ADEMAR DE SOUZA REIS JUNIOR

MILTON SOARES FILHO

APLICAÇÕES DE PROCESSAMENTO DE IMAGENS A SISTEMAS DE SEGURANÇA

Trabalho apresentado à disciplina de Tópicos em Processamento de Imagens do curso de Ciência da Computação, Setor de Ciências Exatas, Universidade Federal do Paraná.

Profa. Dra. Olga Regina Pereira Bellon

CURITIBA

Agosto de 2002

SUMÁRIO

Abstract

In this paper we present an overview of biometric technologies applied for security systems that make use of image processing techniques. We discuss the utilization of technologies for authentication, detection and forensics fields, as long as the implications of such use. This includes face, iris, retina and fingerprint recognition along with movement detection and objects tracking. We conclude that the use of image processing technologies gives a great improvement for the security area and is a promissing subject for research and development.

Resumo

Neste artigo apresentamos uma visão geral das tecnologias biométricas aplicadas em sistemas de segurança que fazem uso de técnicas de processamento de imagens. Discutimos a utilização dessas tecnologias nas áreas de autenticação, detecção e investigação forense, tanto quanto as implicações de seus usos. Isto inclui reconhecimento de faces, íris, retinas e impressões digitais além de técnicas para detecção de movimento e *tracking* de objetos. Por fim concluímos dizendo que o uso de tecnologias de processamento de imagens acrescenta muitos avanços na área de segurança e é um assunto promissor quanto a pesquisas e desenvolvimentos futuros.

.

1. INTRODUÇÃO

É comum, em instituições de qualquer porte, estabelecerem-se restrições de acesso a locais e equipamentos de valor para as mesmas. Não somente evitando-se acesso de pessoal externo, mas, muitas vezes, limitando-se também o acesso do pessoal da própria instituição de acordo com seu nível de hierarquia ou funcionalidade desenvolvida.

Como tal controle pode ser feito? Uma solução rápida seria colocar uma pessoa que conheça todos os funcionários habilitados em cada área a ser protegida, de modo que a verificação fosse feita visualmente.

Qual o problema deste tipo de solução? Basta imaginar uma empresa onde o número de funcionários é consideravelmente grande. Fica difícil confiar somente na suposta boa memória do responsável pela verificação.

Sistemas de segurança são desenvolvidos para se automatizar o processo de verificação de acesso ou ajudar em outras tarefas relativas à proteção de patrimônios críticos. Quando usados para autenticação, consistem de uma base de dados contendo informações sobre o nível de acesso dos funcionários e um esquema para garantir a identificação do mesmo.

Atualmente, muitos sistemas usam cartões de identificação contendo desde um simples código de barras até micro-chips com circuitos inteligentes (smart-cards) ou simples senhas ao se apresentarem aos esquemas de segurança.

É claro que a situação mostrada não é a melhor, pois nenhum destes instrumentos é uma característica inerente à pessoa que o utiliza. Cartões podem ser

usados por outras pessoas interessadas em obter recursos ilícitos e senhas, além de serem facilmente esquecidas, podem ser adivinhadas ou obtidas sem muito esforço.

Felizmente, com o avanço das técnicas de processamento de imagem e um certo barateamento dos equipamentos que complementam as soluções que utilizam estas técnicas, muitas novas tecnologias estão surgindo para ajudar as instituições a melhor zelarem pelos seus bens.

A vantagem evidente da utilização de tais técnicas é o fato de que elas se baseiam em características inerentes à pessoa avaliada por ela. Apesar de não ser impossível, uma impressão digital, por exemplo, é muito mais difícil de ser reproduzida do que um cartão com código de barras.

Apesar de existirem muitas áreas onde estas técnicas possam ser aplicadas, pode-se classificá-las em duas vertentes: aplicações de autenticação e de vigilância. A diferença entre ambas está no ponto de vista do elemento a ser avaliado.

Enquanto que num sistema de autenticação o próprio usuário se apresenta para declarar sua legitimidade, sistemas de vigilância monitoram constantemente um local em busca de eventos que caracterizem presença indevida ou outros tipos de violação às regras de acesso.

Antes de eliminar completamente a necessidade de sistemas alternativos, as técnicas de processamento de imagens aplicadas a sistemas de segurança vêm agregando uma maior precisão e qualidade aos sistemas já existentes. Ainda há algum trabalho a ser feito no caminho da evolução destas técnicas.

Neste trabalho, discorremos genericamente sobre aplicações de técnicas de processamento de imagens em sistemas de segurança e comentamos algumas abordagens apresentadas em artigos do assunto, dando ênfase às tecnologias de biometria reunidas ao processamento de imagens, especialmente quando empregadas na autenticação.

O propósito deste documento é fornecer ao leitor um nível de conhecimento básico sobre o assunto em questão e fornecer referências para um estudo mais

aprofundado através da apresentação dos principais temas relacionados e links sobre os mesmos.

No capítulo seguinte, modelos de autenticação são discutidos, apresentando as principais tecnologias, seu funcionamento e estado de desenvolvimento atual. A base teórica deste capítulo servirá para o terceiro, que discorre sobre outras aplicações além da autenticação de usuários.

Na seção de conclusão, comenta-se o trabalho apresentado e futuros desenvolvimentos relacionados a esta área.

2. AUTENTICAÇÃO

O problema de identificar usuários é antigo e continua sendo amplamente estudado uma vez que as tecnologias para correta autenticação assim como meios de circunvenções e falsificações não deixam de evoluir.

O mais comum e amplamente utilizado meio de autenticação é através do uso de senhas (passwords), onde o usuário escolhe uma combinação de caracteres que o identificam. Seja em uma transação comercial ou uma simples identificação frente a uma base de dados, a senha é como se fosse uma "assinatura" ou uma "chave secreta" e como tal sua confiabilidade reside no segredo da senha.

O principal problema com a autenticação através de senhas é que usuários tendem a escolher senhas fáceis e se confundir com o número excessivo de senhas necessárias atualmente. Nessa era digital, onde a autenticação é necessária para todo tipo de transação, a escolha de senhas diferentes e complexas torna-se uma tarefa extremamente difícil para um usuário comum[1,2].

Esses problemas e a evolução de tecnologias de biometria têm levado à adoção de técnicas de reconhecimento de características físicas do ser humano para autenticação, como voz, íris, retina, impressão digital, face, etc. A identificação e autenticação de usuários através destas tecnologias se mostram mais eficiente do que a tradicional (com o uso de senhas) uma vez que a individualidade de fatores biológicos é muito maior e mais difícil de se falsificar. Em sistemas onde o grau de confiabilidade deve ser muito alto, as possibilidades de falsificação podem ser reduzidas a praticamente zero através da combinação de diversas das técnicas de autenticação.

Exemplos de uso de técnicas de biometria através do processamento de imagens atualmente variam desde simples máquinas de ponto e acesso até dispositivos de autenticação on-line que substituem por completo a necessidade de utilização de senhas.

A seguir fazemos uma breve análise de quatro grandes frentes de autenticação de usuários através de processamento de imagens: reconhecimento de impressões digitais, íris, retina e face.

2.1. Reconhecimento de Impressões Digitais (“Finger Scan”)

O reconhecimento de impressões digitais tem sido utilizado principalmente por órgãos de investigação, sendo que as técnicas foram desenvolvidas ainda nos anos 60. O processo de verificação era manual e exigia grande perícia por parte do investigador. A evolução na capacidade de processamento e memória dos computadores e a crescente demanda por softwares que fizessem o reconhecimento de impressões digitais de maneira automática levou órgãos como FBI e NSA a investirem grandes somas de dinheiro em pesquisa de técnicas que permitissem tal tarefa.

Atualmente o reconhecimento de impressões digitais está relacionado tanto à investigação forense como a autenticação em tempo real, sendo que a primeira utiliza-se dos softwares chamados AFIS ("Automated Fingerprint Identification Systems") que fazem uso de grandes bases de dados e imagens completas das impressões digitais para identificação posterior baseada na imagem capturada geralmente em cenas de crimes.

Para autenticação as técnicas utilizadas são mais leves e conhecidas como "Finger Scan", onde, ao invés de comparação de imagens completas, faz-se um reconhecimento de padrões e gera-se um modelo a partir de detalhes da imagem original. Em tais técnicas, não é possível recuperar a impressão digital original a partir do banco de dados, mas pode-se fazer uma pesquisa rápida em bases relativamente

grandes (comumente com mais de 100.000 usuários) em poucos segundos. As técnicas utilizadas devem levar em conta a necessidade de precisão, possibilidades de erro esperadas e requisitos de desempenho [3].

São três as principais tecnologias utilizadas na captura de imagens de impressões digitais:

a) Ótica

É o mais antigo e usado dos métodos, uma vez que o hardware é barato e qualidade bastante aceitável. Seus principais problemas residem no tamanho do dispositivo e na possibilidade de resíduos deixados por outros usuários interferirem na captura de novas impressões.

b) Chips de Silício

O dispositivo consiste num chip de silício que utiliza sinais elétricos para a formação da imagem, que, em geral, tem uma melhor definição do que a capturada por dispositivos óticos. Por ser um dispositivo pequeno (não mais do que 1cm x 1.5cm), é o meio mais utilizado em pequenos dispositivos como celulares e laptops. Por ser uma tecnologia ainda nova, sua durabilidade é contestada e seu preço ainda é considerado alto.

c) Ultra-som

Talvez a mais precisa das tecnologias de captura de impressões digitais, o método de ultra-som é capaz de gerar imagens de alta definição mesmo em condições adversas como presença de resíduos e sujeira, uma vez que a imagem é formada baseada em cálculos de distância levando em consideração a impedância da pele, do ar e do próprio equipamento. Não é muito utilizado por ser uma tecnologia cara e nova, mas testes evidenciam que a técnica é bastante promissora.

Sistemas de identificação através de impressão digital já vêm sendo utilizados por vários tipos de equipamento, variando desde telefones celulares[1] que identificam seu usuário até soluções de software e hardware para autenticação on-line[2].

2.2. Reconhecimento da Íris

Os algoritmos de reconhecimento de Íris são extremamente eficientes na identificação pessoal de usuários. Patenteados pelo Dr. John Daugman[4], poderiam ser utilizados para reconhecer uma única pessoa em um banco de dados que contivesse toda a população do mundo com margens de erro ínfimas.

Todas as técnicas se baseiam em características visíveis da íris. Com um tamanho de cerca de 11mm, a íris é capaz de prover cerca de 266 pontos únicos de identificação. Como pode ser visto na figura 1, a principal característica da íris é o tecido que aparenta dividir a íris radialmente.

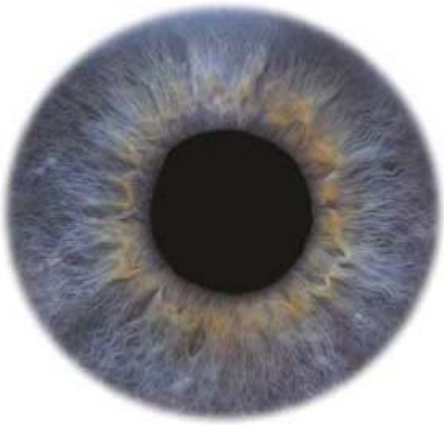

Figura 1: Imagem da íris humana, onde é possível notar suas características visíveis.

[1] Celular com reconhecimento de usuário: http://w4.siemens.de/newsline.d/pressfor/end99101.htm

[2] Software e Hardware para autenticação online: http://www.bioweb.com.br/default_portugues.htm

A captura da imagem é feita a partir de uma câmera que se utiliza tanto de luz visível como infravermelha a distâncias de até 1 metro da face do usuário. A posição do olho é detectada a íris encontrada baseando-se num padrão de modelo de rosto. Os algoritmos mostram-se funcionais mesmo que apenas 1/3 da íris possa ser capturada e tratada, situação que é normal dada a abertura do olho e ângulo de inclinação do rosto/câmera.

É feito um reconhecimento de padrões na imagem, utilizando os dados coletados então. Uma vez que são armazenadas apenas informações e nunca a imagem em si, o processo de reconhecimento e identificação é bastante rápido, podendo ser utilizado em aplicações de autenticação em tempo real.

2.3. Reconhecimento de Retina

O reconhecimento de retina, assim como o de íris, se mostra extremamente eficiente no sentido de identificar com precisão e individualidade uma pessoa. É, porém, um método bastante intrusivo, uma vez que a captura da imagem precisa ser feita próxima ao olho para que se consiga uma boa definição.

Como pode ser visto na figura 2, a retina é o nervo localizado ao fundo do globo ocular. Podemos dizer que a retina é, para o olho humano, o que é um filme para uma câmera fotográfica. Analisando seu aspecto, pesquisadores supuseram já em 1930 que os padrões dos vasos sanguíneos eram particulares a cada indivíduo e que poderiam ser utilizados como identificadores de uma pessoa. É no reconhecimento desses padrões que se baseia o processo de identificação através do reconhecimento de retina.

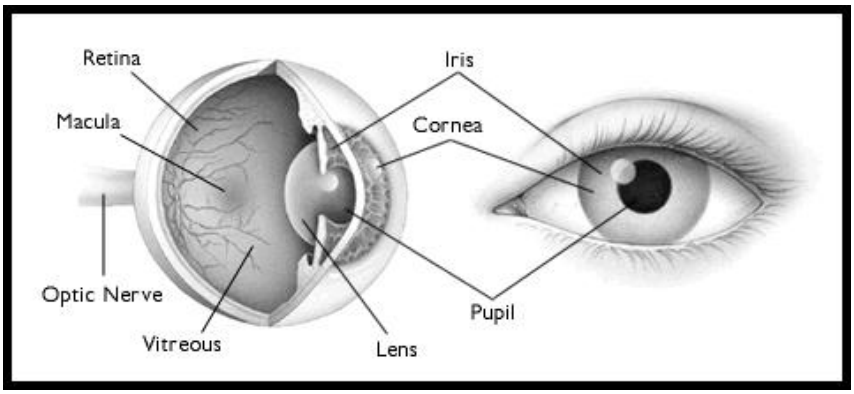

Figura 2: anatomia do olho humano

O reconhecimento de retina não é tão utilizado como o da íris por dificuldades de viabilidade, uma vez que, como já dito, a captura da imagem precisa ser feita a uma pequena distância. Dispositivos atuais ficam a cerca de 1/2 polegada da córnea, o que causa um certo desconforto e apreensão nos usuários, que relutam em expor um órgão sensível como o olho humano.

Embora de pouca utilização, técnicas de identificação podem ser utilizadas em sistemas onde seja grande a relevância por uma identificação precisa e sem erros, uma vez que tais sistemas podem optar pelo uso de várias tecnologias simultaneamente.

2.4. Reconhecimento Facial

O problema de detecção e reconhecimento facial tem vários níveis de aplicação e dificuldade. Por ser um órgão 3D e socialmente alterável, a face está suscetível a uma variedade de modificações por parte da pessoa (idade, posição, estado emocional, etc) e do ambiente (iluminação, cores do ambiente, etc).

O reconhecimento facial depara-se com dois grandes desafios: que são encontrar a face na imagem[5,6] e encontrar características nessa face[6], gerando um modelo para armazenamento e comparação.

Os sistemas de identificação geralmente fazem uso de um conjunto de imagens em um determinado intervalo de tempo. Isso facilita a procura de características e da face em si, uma vez que diferentes ângulos e expressões podem mais facilmente distinguir a face e seus detalhes do restante do ambiente. A partir dessas informações, cria-se um modelo que é então utilizado para a comparação de padrões com a face a ser autenticada ou reconhecida.

Sistemas de autenticação facial são relativamente fáceis de implementar uma vez que a correspondência seja um-para-um (o usuário precisa confirmar que é uma determinada pessoa, previamente cadastrada no sistema) e tanto o ambiente como o usuário cooperem. O grande desafio para o reconhecimento facial consiste em sistemas onde o reconhecimento se dê em ambientes comuns do dia-a-dia. Tais sistemas são discutidos no próximo capítulo.

Existem várias implementações comerciais que podem ser utilizadas em computadores pessoais equipado com uma câmera de vídeo. Alguns dos disponíveis para download (versão demo ou livre) estão listados abaixo:

a) SQIS (System for Quick Image Search)

http://www.tip.csiro.au/Services/SmartSensing/FaceRecognition1.htm

b) FaceMail 1.45

http://www.biometrics.ws/

c) ID-2000

http://www.imagistechnologies.com/Product/Products.htm

3. OUTRAS APLICAÇÕES

Nem somente para autenticação são feitos os sistemas de segurança.Outros exemplos de utilização são sistemas de vigilância, onde o reconhecimento e detecção de movimentos aparecem como subespecializações e serão melhor apresentados nas seções a seguir.

Um sistema de vigilância, diferente de um sistema de autenticação, é um agente que permanece ativo enquanto houver a necessidade de se avaliar o ambiente guardado por ele. Digamos que exista uma área num laboratório X onde precisamente ninguém possa permanecer. Um típico sistema de vigilância usaria os dados de uma câmera digital apontada para tal área para procurar continuamente por indícios de movimentação no ambiente, disparando algum tipo de alarme ou aviso quando os encontrasse.

Além deste tipo de aplicação, pode-se citar o reconhecimento de rostos em multidão e uma técnica chamada tracking, que habilita o sistema a seguir o deslocamento de algum elemento relevante encontrado na área de visualização.

O reconhecimento de faces é bastante utilizado em eventos de segurança máxima, onde as ferramentas de localização varrem todos os rostos encontrados procurando por rostos de criminosos conhecidos.

Um exemplo de utilização de tracking seria o ligamento e direcionamento automático de câmeras de segurança, permitindo ao operador verificar a área relevante ao acontecimento somente no momento de necessidade. Nesses casos, um sistema deste tipo é muito vantajoso, pois um operador humano tende a deixar algum detalhe

escapar, principalmente quando se é exigida atenção contínua e ininterrupta para a realização de sua tarefa.

3.1. Reconhecimento

Basicamente, o fluxo de execução de um sistema de reconhecimento pode ser descrito pelo algoritmo da figura 3.

1. Encontrar, na imagem, a característica a ser analisada;
2. Criar um modelo genérico de representação da característica;
3. Compará-lo com modelos pré-existentes em uma base de dados;
4. Avisar usuários caso a comparação tiver alto grau de equivalência;
5. Repetir os passos anteriores enquanto houver entrada;

Figura 3: Algoritmo de um sistema de reconhecimento (entrada: imagem, saída: ações externas)

Apesar do fato de sistemas de reconhecimento, em seu âmago, tratarem do casamento de padrões entre um modelo montado à partir de um elemento analisado numa imagem e um modelo previamente armazenado, assim como os sistemas de autenticação, existem muitas peculiaridades que diferem esses dois tipos.

Primeiramente, o objeto alvo de um sistema de reconhecimento não faz a mínima questão de se apresentar ao dispositivo de gravação para ser reconhecido. Na prática, não se pode esperar que o objeto alvo se enquadre em algum momento numa posição tal que suas características possam ser reconhecidas. O processo de reconhecimento deve ocorrer a todo o instante, levando em consideração todas as variações possíveis na apresentação do objeto e usando modelagens que incorporem tal preocupação[7]. As variações mais comuns são encontradas na distância do objeto

à câmera, nos deslocamentos horizontal e vertical (translações), nas rotações e iluminação.

Em segundo lugar, trata-se de um sistema vigilante, portanto, a entrada de dados não é interrompida em momento algum e nem existe muito tempo para que uma resposta seja retornada. Esta restrição exige um grande poder de processamento da máquina que roda o aplicativo de reconhecimento.

Neste caso, a tarefa mais dispendiosa computacionalmente é a de encontrar na imagem a característica a ser observada. Uma solução sugerida[5] para contornar o problema de tempo de processamento sem comprometer a eficácia da comparação é a utilização de duas técnicas complementares de processamento de imagens. Uma delas, baseada em movimento e de rápida execução, porém com precisão questionável, é utilizada para se restringir ao máximo o espaço de busca das características, enquanto que a outra técnica, baseada em modelos e lenta por lidar com estruturas complexas como grafos, é usada no espaço de busca restante para compensar a falta de precisão da técnica anterior.

Para o reconhecimento de faces à longa distância ou em meio à multidões há uma forte correlação entre capacidade de processamento e a qualidade da câmera, como visto em [8].

3.2. Detecção de Movimento

A detecção de movimento é um processo relativamente mais fácil de ser realizado do que o reconhecimento, por este motivo, sua execução é mais rápida e existem muitas implementações comerciais desta solução, inclusive por preços bem acessíveis.

Um sistema de detecção de movimento procura, numa seqüência de imagens, sinais que confirmem a existência de movimentação no ambiente monitorado, marcando os locais onde o movimento ocorreu e tomando as devidas medidas de

prevenção. Opcionalmente, este sistema pode realizar o tracking, que é a habilidade de se rastrear a movimentação do objeto detectado.

Uma peculiaridade desta categoria é a de que existe uma preocupação com um conjunto de imagens processadas e não somente com o quadro atual da imagem, diferentemente das técnicas anteriores. Em vista disso, os algoritmos que implementam esta solução são obrigados a levarem em consideração o histórico de alteração de intensidade de cada píxel tal como outros fatores. Um exemplo de técnica preocupada com tais fatores pode ser encontrada em[5] (zero crossing detection).

3.3. Contribuições em Outras Áreas

Um dos maiores objetivos dos desenvolvedores de sistemas inteligentes é permitir ao computador o reconhecimento do ambiente em que se encontra. Através desta percepção, abrir-se-ão caminhos para o desenvolvimento de sistemas interativos que ultrapassam de longe a definição de sistemas inteligentes.

A habilidade de reconhecer elementos do ambiente externo não é trivial, porém vem crescendo promissoramente no ramo de visão computacional. Na área de segurança, podemos encontrar grandes avanços neste sentido. Tais avanços vêm angariando cada vez mais respeito às soluções de segurança que utilizam biometria ou detecção de movimento em suas implementações.

Além de favorecer instituições com necessidades rígidas quanto ao acesso disponibilizado ao público interno e externo, ramos como a investigação policial, segurança pública e até mesmo interação homem-máquina podem aproveitar as vantagens oferecidas pelos métodos de vigilância aqui apresentados.

4. CONCLUSÃO

A utilização de biometria tem adicionado significativas melhorias a sistemas de segurança. Tanto em processos de autenticação de usuários, onde a gama de tecnologias a serem utilizadas é maior, como nos processos de detecção, tracking e investigação forense, as técnicas de processamento de imagens têm se mostrado de grande valia. Mesmo que certas tecnologias se mostrem caras e de difícil implementação, elas não podem ser desprezadas na área de segurança, uma vez que o custo pode justificar sua necessidade. A combinação de várias tecnologias pode significar uma barreira praticamente intransponível se bem implementada. Além disso, a comodidade e facilidade de utilização do sistema por parte do usuário devem ser levadas em conta já que com a crescente demanda por autenticação a atenção que este dispensa a senhas e métodos de autenticação tende a diminuir.

A utilização de técnicas de processamento de imagens tem sido utilizada em diversos projetos comerciais de sucesso. Além disso, órgãos de segurança (como FBI e NSA) têm investido grandes somas em pesquisa e desenvolvimento de tecnologias no intuito de estar sempre um passo à frente dos criminosos e usuários mal intencionados.

Ainda há muito que se pesquisar e implementar para a melhoria dos processos e métodos aqui discutidos. Diminuir as margens de erro, aumentar o desempenho e tempo de resposta e descobrir novas tecnologias são todos fatores que não podem e nunca serão desprezados em sistemas de segurança.

5. REFERÊNCIAS BIBLIOGRÁFICAS

1. Adams, A., Sasse, M.A. 1999. ***Users are not the enemy: Why users compromisse security mechanisms and how to take remedial measures***. Communications of the ACM, 42, 41-46.

2. M. A. Sasse, S.Brostoff, & D. Weirich 2001. ***Transforming the "weakest link": a human-computer interaction approach to usable and effective security***. BT Technical Journal, Vol 19 (3) July 2001, pp. 122-131

3. A. Roddy and J.D. Stosz 1997. ***Fingerprint Features: Statistical Analysis and System Performance Estimates***. Proc. IEEE, vol. 85, no. 9, Sept. 1997, pp. 1390-1397.

4. DaugmanHow, J. ***How Iris Recognition Works***. available at http://www.cl.cam.ac.uk/users/jgd1000/ on August, 2002. To be presented as a "Special Session Lecture" on the "IEEE 2002 International Conference on Image Processing", New York, September 2002.

5. McKenna, Stephen J. and Gong, Shaogang 1996. ***Tracking Faces***. Second International Conference on Automated Face and Gesture Recognition, October 1996, Killington, Vermont.

6. A.W. Senior, 1999. ***Face and Feature Finding for a Face Recognition System In proceedings of Audio- and Video-based Biometric Person Authentication '99***. pp. 154-159. March 22-24, 1999, Washington D. C. USA.

7. Laurenz Wiskott, Jean-Marc Fellous, Norbert Krüger, et al 1999. ***Face Recognition by Elastic Bunch Graph Matching***. Proc. 7th Intern. Conf. on Computer Analysis of Images and Patterns, CAIP'97, Kiel

8. P. Jonathon Phillips et al 2000. ***The FERET Evaluation Methodology for Face-Recognition Algorithms****.* IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 22, no. 10, Year 2000, pp 1090-1104.