconocimiento facial. 2013. Disponível em: <http://www.cienciaeingenieria.com/2013/09/la-gran-tendencia-reconocimiento-facial.html>. Acesso em: 24 fev. 2016.

MAERSA. **Historia de la Biometría y la Huella Digital**. México, 2010. Disponível em: <http://www.maersa.com.mx/historia.html>. Acesso em: 22 fev. 2016.

MONTIBELER, D. C. G. C.; FERNANDES, J. C. L. **Controle de acesso através dos sistemas biométricos como ferramenta de combate a fraudes**. Faculdade de Tecnologia de São Caetano do Sul. São Caetano do Sul, 2012.

NEFIAN, A. A hidden Markov model-based approach for face detection and recognition. **PhD Thesis**, Atlanta, Georgia Institute of Technology, 1999.

OLIVEIRA, D. R. **Reconhecimento de Faces Usando Redes Neurais e Biometria**. São José dos Campos: Instituto Nacional de Pesquisas Espaciais, 2006.

OMAIA, D. **Um sistema para detecção e reconhecimento de face em vídeo utilizando a transformada cosseno discreta**. Departamento de Informática. Universidade Federal da Paraíba. João Pessoa, 2009.

OTEGUI, C. A. et al. **Proyecto Aguará – Reconocimiento de Caras**. Montevideo: Facultad de Ingeniería Universidad de la República, 2006.

PEREZ, N. L.; AGUDELO, J. J. T. **Tecnicas de biometria basadas en patrones faciales del ser**. 2012. Disponível em: <http://repositorio.utp.edu.co/dspace/bitstream/11059/2738/1/0053682L864.pdf>. Acesso em: 3 mar. 2016.

RIBEIRO, L. Governo financiará videomonitoramento em fronteiras. **O Estado de S.Paulo.** 14 maio 2013. Disponível em: <http://politica.estadao.com.br/noticias/geral,governo-financiara-videomonitoramento-em-fronteiras,1031668>. Acesso em: 1 mar. 2016.

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

SUCAR, L. H. **Visión Computacional**. Puebla, México: Instituto Nacional de Astrofísica, Óptica y Electrónica, 2010.

TRASLAVIÑA, C. M. G. **Introducción a la biometría**. 2007. Disponível em: <http://www.academia.edu/9374109/Introduccion_a_la_biometría>. Acesso em: 24 fev. 2016.

TUCKER, J. How facial recognition technology came to be The FBI's astonishing new identification system is the product of 175 years of innovation – and paranoia. A visual history. **Boston Globe**. 2014. Disponível em: <https://www.bostonglobe.com/ideas/2014/11/23/facial-recognition-technology-goes-way-back/CkWaxzozvFcveQ7kvdLHGI/story.html>. Acesso em: 1 mar. 2016.

TURK, M.; PENTALEND. Eigenfaces for recognition. **Jounal of Cognitive Neurosicence**, v.3, n.1, p. 71-86, 1991.

VALLEJO, J. A. S.; NEIRA, J. C. S. **Diseño e implementación de un sistema de seguridad basado en reconocimiento de rostros**. 2005. Disponível em: <http://bibdigital.epn.edu.ec/bitstream/15000/5504/1/T2481.pdf>. Acesso em: 24 fev. 2016.

WISKOTT, L.; FELLOUS. J. M.; KRÜGER, N.; MALSBURG, C. Face recognition by elastic bunch graph matching. In: JAIN, L. C.; HALICI, U.; HAYASHI, I.; LEE, S. B. (ed.). **Intelligent Biometric Techniques in Fingerprint and Face Recognition**, chapter 11, p 355-396. CRC Press, 1999.

YANF, M. H. Face recognition using kernel methods. In: DIETTERICH, T. G.; BECKER, S.; GHAHRAMANI, Z. (ed.) **Proceedings of the Neural Information Processing Systems Conference**, NIPS'01. Vancouver, Canada: MIT Press, v.14, p. 1457-1464, Dec. 3-8, 2001.

ZHAO, W.; CHELLAPPA, R.; KRISHNASWAMY, A. Discriminant analysis of principal components for face recognition. **Proceedings of the 3rd International Conference on Automatic Face and Gesture Recognition**, FG '98. Nara, Japan: April 14-16, 1998, p. 336-341.