UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL
INSTITUTO DE INFORMÁTICA
PROGRAMA DE PÓS-GRADUAÇÃO EM COMPUTAÇÃO

Autenticação de Usuários Através da Utilização de Sistemas Biométricos

por

RENATA MONTEZ DE MATOS

Dissertação submetida à avaliação, como
requisito parcial para a obtenção do grau de
Mestre em Ciência da Computação

Prof. Dr. Raul Fernando Weber
Orientador

Porto Alegre, novembro de 2000.

CIP – CATALOGAÇÃO NA PUBLICAÇÃO

Matos, Renata Montez de
Autenticação de usuários através da utilização de sistemas biométricos / por Renata Montez de Matos. – Porto Alegre: PPGC da UFRGS, 2000.
98p.: il.

Dissertação (mestrado) – Universidade Federal do Rio Grande do Sul. Programa de Pós-Graduação em Computação, Porto Alegre, BR-RS. Orientador: Weber, Raul Fernando.
1. Sistemas biométricos. 2. Autenticação de usuários. 3. Verificação de usuários. I. Weber, Raul Fernando. II. Título.

UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL
Reitora: Profa. Wrana Panizzi
Pró-Reitor de Ensino: Prof. José Carlos Ferraz Hennemann
Superintendente de Pós-Graduação: Prof. Philippe Olivier Alexandre Navaux
Diretor do Instituto de Informática: Prof. Philippe Olivier Alexandre Navaux
Coordenadora do PPGC: Profa. Carla Maria Dal Sasso Freitas
Bibliotecária-Chefe do Instituto de Informática: Beatriz Haro

Agradecimentos

Até começar a realizar este trabalho, toda vez que tinha oportunidade de ler qualquer tese ou dissertação que contivesse qualquer tipo de agradecimento a quem quer que fosse, sempre pensava que estes agradecimentos eram mera formalidade e que, no dia em que o meu trabalho estivesse concluído, e quando chegasse a minha vez de agradecer, não teria ninguém a não ser eu mesma para quem direcionar meus agradecimentos, uma vez que a conclusão do meu trabalho teria sido mérito única e exclusivamente meu.

Com o decorrer do tempo, minha opinião mudou. Aprendi que tudo que você faz, especialmente um trabalho tão solitário como uma dissertação de mestrado, pode não ter ajuda direta de alguém, mas indiretamente está sempre ligado a alguma forma de colaboração e participação de outras pessoas, e que no fim você tem vontade de agradecer até àquele desconhecido que sorriu pra você na rua em algum momento em que tudo parecia tão difícil que você tinha quase certeza que não iria conseguir. Aprendi que ninguém faz nada sozinho, mesmo que esteja se sentindo sozinho.

Estou dividindo meu mérito. O trabalho pode ser meu, mas o fato de eu ter conseguido chegar até aqui foi obra de muita gente.

Em primeiro lugar, ninguém foi mais relevante para a realização deste trabalho do que o meu orientador, Prof. Raul Fernando Weber. Seu voto de confiança me permitiu começar e seu incentivo constante fez com que este trabalho pudesse ser concluído. A consideração e apreço por seus alunos fez com que ele fosse sempre generoso nos elogios e justo nas críticas. Além de um profissional competente, um professor cuidadoso, um orientador extremamente interessado e atencioso, o prof. Weber é uma grande pessoa que respeita seus alunos. E o fato de o prof. Weber ser meu orientador foi só mais um incentivo para que eu concluísse este trabalho, pelo simples fato de que ele merecia que eu assim o fizesse.

Tenho que agradecer muito também à minha família, que me deu boa parte do suporte financeiro e a quase totalidade do suporte emocional que eu precisei para concluir este trabalho, acreditando em mim e me empurrando pra frente nos momentos mais críticos. E que, mesmo estando fisicamente longe, esteve sempre presente.

Aos meus colegas de curso, que rapidamente deixaram de ser colegas para se tornar amigos, e aos meus amigos e bichinhos gaúchos, que se tornaram minha família, e que me fizeram sentir Porto Alegre como se fosse a minha casa, mesmo eu estando tão distante da minha.

Também nem sei como agradecer às minhas abnegadas cobaias, que não se importaram em pagar mico botando peruca e fazendo careta em benefício da Ciência.

Agradeço também ao CNPQ, pela bolsa de estudos no segundo ano do curso.

E aos desconhecidos que sorriram pra mim na rua, porque isto sempre faz diferença.

Sumário

Lista de Figuras

Lista de Tabelas

Resumo

Diversas formas de ameaças podem por em risco a segurança dos sistemas de informação eletrônicos, e uma das que apresentam maior risco é a personificação, onde alguém alega ser alguma outra pessoa com mais ou diferentes privilégios no acesso e manipulação do sistema. A proteção dos sistemas contra este tipo de ameaça é a sua capacidade de autenticar seus usuários, verificando sua identidade.

Os procedimentos de autenticação de usuários podem ser classificados em três categorias básicas, de acordo com o tipo de prova de identidade que o usuário vai fornecer ao sistema. Estas categorias são:

- Autenticação por conhecimento;
- autenticação por propriedade;
- autenticação por característica.

Os sistemas biométricos se enquadram na categoria de autenticação por característica, onde o usuário é autenticado pelo sistema através da apresentação de alguma característica física ou comportamental.

A utilização de partes do nosso corpo ou características do nosso comportamento para nos distinguir de qualquer outra pessoa é um processo que faz parte da interação humana. Os sistemas biométricos automatizam este processo, tentando reproduzir o que o ser humano já faz naturalmente.

O objetivo deste trabalho é apresentar o funcionamento geral dos sistemas biométricos e as tecnologias existentes como base para seu desenvolvimento, bem como questões específicas relacionadas à utilização destes sistemas.

PALAVRAS-CHAVE: Sistemas biométricos, autenticação de usuários, verificação de usuários.

Title: ”User Authentication Using Biometrics”

Abstract

Many ways of threat may put electronic information systems in risk, and impersonation is one of the most dangerous, where someone pretends to be another person with more or different privileges to access and manipulate the system. Protection against that kind of menace lies upon systems capability to proof users by checking their identity.

Authentication procedures may be classified on three basic categories, considering the kind of identity proof the user will furnish to the system:

- Proof by knowledge;
- proof by possession;
- proof by something that you are.

Biometrics are classified as ”proof by something that you are”, where the user is authenticated by the presentation of any physical or behavioural character.

The use of part of the body or behavioural character to distinguish one person from another belongs to human interaction. Biometrics automatize this process in order to transcript what human beings naturally already do.

This work intends to present biometrics general functioning and technologies basis for its development, as well as to discuss some specific questions related to these systems managements.

KEYWORDS: Biometrics, user authentication, user verification.

1 Introdução

1.1 O processo de autenticação de usuários

Durante o período em que ocorria a Revolução Industrial, algum filósofo observador poderia afirmar que nenhum processo de evolução na sociedade humana seria tão determinador e irreversível quanto o que estava estabelecendo os rumos da sociedade naquele momento. Mas a sociedade atual está passando por outro processo evolucionário que aparenta ser ainda mais intenso e mais desafiador. A disseminação da informação tem trazido alterações nas relações profissionais, comerciais e humanas, e estas alterações têm sido rapidamente absorvidas pela sociedade.

A utilização dos sistemas de informação eletrônicos tem dado às empresas uma forma de armazenar suas informações sem a necessidade de manter eventuais registros em papel. Estes sistemas de informação, bem como os dados por eles armazenados e processados, tornaram–se recursos extremamente valiosos, por vezes vitais para as empresas e, em função disto, precisam ser cuidadosamente protegidos. A segurança destes dados pode ser determinada se forem garantidas suas três principais características: a integridade, a confidencialidade e a disponibilidade, o que significa que os dados devem ser consistentes, acessíveis somente a operações autorizadas e disponíveis no momento em que forem necessários.

No passado, era relativamente simples proteger sistemas informatizados, porque estes eram tipicamente centralizados. Estações terminais normalmente estavam localizadas em um mesmo prédio, de forma que o acesso aos sistemas só seria possível aos usuários que tivessem acesso físico às instalações. Com a disseminação dos sistemas compartilhados e em rede, esta proteção garantida pelo controle de acesso físico não é mais realidade. O gradativo aumento da interconexão entre sistemas informatizados permitiu distribuição e processamento de informação muito mais fácil e rapidamente do que num passado não muito distante, mas em compensação tornou bem mais difícil a identificação do usuário baseado em sua localização física. A interconexão dos sistemas através da utilização de redes de computadores também possibilitou o aumento de oportunidades para abusos nestes sistemas [FED 91].

Uma das mais perigosas ameaças à segurança dos sistemas de informação é a personificação, onde alguém alega ser alguma outra pessoa que tenha mais ou diferentes privilégios no acesso e manipulação do sistema. A proteção dos sistemas contra este tipo de ameaça é a sua capacidade de verificar a identidade dos seus usuários. O problema de verificação da identidade de usuários é bastante complexo, e sistemas que não são capazes de diferenciar entre requisições de usuários legítimos e tentativas de acesso não autorizados são vulneráveis a diversos tipos de ataque.

O processo de verificação da identidade de usuários faz parte de um conjunto mais amplo de operações que determinam o mecanismo de controle de acesso ao sistema. As operações necessárias para o controle de acesso ao sistema ocorrem na seguinte sequência:

- IDENTIFICAÇÃO: O processo de identificação é o momento em que o usuário fornece algum identificador que o individualiza em relação aos outros usuários do sistema. Esta identificação pode, na prática, representar um indivíduo ou um grupo de indivíduos, mas para o sistema isto será indiferente.

- AUTENTICAÇÃO: No processo de autenticação o usuário estabelece a validade da sua identidade. Neste momento, o usuário fornece ao sistema alguma evidência de que ele é realmente o detentor da identidade apresentada. A autenticação é um dos mais importantes princípios para segurança de sistemas informatizados, e a capacidade dos sistemas de verificar com precisão a identidade dos seus usuários é vital para a proteção de seus dados.

- AUTORIZAÇÃO: Após a verificação da identidade do usuário, ocorre a liberação de seu acesso ao sistema de acordo com o perfil de acesso estabelecido para aquele usuário, ou seja, em função dos direitos de acesso definidos para aquela identificação no sistema.

- AUDITORIA: É um procedimento opcional mas extremamente importante no processo de controle de acesso ao sistema. O registro de operações no sistema permite as atividades dos usuários ou mesmo do próprio sistema sejam acompanhadas. Estes registros fornecem uma trilha de auditoria e, em caso de fraude, é possível verificar quais usuários tiveram oportunidade ou efetivamente fraudaram o sistema.

A segurança e o desempenho dos processos de identificação e autenticação podem afetar diretamente outras funções do sistema, como a de auditoria. Os procedimentos de autenticação podem ser divididos em três categorias básicas, de acordo com o tipo de prova de identidade que o usuário vai fornecer ao sistema, e podem ser combinados para garantir maior confiabilidade no processo de autenticação. Estas três categorias são:

- AUTENTICAÇÃO POR CONHECIMENTO: apresentação de algo que o usuário saiba, como uma senha;

- AUTENTICAÇÃO POR PROPRIEDADE: apresentação de algo que o usuário possua, como uma chave ou cartão magnético;

- AUTENTICAÇÃO POR CARACTERÍSTICA: apresentação de alguma característica física ou comportamental do usuário, ou seja, a partir de algo que ele seja ou faça. Estas são as características biométricas do indivíduo.

O principal objetivo de um sistema de autenticação deve ser o de fazer com que o custo de um ataque ao sistema seja muito maior do que o possível ganho que o atacante poderia ter. A robustez de um sistema de autenticação deve ser escolhida de forma a prover o grau de confiança necessário para os requerimentos de segurança da aplicação [FED 91]. Sistemas de autenticação por conhecimento ou propriedade são relativamente pouco confiáveis, pois senhas podem ser divulgadas, descobertas ou esquecidas; cartões magnéticos podem ser duplicados, roubados ou perdidos.

Características biométricas são inerentes ao indivíduo, e o acompanham para onde ele for.

1.2 Estrutura do trabalho

Esta dissertação está dividida em 13 capítulos, sendo esta Introdução o primeiro, e 2 apêndices.

No Capítulo 2 são apresentadas as formas de autenticação de usuários por conhecimento e propriedade.

O Capítulo 3 descreve o funcionamento de sistemas biométricos, bem como suas características mais importantes.

Os Capítulos 4 a 9 apresentam as características físicas e comportamentais humanas mais utilizadas em sistemas biométricos: o Capítulo 4 trata da utilização da impressão digital; o Capítulo 5 apresenta a geometria da mão; o Capítulo 6 descreve sistemas que utilizam a face; o Capítulo 7 mostra a utilização da íris; o Capítulo 8 fala sobre o sistema baseado em imagens da retina, e o Capítulo 9 apresenta sistemas baseados no reconhecimento da voz.

O Capítulo 10 relaciona algumas tecnologias utilizadas em sistemas biométricos emergentes.

No Capítulo 11 é abordado o problema de realização de testes e certificação dos sistemas biométricos apresentados para o mercado.

O Capítulo 12 descreve as utilizações mais comuns para sistemas biométricos atualmente.

O Capítulo 13 apresenta a conclusão deste trabalho.

O Anexo A apresenta tabela de comparação resumida entre os sistemas biométricos descritos nos principais capítulos deste trabalho.

E, finalmente, o Anexo B apresenta os resultados de um experimento sobre a utilização de um sistema biométrico baseado em reconhecimento de faces.

2 Sistemas Tradicionais de Autenticação de Usuários

2.1 Autenticação por conhecimento

A abordagem mais comum para autenticação de usuários é a da apresentação de uma prova de conhecimento, normalmente através da utilização de senhas. O usuário possui uma senha supostamente secreta, que deve ser submetida ao sistema no momento de sua solicitação de acesso.

A principal vantagem da utilização de autenticação baseada somente em senhas é que este procedimento pode ser implementado apenas com a utilização de software; nenhum hardware adicional é necessário. Sua implementação é, em geral, extremamente simples.

Mas a autenticação por conhecimento apresenta a desvantagem de que as senhas representam uma informação que está na memória do usuário, mas não necessariamente têm qualquer relação com ele. O usuário pode fazer com sua senha o que bem entender. Senhas podem ser facilmente descobertas, adivinhadas, divulgadas, observadas e esquecidas.

2.1.1 Vulnerabilidades na utilização de senhas

Sistemas de autenticação que utilizam somente senhas falham em proteger integralmente o acesso ao sistema por diversas razões. Senhas deveriam ser de conhecimento somente do próprio usuário, mas frequentemente não são. Usuários com permissão de escolher suas próprias senhas muitas vezes optam por senhas fáceis de serem memorizadas e, consequentemente, fáceis de serem adivinhadas. Senhas geradas automaticamente podem ser formadas por uma sequência de caracteres randômica que seja de difícil memorização, obrigando o usuário a anotá-las em algum lugar, e permitindo então que sejam descobertas por outras pessoas.

Um atacante do sistema poderia determinar a senha de um usuário utilizando as seguintes abordagens:

- BUSCA PELA LISTA DE SENHAS: O atacante mais familiarizado tecnicamente com o sistema pode vasculhá-lo à procura do local onde as senhas estão armazenadas. Isto representará alguma ameaça mais evidente se as senhas forem armazenadas em local não protegido do sistema e sob a forma de texto claro.

- ATAQUE EXAUSTIVO: Envolve a submissão ao sistema de tantos quantos forem os valores possíveis para determinada senha até encontrar o valor que seja correto. Isto significa, na pior das hipóteses, tentar todas as combinações possíveis para aquele tipo de senha em função de seu tamanho e da faixa de valores permitidos para sua composição (vide 2.1.2).

- ATAQUE DO DICIONÁRIO: Os valores submetidos ao sistema representam palavras reais, com algum significado, escolhidas em sequência em um dicionário.

- ENGENHARIA SOCIAL: Usuários que têm permissão para escolher suas próprias senhas frequentemente escolhem senhas que têm alguma relação com a sua pessoa. Datas de aniversários, números de telefone, nomes de parentes e animais de estimação ou esportes preferidos geralmente estão incluídos nas escolhas mais comuns. O trabalho do atacante é conhecer um pouco da vida pessoal do usuário e verificar se suas senhas têm alguma relação com as informações obtidas.

- COLABORAÇÃO DO USUÁRIO: A forma mais simples de se obter a senha de um usuário é simplesmente perguntando a ele. Muitas vezes o usuário tem interesse em divulgar sua senha como forma de compartilhar algum recurso ao qual ele tenha acesso e outros não. Adicionalmente, o usuário pode ingenuamente colaborar com o atacante quando este solicita sua senha para alguma operação para a qual ele (o atacante) não tenha direitos de acesso, abusando da confiança do usuário.

2.1.2 Fatores que afetam a segurança de senhas

Existem vários motivos pelos quais a utilização de senhas para a autenticação de usuários é um processo inseguro, e que na prática restringem sua utilização a sistemas com requerimentos de segurança mínimos. Diversos fatores afetam a segurança de um sistema que utiliza senhas para autenticação. Entre estes fatores estão a composição da senha, seu tamanho, tempo de vida, fonte, distribuição, armazenamento, e entrada da senha no sistema, que são descritos a seguir [FED 91].

- COMPOSIÇÃO: A composição da senha se refere à faixa de valores da qual cada caracter da senha pode ser escolhido. Por exemplo, uma determinada aplicação pode permitir que cada caracter da senha seja escolhido entre todas letras do alfabeto. Admitindo que não há diferenciação entre letras maiúsculas e minúsculas, existem 26 valores possíveis que cada caracter pode assumir. Neste caso, se cada caracter for armazenado em um byte, existem 256 valores virtualmente possíveis para cada caracter, e a restrição à utilização somente das 26 letras do alfabeto diminuiria a possível segurança do sistema de senhas. Mas muitas vezes é necessário restringir a faixa de valores por razões práticas. Muitos teclados não possuem todos caracteres especiais permitidos nesta representação de 1 byte. Além disso, se os caracteres para composição da senha forem escolhidos randomicamente entre todos os valores possíveis, formarão combinações de difícil memorização, obrigando o usuário a anotá-las.

- TAMANHO: O tamanho da senha representa o número total de caracteres que a compõem. Em combinação com a faixa de valores permitidas para cada caracter, determina o número total de valores possíveis para cada senha. O aumento do tamanho da senha e/ou sua composição aumenta proporcionalmente o número de combinações possíveis, aumentando a segurança geral do sistema. Ataques exaustivos se tornam mais difíceis, mas os usuários podem encontrar maiores problemas para memorização da senha.

- TEMPO ÚTIL: O tempo útil de uma senha vai indicar também a quantidade de tempo que um possível atacante poderá utilizar para tentar descobrir a senha

correta, através de busca exaustiva ou outras técnicas. Se a senha do usuário não é modificada em intervalos regulares, se torna mais fácil de ser descoberta pelo atacante. A segurança com a troca de senhas é garantida somente se a nova senha não apresenta qualquer relação com a anterior. Em sistemas onde é permitida a escolha de senha pelos usuários, estes normalmente escolhem novas senhas que são variações das senhas anteriores, aumentando o risco de o atacante descobrir a nova senha no caso de a anterior ser de seu conhecimento, pois a senha anterior fornece informação sobre os valores possivelmente escolhidos para a mais recente. O tempo útil das senhas em uma determinada aplicação deve ser balanceado entre a segurança resultante de um período curto entre trocas e o incômodo causado para os usuários pela troca frequente de senhas. A dificuldade de memorizar muitas senhas em curtos períodos pode fazer com que os usuários escolham senhas mais triviais e, consequentemente, mais fáceis de serem descobertas.

- FONTE: A fonte geradora de novas senhas no sistema tem grande impacto na sua segurança. Se as senhas são geradas por um sistema automático, este deverá ser confiável e responsável por garantir a segurança dos valores gerados. Os usuários também podem ser autorizados a determinar suas próprias senhas. Neste caso, algum tipo de conferência deve ser feito pelo sistema para verificar se estas senhas são muito evidentes e, caso sejam, solicitar a apresentação de uma nova senha.

- DISTRIBUIÇÃO: Senhas geradas automaticamente devem ser distribuídas para os usuários, e devem ser protegidas contra tentativas de interceptação. Esquemas de criptografia podem ser utilizados para senhas que são divulgadas eletronicamente.

- ARMAZENAMENTO: A proteção de senhas armazenadas pode ser conseguida se elas estiverem em uma área lógica ou fisicamente protegida e que só poderia ser acessada por componentes autorizados do sistema, ou ainda se a elas for aplicado algum esquema de criptografia antes de seu armazenamento.

- APRESENTAÇÃO AO SISTEMA: Os usuários devem submeter suas senhas ao sistema durante o processo de solicitação de acesso, e a senha pode ser observada de alguma forma no momento de sua apresentação. O terminal não deve exibir a senha conforme ela esteja sendo digitada, para que outros usuários não possam lê-la a partir do terminal. As mensagens de erro informadas pelo sistema devem ser cuidadosas. Por exemplo, em caso de erro de digitação da senha, o sistema deveria informar algo como “acesso negado” no lugar de “senha inválida”, para que um possível atacante ficasse na dúvida se somente a senha não estava correta ou se o usuário informado também não estava cadastrado no sistema. Os usuários devem ter o direito de reapresentar sua senha para o caso de qualquer possível erro de digitação, mas deve haver um limite no número de senhas incorretas aceitas pelo sistema, para protegê-lo de ataques exaustivos. Quando este limite é excedido, o sistema deve bloquear a conta do usuário, que deverá notificar o administrador do sistema para que este providencie o desbloqueio de sua conta e o cadastramento de nova senha.

2.2 Autenticação por propriedade

Os sistemas de autenticação baseados unicamente na possessão de algum objeto são os mais sujeitos a fraude. Isto ocorre porque estes objetos, teoricamente, não têm absolutamente qualquer relação com o seu proprietário.

A identidade de um usuário pode ser provada solicitando-se a ele a confirmação da possessão de algum objeto físico que deveria ser único para aquele usuário ou grupo de usuários. Objetos utilizados com esta finalidade são denominados *tokens de autenticação.* Por exemplo, uma carteira de motorista pode ser considerada um token de autenticação, pois pode ser utilizada para provar que seu usuário tem permissão para dirigir. Numa sociedade acostumada ao uso de documentos para identificar as pessoas, tokens utilizados normalmente no dia a dia incluem documentos de identidade, passaportes e cartões de crédito, por exemplo.

O problema da utilização de tokens para autenticação de usuários é que a possessão do token autoriza o usuário a fazer algo, mas não garante que a pessoa que está de posse do token seja realmente o usuário autorizado. Tokens podem ser perdidos, roubados e duplicados, e o risco de outra pessoa tirar proveito da perda ou roubo de um token, assumindo a identidade da pessoa autorizada, está implícito no tipo de autenticação estritamente baseada em tokens. A pessoa que possuir o token se torna um usuário autorizado, mesmo que não o seja. Para reduzir este risco, é comum a utilização de algum processo subsequente de autenticação do proprietário em conjunto com a autenticação pelo token. Por exemplo, o passaporte autoriza seu proprietário a viajar, e a fotografia no passaporte é a garantia de que o proprietário do passaporte é o usuário que o está apresentando. A fotografia é informação registrada com o propósito de autenticar o proprietário do passaporte. O mesmo vale, por exemplo, para assinaturas em cartões de crédito.

Cartões magnéticos frequentemente são utilizados para o armazenamento de senhas ou chaves criptográficas, e não requerem nenhuma autenticação adicional do proprietário. Estes cartões atuam somente como um meio de armazenamento auxiliar, armazenando dados que o ser humano não poderia manter em sua memória. Na verdade, o processo operacional seria baseado em token, mas a autenticação em si seria feita via prova de conhecimento.

Os tipos de tokens comumente utilizados em sistemas de autenticação são:

- CARTÕES DE TARJA MAGNÉTICA: São largamente aceitos, uma vez que sua utilização já é frequente em diversas aplicações, como caixas eletrônicos, cartões de crédito e controle de acesso físico. A identidade do usuário fica armazenada no cartão. Normalmente são utilizados em associação com alguma senha. Por serem padronizados, estes cartões podem ser duplicados sem maiores problemas. Algumas novas tecnologias garantem maior segurança a estes cartões incorporando técnicas adicionais contra falsificação [POL 97].

- CARTÕES RF-ID: São cartões que contém um minúsculo rádio-transmissor, que é ativado a partir do recebimento de sinal de uma frequência específica. A identidade do usuário pode ser enviada ao sistema mesmo sem o seu conhecimento.

– SMART–CARDS: Os smart-cards são na verdade portadores de dados no formato de um cartão plástico comum, que contém um ou mais circuitos integrados para armazenamento e processamento de dados. Um smart-card típico contém normalmente um microprocessador, ROM para armazenar instruções operacionais, RAM para armazenar dados durante o processo, e EPROM ou EEPROM para armazenamento não-volátil de informações [UNI 98]. Na verdade, a classificação da utilização de smart-cards como autenticação por propriedade peca por subestimar sua capacidade de utilização. Um smart-card pode realizar diversas operações de autenticação independente de outros componentes do sistema.

3 Sistemas Biométricos

3.1 Introdução

O conceito da individualidade dos traços pessoais existe desde os tempos mais remotos e a identificação das pessoas baseada nestes traços não é recente. Partes do nosso corpo ou características do nosso comportamento são normalmente utilizadas para nos distinguir de qualquer outra pessoa, num processo repetido diversas vezes a cada dia e que faz parte da interação entre seres humanos.

O reconhecimento informal e primitivo pelo formato do rosto ou pelo som da voz, ou o reconhecimento formal, como assinaturas ou impressão digital, são métodos que utilizam características físicas e comportamentais dos seres humanos para estabelecer ou verificar sua identidade.

Artefatos arqueológicos indicam que a individualidade das impressões digitais já era reconhecida desde pelo menos o período neolítico. Em 1882, Alphonse Bertillon, chefe do Departamento de Identificação Criminal da Polícia de Paris, desenvolveu um método extremamente detalhado de identificação de pessoas baseado em diversas medidas, descrições físicas e fotografias. O Sistema Bertillon de Identificação Antropométrica teve grande aceitação até ser substituído pelos sistemas de identificação baseados em impressão digital [JAI 99a].

Algumas características do indivíduo, como DNA, impressão digital e assinatura, ganharam status legal e podem se utilizadas como evidência para a Justiça para o estabelecimento de uma prova de identidade. Até recentemente, a decisão de se duas amostras de uma característica biométrica pertenciam à mesma pessoa era uma tarefa de sistemas manuais ou semi-automáticos, que requeriam especialistas bem treinados para realizar os processos de classificação e comparação das amostras [JAI 99a].

O termo “biometria” denomina a ciência que envolve análises estatísticas no estudo de fenômenos biológicos, e consequentemente pode ser aplicado para incluir o estudo estatístico de medidas de características humanas. Mas, quando se fala em sistemas biométricos, normalmente o significado é a utilização de tecnologias que analisam as características humanas para propósitos de segurança. A ciência estatística continua em background [ROE 98].

A utilização de sistemas biométricos em aplicações totalmente automatizadas é relativamente recente. Esta automatização significa que o sistema está livre da subjetividade e de possíveis erros inerentes às avaliações humanas. Estes sistemas são considerados um grupo de tecnologias de alto nível, podendo englobar tanto o hardware quanto o software necessários para o processamento dos dados biométricos, medindo, registrando e avaliando as características do indivíduo.

Uma característica biométrica é uma característica única de um ser humano, possível de ser medida, utilizada para verificar ou reconhecer automaticamente sua identidade [ROE 98]. De uma forma geral, podem ser divididas em duas categorias:

- CARACTERÍSTICAS FÍSICAS OU FISIOLÓGICAS: São características físicas inerentes ao indivíduo, relativamente estáveis e de difícil modificação. Nesta categoria estão incluídas impressões digitais, geometria da mão, os padrões da retina e da íris e as características da face.

- CARACTERÍSTICAS COMPORTAMENTAIS: São características referentes a aspectos do comportamento do indivíduo, influenciadas por sua personalidade e seus costumes, e que geralmente podem ser alteradas de acordo com a sua vontade. Entre estas características estão a assinatura e o padrão de voz.

3.2 Funcionamento geral dos sistemas biométricos

Embora diferentes sistemas biométricos sejam baseados em diferentes tecnologias, todos os sistemas operam essencialmente da mesma forma e muito pode ser dito sobre seu funcionamento em geral e sobre os mesmos fatores externos que os afetam [ROE 98].

Todos os sistemas biométricos são essencialmente baseados em conceitos de reconhecimento de padrões, cujas operações são divididas em três atividades básicas: extração e seleção das características, comparação entre as amostras e decisão. Os sistemas biométricos realizam ainda as operações de aquisição do sinal, na forma da tomada dos dados biométricos, e o armazenamento dos templates gerados a partir da extração das características. Embora estas operações possam ser classificadas separadamente, na verdade são totalmente interdependentes [CAM 99]. O funcionamento geral dos sistemas biométricos é ilustrado na figura 3.1 e descrito a seguir.

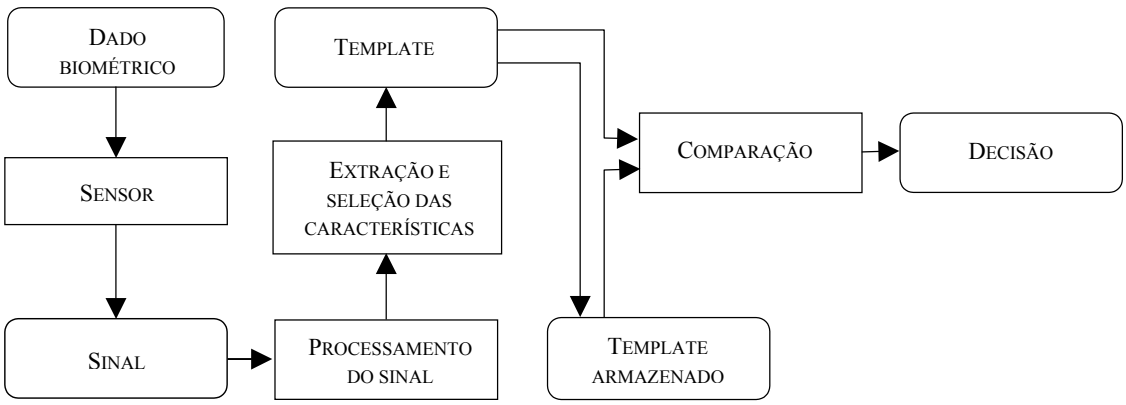

Figura 3.1 – Funcionamento geral dos sistemas biométricos

3.2.1 Tomada de dados

A aquisição do sinal pelo sistema biométrico é representada pela tomada dos dados biométricos do usuário. Este é um dos processos críticos para o bom funcionamento do sistema, uma vez que a precisão com que as amostras são fornecidas ao sistema muitas vezes tem influência direta na sua performance geral [JAI 99a].

Durante o processo de reconhecimento de usuários através de um sistema biométrico, o usuário vai interagir com o sistema para tomada de seus dados em duas situações distintas: no momento de seu registro no sistema e na apresentação de uma nova amostra para comparação.

Para que o usuário possa ser verificado em um sistema biométrico, é necessário primeiro que ele seja conhecido pelo sistema. O cadastramento é o processo durante o qual o novo usuário fornece ao sistema uma amostra da característica biométrica utilizada, para que a partir daquele momento o sistema saiba que o usuário existe e tenha as informações necessárias para poder determinar sua identidade. Alguns sistemas biométricos necessitam que apenas uma amostra do dado biométrico seja fornecida durante o processo de cadastramento, enquanto outros exigem a apresentação de mais de uma amostra. Estas várias leituras podem ser utilizadas para a elaboração de um perfil da característica biométrica, ou então todas as leituras podem ser mantidas para permitir uma avaliação da variação da característica do usuário. Durante o processo de cadastramento também são fornecidas ao sistema outras informações adicionais necessárias, como a identidade do usuário à qual aquela característica está relacionada

A fase de cadastramento deve ser precedida de treinamento do usuário, para que a qualidade dos dados obtidos seja a melhor possível. Quando o usuário demonstrar que está apto a interagir com o sistema corretamente, poderá ser considerado apto a efetuar seu registro no sistema. O processo de cadastramento acontece teoricamente uma única vez para cada usuário, e alterações no seu registro devem acontecer em caso de alteração relevante na característica biométrica [MCD 94].

O usuário irá interagir novamente com o sistema a cada vez que necessitar ter sua identidade verificada. Nesta ocasião, uma nova amostra da característica biométrica deverá ser apresentada ao sistema, para que possa ser comparada à amostra armazenada no momento do registro do usuário.

Para que a amostra fornecida tenha um mínimo de qualidade garantida, algum tipo de auxílio deve permitir que o usuário possa verificar se está fornecendo a amostra ao sistema corretamente. A visualização da imagem durante o processo de captura óptica dos dados, por exemplo, é importante para que o usuário avalie se a sua interação com o dispositivo está correta. Este procedimento pode diminuir o número de tentativas de verificação frustradas devidas a erros de leitura causados por falhas na interação com o sistema. Além disso, em sistemas que possuem esta capacidade, pode ser difícil para o usuário sabotar o processo de captura dos dados, uma vez que seria possível a monitoração deste processo por um operador. Este seria o caso típico de um usuário que tenta um novo registro no sistema alegando ainda não estar cadastrado. Uma boa aquisição dos dados resulta no aumento das chances de detecção do registro do usuário no sistema, por isso o fraudador vai tentaria degradar a qualidade dos dados apresentados. Por outro lado, numa situação de controle de acesso, o usuário tenta fazer

o melhor possível para obter uma identificação positiva, o que faz o mecanismo de auxílio extremamente útil [RUG 98].

Os procedimentos de coleta de dados também são diferentes dependendo do dispositivo biométrico utilizado. Algumas características biométricas são mais propensas a erros durante a tomada de dados, enquanto outras conseguem produzir resultados consistentes a cada leitura. Além disso, a dificuldade no processo de tomada de dados pode influenciar na aceitação do sistema pelo usuário: se o percentual de leituras não aceitas pelo sistema é alto, a confiança do usuário no sistema como um todo tente a diminuir, causando também incômodo pela repetição da tomada de dados.

3.2.2 Extração e seleção das características

A partir do sinal obtido na tomada de dados, serão extraídas as características consideradas relevantes para a geração do template. O coração dos sistemas biométricos são os mecanismos, compostos por algoritmos ou redes neurais, por exemplo, que executam este processo de extração de características e posterior comparação dos dados resultantes [ROE 98].

Inicialmente, o sinal adquirido deve ser processado de forma a eliminar possíveis ruídos causados por condições ambientais, interação inadequada do usuário com o dispositivo ou erros ocasionados pela digitalização do sinal. Após a eliminação de possíveis ruídos, devem ser selecionadas, dentre todas as informações contidas no sinal resultante, aquelas que são realmente relevantes e discriminatórias e que deverão ser consideradas para comparação.

O resultado gerado por este processo é uma representação matemática das características essenciais contidas na amostra e é a partir deste resultado que é gerado o template. Em alguns sistemas, quando o usuário é solicitado a fornecer diversas amostras no momento de seu registro, os templates resultantes podem ser armazenados separadamente ou podem ser condensados em um resultado médio que melhor represente a característica biométrica do indivíduo.

Uma vez que o template é gerado a partir de uma representação matemática que contém somente as características relevantes do dado biométrico, é impossível que o dado biométrico original seja reproduzido a partir do template. Ou seja, a partir do template não seria possível, por exemplo, gerar uma cópia artificial fiel de uma impressão digital ou íris.

3.2.3 Armazenamento do template

Os dados gerados no momento do cadastramento do usuário no sistema precisam ser armazenados de alguma forma, para que possam ser recuperados para comparação no momento em que o usuário apresenta uma nova amostra ao sistema. O armazenamento destes templates será apresentado com mais detalhes no ítem 3.6.

Como as características biométricas eventualmente podem sofrer pequenas mas contínuas alterações, a tendência seria que, com o passar do tempo, as novas amostras

fornecidas fossem se distanciando cada vez mais da amostra original. A forma com que os sistemas biométricos poderiam ”aprender” a reconhecer estas alterações seria através da atualização dos templates. Em caso de verificação positiva do usuário, a amostra contida no template deveria ser substituída pela nova amostra, e assim sucessivamente, fazendo com que o template seja continuamente atualizado e reflita sempre o estado mais recente da característica biométrica.

3.2.4 Comparação e decisão

O passo seguinte para a verificação do usuário é a comparação da sua nova amostra fornecida ao template armazenado. Esta nova amostra poderá ser comparada com um template específico (autenticação) ou com todos os templates armazenados na base de dados (identificação). Estes dois tipos de busca na base de dados do sistema biométrico são discutidos com mais detalhes no ítem 3.5.

A comparação entre a nova amostra e o template ganha uma pontuação, que é analisada em função de um determinado valor limite. Esta pontuação vai permitir que o sistema avalie se a nova amostra é suficiente similar ao template armazenado para que possam ser considerados coincidentes. Neste momento, o sistema está apto "aceitar" ou "rejeitar" o usuário baseado na política de verificação previamente definida. A avaliação desta pontuação e seus resultados serão apresentados no ítem 3.4.

3.3 Características biométricas

Muitas características fisiológicas e comportamentais dos seres humanos são supostamente únicas, ou possuem uma chance remota de haver um indivíduo na mesma população alvo que possua esta característica com o mesmo valor de outro indivíduo. Teoricamente, qualquer destas características poderia ser utilizada como base de um sistema biométrico, desde que apresentasse as seguintes propriedades:

- UNIVERSALIDADE: Todo os indivíduos da população alvo devem possuir esta característica;

- SINGULARIDADE: Quaisquer duas pessoas escolhidas dentre os indivíduos da população alvo não devem ter o mesmo valor para esta característica;

- ESTABILIDADE A LONGO PRAZO: A característica deve ser relativamente invariante no tempo;

- COLETABILIDADE: A característica deve poder ser medida quantitativamente de alguma forma [JAI 99a].

Os sistemas biométricos utillizam os princípios básicos de qualquer sistema de reconhecimento de padrões. A questão central em reconhecimento de padrões é a relação entre a variabilidade intra-classe e variabilidade entre-classes. Estas variabilidades são determinadas pelo número de graus de liberdade (formas de variação) entre as classes de padrões. Podemos aqui considerar como “classe” o próprio

indivíduo. Idealmente, a variabilidade intra-classe deve ser pequena e a variabilidade entre-classes deve ser grande, de forma que a decisão do que é "igual" e "diferente" possa ser feita facilmente. No caso de identificação biométrica de pessoas, este princípio básico implica que uma medida biométrica ótima deve ter máxima variação entre indivíduos, e mínima variação para uma mesma pessoa em tempo ou condições diferentes [DAU 99].

Estas duas variabilidades vão determinar as medidas de performance do sistema: a variabilidade intra-classe vai determinar a taxa mínima de falsa rejeição para uma população, e o limite mais baixo da variabilidade entre-classes vai determinar a taxa mínima de falsa aceitação.

Estas duas dimensões das variações biológicas refletem as influências genéticas e ambientais associadas com os conceitos de genótipo, fenótipo e penetrância genética [DAU 99].

O genótipo se refere à constituição genética, e o fenótipo se refere à expressão de uma característica pela interação do genótipo, do desenvolvimento e da influência ambiental. A penetrância genética indica a capacidade de herança ou a extensão de como a característica expressada é determinada geneticamente.

Pessoas geneticamente idênticas compartilham todas as características genéticas, como tipo sanguínio e sequência de DNA. Muitas características podem ser firmemente classificadas como genótipas ou fenótipas (como, por exemplo, gênero e impressão digital, respectivamente). Algumas características, como a aparência do rosto, possuem fatores genótipos e fenótipos [DAU 99].

É desejável que as decisões para reconhecimento sejam baseadas em características que tenham muito pouca penetrância genética, para que indivíduos geneticamentoe idênticos ou com algum parentesco ainda possam ser distinguíveis. Estas características biométricas devem ainda ser formadas por padrões randômicos e com alta complexidade, e ter estabilidade a longo prazo na vida do indivíduo.

3.4 Medidas de performance

A principal diferença entre a verificação de identidade feita por sistemas biométricos e a utilização de senhas ou cartões é que um sistema biométrico não pode dar uma resposta absoluta de "sim" ou "não" quando solicitado a verificar a identidade de um usuário. Uma senha ou é "ABCD" ou não é e, quando digitada, é somente correta ou incorreta; um cartão tem o número serial "1234" ou não tem. Já uma característica biométrica pode sofrer variações cada vez que uma medida da característica é feita.

Os sistemas biométricos apresentam variações na medida das características físicas ou comportamentais dos seres humanos, justamente porque seres humanos são inconsistentes e suas características físicas e comportamentais podem variar sutilmente com o passar do tempo. Além disso, a própria forma como o usuário interage com o sistema também não é constante [POL 97].

Por exemplo, mesmo considerando que uma assinatura se mantenha constante, até o indivíduo com o comportamento mais consistente vai variar a sua assinatura ligeiramente a cada vez que ela for feita. Em sistemas biométricos que utilizam técnicas ópticas de captura de imagem da característica, como uma imagem de impressão digital ou da íris, a qualidade da imagem capturada pode variar cada vez que uma uma nova tomada da imagem é feita, ou a parte do corpo contendo a característica pode variar sua posição relativa ao dispositivo a cada tomada de imagem. Desta forma, mesmo que o padrão da íris ou da impressão digital não apresente variação entre as tomadas de imagem, o template resultante não será uma cópia exata do template previamente armazenado, ou seja, a nova amostra e o template armazenado não vão produzir uma coincidência de 100%. Na maioria dos casos, esta variação não é muito grande, e a amostra e o template podem ser realmente muito próximos [NEW 99].

Desta forma, as variações nas medidas das características fisiológicas e comportamentais humanas impedem que o sistema biométrico possa verificar absolutamente a identidade de um indivíduo; o sistema somente é capaz de afirmar que existe uma probalilidade *x* de a pessoa ter aquela identidade específica associada. E, obviamente, em condições ideais essa probabilidade deve ser bem próxima de 100%, mas algum mecanismo deve estar embutido no sistema de forma a permitir que o usuário autorizado produza, por exemplo, uma assinatura 99% semelhante à original e ainda assim seja reconhecido pelo sistema [NEW 99].

A implicação desta variação nas medidas da característica é que os sistemas biométricos devem incorporar algum grau de tolerância. Se o sistema estiver preparado para requerer uma coincidência de 100% entre o template e a nova amostra, a quase totalidade dos usuários legítimos será rejeitada pelo sistema, porque a nova amostra muito dificilmente gerará uma coincidência exata com o template. Na prática, os sistemas biométricos devem requerer no máximo que a nova amostra e o template sejam somente uma coincidência próxima, não uma coincidência exata.

Por outro lado, permitindo que a coincidência entre a nova amostra e o template seja livre o suficiente para que nenhum usuário legítimo seja rejeitado, outro problema ocorre: a tolerância poderá ser tão baixa que o sistema talvez permita a aceitação de impostores [NEW 99].

Cada tecnologia utilizada em sistemas biométricos possui uma forma diferente de associar uma pontuação para a comparação entre a nova amostra e o template, mas o objetivo desta avaliação é o mesmo para todos os sistemas. Esta pontuação é comparada a um valor limite previamente determinado, e o resultado desta comparação vai determinar se existe a coincidência entre a nova amostra e o template. Pontuações que ultrapassem o valor limite indicam que a nova amostra é suficientemente similar ao template e o sistema considera como se os dois realmente coincidissem; para pontuações abaixo do valor limite, o sistema não identificará a coincidência e o usuário não será reconhecido. Em situações onde a pontuação obtida pela comparação esteja muito próxima do valor limite, o ideal seria que o sistema biométrico exigisse a apresentação de mais uma amostra para nova comparação.

A definição deste valor limite é crítica para a performance geral do sistema. Valores limite muito altos vão requerer que a nova amostra seja extremamente similar ao template e variações um pouco mais significativas na tomada da amostra acarretarão na

rejeição do usuário. Por outro lado, valores limite muito baixos permitirão que uma amostra, mesmo que não seja amostra de um usuário autorizado, mas que possua pelo menos uma semelhança razoável com o template, seja aceita pelo sistema.

Para avaliar a habilidade do sistema em em reconhecer usuários cadastrados e rejeitar usuários não conhecidos pelo sistema, são utilizadas duas medidas de performance que consideram o nível de precisão com que o sistema determina a coincidência entre uma amostra e o template. Essas medidas são avaliadas em função dos dois tipos de erro que o sistema biométrico pode cometer: considerar que uma amostra legítima não coincide com o template armazenado, ou considerar que uma amostra inválida é coincidente com o template armazenado.

Estes dois tipos de erro normalmente são conhecidos por suas denominações em sistemas de identificação positiva: erros de falsa rejeição (Tipo 1) e falsa aceitação (Tipo 2). Um erro de falsa rejeição ocorre quando uma coincidência legítima gera uma pontuação abaixo do valor limite, e um erro de falsa aceitação ocorre quando uma amostra não pertinente gera uma pontuação acima do valor limite. Estes erros são computados em forma de taxas, que normalmente são apresentadas no intervalo [0,1] ou em valores percentuais.

Se as taxas de erro Tipo 1 e Tipo 2 forem plotadas em função dos valores limite, formarão curvas que se interceptarão em um determinado valor limite. Este ponto de intersecção, onde a taxa de erros Tipo 1 se iguala à taxa de erros Tipo 2, determina o *equal error rate* (ERR), e representa, de uma forma geral, a melhor performance geral do sistema. Um gráfico representativo de possíveis curvas de taxa de erro de um sistema biométrico hipotético é apresentado na Figura 3.2.

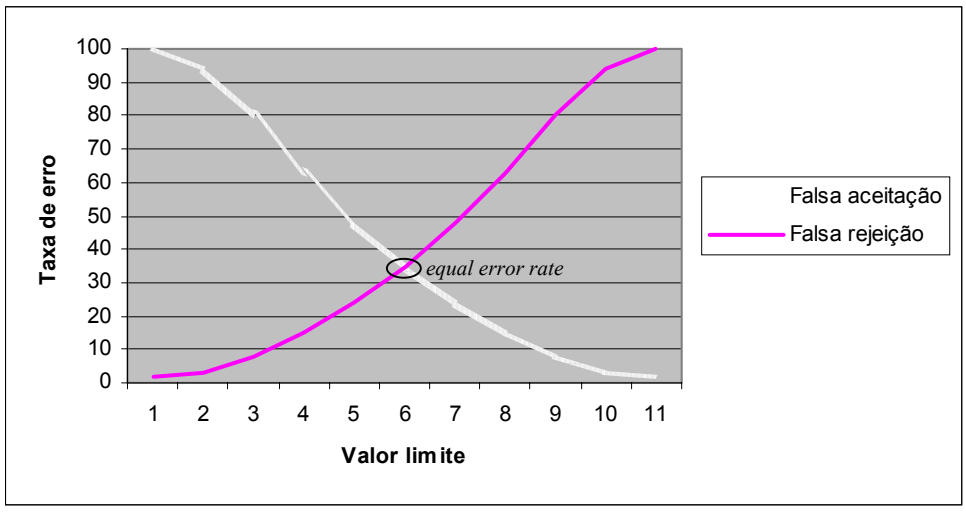

Figura 3.2 – Curvas de taxas de erro

É importante observar que, em sistemas de identificação negativa, a idéia de falsa aceitação e falsa rejeição é inversa à dos sistemas de identificação positiva. Nos sistemas de identificação negativa, a intenção é verificar se o usuário NÃO está

cadastrado no sistema. A falsa aceitação ocorreria quando o sistema considerasse que o usuário ainda não está cadastrado, ou seja, o sistema não identificou uma coincidência com nenhum template existente na sua base de dados, quando na verdade pelo menos uma coincidência existe. Da mesma forma, a falsa rejeição seria quando o sistema não permitisse que o usuário fosse cadastrado por ter encontrado um template que erradamente foi considerado coincidente com a sua amostra. Neste trabalho estaremos sempre considerando a denominação utilizada para os erros em sistemas de identificação positiva.

A falsa rejeição significa um usuário legítimo que foi rejeitado pelo sistema, e a falsa aceitação significa que um impostor conseguiu ter acesso ao sistema. Falsa rejeição causa frustração e falsa aceitação acarreta fraude. Para minimizar estes inconvenientes, os sistemas biométricos normalmente são projetados para permitir que sua precisão possa variar de acordo com os requerimentos de segurança da aplicação. Isto pode ser feito com a adaptação do valor limite que define quando uma comparação entre uma amostra e o template é considerada uma coincidência. Em outras palavras, os sistemas devem permitir a alteração do valor limite de modo a aumentar ou diminuir a segurança do sistema conforme os requerimentos de segurança da aplicação. O objetivo é encontrar um meio-termo entre aceitar todos os usuários legítimos e rejeitar todos os usuários não legítimos.

Por exemplo, para aplicações bancárias, seria razoável que o sistema estivesse configurado de forma a permitir que muito poucos usuários legítimos fossem rejeitados, evitando que estes usuários enfrentassem o inconveniente de ter que apresentar diversas amostras tentando ganhar acesso ao sistema, e evitando ainda que a insatisfação destes usuários fizesse com que eles migrassem para outra instituição financeira. Em contrapartida, muitos usuários não autorizados teriam acesso ao sistema, causando prejuízos financeiros à instituição. Já em aplicações militares de grande segurança, por exemplo, o ideal é que o sistema esteja configurado para a rejeição do maior número de usuários não autorizados possível, o que resultaria em usuários legítimos sendo rejeitados. Um outro exemplo seria a alteração do valor limite na fase de cadastramento dos usuários de forma que a falsa rejeição fosse extremamente baixa, a fim de identificar templates que potencialmente poderiam pertencer ao usuário em questão.

A avaliação correta das aplicações do sistema vai indicar se o mais importante é não permitir que um usuário não autorizado tenha acesso ao sistema ou não impedir o acesso de um usuário legítimo. O sistema deve ter um grau de flexibilidade, mas flexibilidade demais pode comprometer o objetivo do sistema de segurança [NEW 99].

Em geral, as taxas de falsa rejeição e falsa aceitação de um determinado sistema são divulgadas por seu fabricante, sem informações adicionais sobre como estes valores teriam sido alcançados. Normalmente estes valores são obtidos pelos fabricantes em ambientes de teste extremamente controlados e tendenciosos para que indiquem a melhor performance possível. Atualmente, órgãos independentes vêm realizando testes confiáveis que auxiliam os usuários destes sistemas na avaliação e comparação entre os sistemas disponíveis. Este assunto será tratado com mais detalhes no Capítulo 12.

3.5 Tipos de busca na base de dados

Existem três objetivos distintos que podem ser alcançados por sistemas biométricos: provar que você é quem diz ser, provar que você não é quem diz não ser, e descobrir quem você é. Estas operações podem ser basicamente classificadas em dois tipos de interação do sistema com seus templates: autenticação e identificação.

3.5.1 Autenticação

O processo de autenticação - ou verificação - se refere ao problema de confirmar ou negar a identidade alegada pelo usuário. Este processo ocorre quando o usuário já é conhecido pelo sistema e precisa apenas provar que ele é o detentor da identidade alegada. O processo de verificação responde basicamente a pergunta: "Este usuário é realmente quem diz ser?".

Este é um processo um-para-um, onde o sistema verifica a identidade do usuário comparando a amostra fornecida com com um único template específico. Ou seja, o processo de verificação se resume à comparação de dois conjuntos de dados biométricos para determinar se eles pertencem ao mesmo indivíduo.

Para poder realizar a verificação do usuário, o sistema deve primeiro conhecer qual template deverá ser comparado à nova amostra. A localização deste template pode se dar de duas formas, dependendo de como os templates estejam armazenados:

- TEMPLATES ARMAZENADOS INDIVIDUALMENTE: O template é armazenado em algum dispositivo que o usuário carrega consigo, como um cartão magnético. No momento da verificação, o usuário apresenta o seu template ao sistema, e fornece uma nova amostra da característica biométrica. O sistema então compara esta amostra com o template fornecido.

- TEMPLATES ARMAZENADOS EM CONJUNTO: Se templates estão todos armazenados em base de dados ou na memória do dispositivo, o usuário primeiro fornece algum tipo de identificação primária, como um nome ou um código, que foi previamente relacionada ao template no momento do seu registro. Através da identificação fornecida, o sistema localiza o template na base de dados e o compara com a nova amostra fornecida pelo usuário.

A autenticação é um processo rápido porque compara somente um único template à amostra fornecida.

3.5.2 Identificação

O processo de identificação de usuários pode ser dividido em dois tipos: identificação positiva e identificação negativa. Em ambos os casos, a identidade do usuário não é conhecida, e o desafio do sistema é estabelecer – ou não – sua identidade. Operacionalmente os dois tipos de identificação funcionam da mesma forma, mas seu

objetivo é diferente. Na identificação positiva, o sistema responde a pergunta: “Quem é este usuário?”. Na identificação negativa, o sistema precisa descobrir se o usuário realmente ainda não é conhecido pelo sistema, respondendo a pergunta: “Este usuário realmente ainda não existe?”.

Uma forma mais clara de compreender a diferença entre identificação positiva e identificação negativa seria, por exemplo, tomando-se um sistema de concessão de benefícios. Quando o usuário fosse solicitar seu registro no sistema, seria realizada uma identificação negativa – a princípio o sistema não conhece o usuário e só pretende verificar se ele não estaria tentando se registrar com outra identificação. No momento em que ele fosse receber o seu benefício, considerando que sua identidade não fosse previamente informada (neste caso o sistema realizaria uma verificação), o sistema buscaria na sua base de dados o template correspondente à amostra daquele usuário para determinar sua identidade, realizando então uma identificação positiva.

O processo de identificação é um processo um-para-muitos, onde o sistema tenta descobrir a identidade do usuário comparando a nova amostra submetida ao sistema com todos, ou parte, dos templates existentes na base de dados. Como resultado desta comparação, o sistema pode chegar a duas conclusões: se for encontrado algum template que possa ser considerado coincidente com a amostra fornecida, o usuário é considerado proprietário da identificação associada àquele template. Se nenhum template puder ser considerado coincidente com a amostra, o usuário é considerado desconhecido pelo sistema.

O processo de identificação requer um maior poder de processamento, uma vez que a comparação entre a nova mostra e um template é feita até que uma coincidência seja encontrada ou até o último template armazenado na base de dados.

Uma vez que a precisão da busca geralmente diminui com o aumento do número de registros comparados na base de dados, para identificação a partir de um grande número de templates normalmente é realizada alguma forma de categorização da base de dados. Esta categorização é feita subdividindo-se virtualmente a base de dados em partições a partir de alguma regra ou característica abrangente. Templates que sejam classificados numa mesma categoria são colocados na mesma partição da base de dados. Templates que não se enquadrem em nenhuma categoria podem ser colocados numa partição à parte. Quando a nova amostra é fornecida, ela também é classificada e, a partir do resultado desta classificação, somente um sub-conjunto da base de dados - a partição com os templates na mesma categoria da amostra - é percorrido [RUG 98].

O tamanho do template é importante para o particionamento da base de dados. Templates com tamanho muito pequeno possibilitam que haja registros idênticos, ou quase idênticos, em uma base de dados grande. Em geral, quanto maior for o tamanho do template, mais simples será a associação deste registro a uma determinada partição da base de dados. Também a base de dados poderá ser dividida em um maior número de partições se o tamanho do registro for grande, ou seja, existem maiores possibilidades de gerar partições distintas [RUG 98].

Uma outra forma de diminuir o número de templates comparados à nova amostra é a utilização de dados adicionais associados ao template que permitam algum outro tipo de classificação. Estes dados permitem a criação de filtros de busca que direcionam a

seleção dos templates que serão comparados. Estes dados poderiam conter, por exemplo, informações demográficas sobre a população-alvo do sistema. A identificação do sexo do usuário como "feminino", por exemplo, restringiria a comparação aos templates que tivessem esta mesma identificação de sexo [UNI 98].

3.6 Armazenamento de templates

A decisão sobre o local onde os templates dos usuários cadastrados devem ser armazenados no sistema biométrico vai depender diretamente do tipo da aplicação para qual o sistema está sendo planejado, dos requisitos de segurança desta aplicação, do dispositivo biométrico a ser utilizado, do tamanho do template e do número de pessoas que serão cadastradas no sistema [NEW 99] [POL 97].

Os templates podem ser armazenados de três formas: na memória do próprio dispositivo, em uma base de dados centralizada, ou ainda em formas de armazenamento externo, como cartões magnéticos.

3.6.1 Memória do dispositivo

Muitos dispositivos biométricos possuem memória própria na qual os templates podem ser armazenados. A capacidade desta memória varia de acordo com cada dispositivo, e alguns dispositivos permitem ainda que seja feito um upgrade para aumentar sua capacidade de armazenamento [NEW 99]. O armazenamento de templates na memória dos dispositivos aumenta a segurança do sistema, uma vez que os templates não são transmitidos ou armazenados em outro local. Também é econômico, pois não existe custo adicional com telecomunicações, processamento adicional, utilização de leitores de cartão ou fornecimento de cartões aos usuários. Permite ainda que seja realizada identificação de usuários. Mas esta solução não é indicada se a aplicação atende um grande número de usuários – maior que a capacidade de armazenamento do dispositivo – ou se estes usuários precisam ser verificados remotamente e em locais diferentes [POL 97].

3.6.2 Base de dados central

O número de templates que podem ser armazenados numa base de dados centralizada é limitado somente pela capacidade da máquina em questão. Esta solução é indicada para aplicações onde o número de usuários é grande demais para que os templates sejam armazenados na memória do dispositivo, quando é necessária verificação remota [NEW 99], ou ainda quando o sistema realiza identificação de usuários. Nesta solução, o template é transmitido entre o dispositivo e a base de dados (ou em sentido contrário, dependendo da arquitetura da aplicação). A segurança dos templates pode ser comprometida em função de abuso de privilégios na administração ou intrusão na base de dados, ou ainda por transmissão insegura para dispositivos remotos através de sistemas de telecomunicações e redes vulneráveis [POL 97].

3.6.3 Armazenamento externo

Em muitas aplicações, a movimentação dos usuários entre diversas localidades e a necessidade de um tempo de resposta pequeno para seu reconhecimento pelo sistema podem fazer com que a utilização de uma base de dados centralizada não seja a opção mais adequada. Em algumas aplicações, o número de usuários pode ser muito grande a ponto de não ser recomendada a utilização de uma base de dados centralizada. Para estas aplicações, a solução é armazenar os templates em algum dispositivo que permita que o usuário os carregue consigo [NEW 99]. Este tipo de armazenamento permite que os templates sejam transmitidos para o dispositivo biométrico de uma forma rápida e segura [POL 97]. Obviamente, para o caso de não existir em paralelo uma base de dados centralizada, não existe a possibilidade de realizar identificação de usuários.

Este tipo de armazenamento normalmente utiliza algum tipo de cartão magnético, e a definição do tipo mais indicado vai depender muito da aplicação e da quantidade e tipo de informações adicionais que devem ser armazenadas.

Smart–cards incorporam microprocessadores e oferecem um nível de segurança maior, porque possuem uma "zona secreta" que não pode ser acessada por nada além do próprio microprocessador do cartão. Este fato poderia permitir inclusive que a aplicação fosse desenvolvida de forma a não necessitar a transmissão da informação para fora do cartão – seria possível que fosse tratada pelo seu próprio microprocessador [NEW 99].

3.7 Avaliações relevantes

Nenhum sistema biométrico isolado é capaz de satisfazer completamente as necessidades de todas as aplicações. Cada sistema biométrico tem seus pontos fortes e suas limitações, que deverão ser avaliadas para verificar a adequação do sistema biométrico a cada aplicação particular.

Diversos ítens devem ser considerados para avaliar qual tipo de sistema biométrico pode ser considerado a melhor solução para uma determinada aplicação. A adequação do sistema biométrico à aplicação deve ser determinada pelas características da aplicação e pelas propriedades do próprio sistema biométrico. É importante que sejam avaliados pelo menos os seguintes ítens:

- PERFORMANCE: A precisão com que cada sistema biométrico verifica seus usuários pode ser decisiva para a determinação do tipo de tecnologia biométrica escolhida para a aplicação, e até mesmo de um produto específico. Algumas tecnologias biométricas são inerentemente mais precisas em rejeitar impostores do que outras, independente do valor limite imposto. Adicionalmente, o número de tentativas permitidas ao usuário para tomada de dados pode ser aumentado ou diminuído de forma a modificar a performance do sistema. Além disso, a performance do sistema melhora sensivelmente a partir do momento em que o usuário se sente mais confortável com a utilização do sistema e instintivamente aprende como realizar tomadas de dados com melhores resultados (isto é mais verdadeiro para alguns sistemas do que para outros; é muito mais difícil, por exemplo, conseguir uma imagem que não que não seja boa da retina do que uma de uma impressão digital).

- VULNERABILIDADE À FRAUDE: O grau de segurança do sistema biométrico também pode ser avaliado por sua capacidade de se proteger contra a utilização de técnicas fraudulentas. Estas técnicas incluem normalmente réplicas da característica biométrica, e os sistemas devem possuir mecanismos que possibilitem sua identificação. Por exemplo, um sistema de controle de presença identificando o locutor deveria ter mecanismos que impedissem que uma voz gravada fosse apresentada e aceita pelo sistema.

- ACEITAÇÃO DO USUÁRIO: A utilização do sistema biométrico não deve ser motivo de qualquer constrangimento ao usuário. Os padrões culturais, éticos, religiosos e higiênicos da sociedade à qual pertence o público alvo daquele sistema devem ser respeitados. O sistema também não pode ser socialmente desagradável. O dispositivo deve ser de utilização mais simples possível, conveniente, confortável e satisfazer os requisitos de segurança e privacidade dos usuários. Adicionalmente, o sistema biométrico não deve ser discriminatório. Idade, gênero, cor da pele, condições físicas ou profissionais não deveriam, teoricamente, ter qualquer influência na utilização do sistema [POL 97].

- TIPO DE BUSCA: A natureza da operação que o sistema biométrico vai realizar em sua base de dados também deve ser considerada. Aplicações que requerem a identificação de usuários em grandes bases de dados necessitam de sistemas biométricos escaláveis e características biométricas relativamente únicas.

- CONVENIÊNCIA DE USO: O tempo necessário para realizar as funções do sistema, como preparação do usuário, aquisição de dados, cadastramento, criação do template, comparação, autenticação ou identificação, deve ser o menor possível. O usuário deve realizar a menor quantidade possível de operações para ser verificado. Por exemplo, para um sistema de controle de acesso na entrada de uma empresa, na hora do início do expediente, um tempo de autenticação elevado poderia causar grandes transtornos. Além disso, sistemas que requerem concentração do usuário em ambientes estressantes podem ter sua performance prejudicada [POL 97].

- PÚBLICO ALVO: A escolha do sistema biométrico também pode variar se a aplicação for privada ou pública. Aplicações privadas são aquelas direcionadas a um público interno, composto de, por exemplo, funcionários de uma empresa. Em aplicações públicas o público alvo é externo, como por exemplo clientes desta empresa. A diferença está no fato de que, para aplicações privadas, a preocupação com a aceitação do sistema por parte do usuário não é tão relevante como em aplicações públicas. Em aplicações públicas, a aceitação do usuário pode ser vital. A insatisfação do usuário com determinado sistema, se ele se sente incomodado ou constrangido por um sistema intrusivo ou de difícil utilização, pode fazer com que ele simplesmente deixe de utilizar os serviços desta empresa [NEW 99].

- COOPERAÇÃO DO USUÁRIO: O usuário pode estar disposto ou não a cooperar com o sistema. O usuário cooperativo deseja ser reconhecido pelo sistema e colabora para que a tomada de dados seja a melhor possível, para diminuir a possibilidade de ser equivocadamente rejeitado pelo sistema. Usuários não cooperativos não estão dispostos a ser reconhecidos pelo sistema, e procuram uma forma de alterar sua característica biométrica no momento da tomada de dados. Aplicações que

envolvam usuários não cooperativos necessitam de características biométricas estáveis que não possam ser alteradas pelo usuário. Para estas aplicações, sistemas biométricos que utilizem, por exemplo, assinatura ou aparência do rosto, não devem ser considerados como melhor alternativa.

- REQUERIMENTOS DE ARMAZENAMENTO: Diferentes aplicações podem impôr limites no tamanho do espaço disponível para armazenamento dos templates. O dispositivo escolhido deverá levar em conta as características de armazenamento mencionadas no ítem 3.6.

- FUNCIONAMENTO DA APLICAÇÃO: Algumas aplicações necessitam que seu funcionamento se dê de forma não divulgada. Nem todos os dados biométricos podem ser capturados sem o conhecimento do usuário, e mesmo sistemas biométricos que permitam a tomada de dados sem que o usuário esteja ciente podem não ser indicados para aplicações em países que têm legislação atenta à privacidade do indivíduo.

- AUTOMATIZAÇÃO DA TOMADA DE DADOS: Uma aplicação pode ou não requerer um operador humano no estágio de aquisição do dado biométrico. Em aplicações remotas com ambiente não amigável ou inseguro, a utilização de sistemas biométricos que necessitem da assistência de um operador para a captura dos dados biométricos pode não ser viável.

- INTERFACE COM OUTROS SISTEMAS: Se o sistema precisar, agora ou no futuro, intercambiar dados com outros sistemas, sua arquitetura deve ser conhecida ou pelo menos pertencer a algum padrão estabelecido. Sistemas proprietários podem impossibilitar a troca de dados com outros sistemas.

- CUSTOS: Os custos de implementação de um sistema biométrico devem ser analisados cuidadosamente. Há alguns anos, o custo de implantação de um sistema biométrico era tão proibitivo que somente aplicações de alta segurança, onde o custo não era a maior prioridade, justificavam sua utilização [NEW 99]. Em consequência da maior utilização dos sistemas biométricos no mercado atualmente, os preços destes produtos tendem a cair, mas outros custos devem ser avaliados além dos custos iniciais de sensores ou software de comparação. Muitas vezes, o custo do suporte para administração do sistema durante seu ciclo de vida pode superar o custo inicial de hardware, por exemplo [CAM 99a].

4 Impressão Digital

4.1 Introdução

Impressões digitais são saliências em forma de linhas geralmente contínuas e que seguem um fluxo regular na pele dos dedos humanos, formando um padrão peculiar. Existem evidências arqueológicas que impressões digitais foram utilizadas como forma de identificação pelo menos desde 7000 a 6000 antes de Cristo pelos povos assírios e chineses. Potes de argila desta época algumas vezes continham impressões digitais marcando a cerâmica. Documentos chineses traziam um selo de argila marcado pela impressão do polegar de seu criador. Tijolos utilizados na antiga cidade de Jericó tinham estampados pares de impressões digitais dos polegares do oleiro. Mas, mesmo a individualidade das impressões digitais tendo sido reconhecida, não existem evidências que foram utilizadas como fundamento para identificação em larga escala em nenhuma destas sociedades [OGO 99].

Apesar de a história das impressões digitais datar de tempos antigos, a base das técnicas modernas de comparação de impressões digitais pode ser datada de 1684. Neste ano, Nehemiah Gruw, da Royal Society em Londres, observou pela primeira vez que as impressões digitais de cada indivíduo eram diferentes e que poderiam ser classificados por alguns padrões-chave. Nos sistemas atuais, além destas classificações principais, as impressões digitais também são classificadas por características menores, chamadas *minutiae*, que ocorrem nas terminações e ramificações das saliências na impressão digital [NEW 99] .

A classificação sistemática de impressões digitais começou durante a ocupação britânica da Índia no século XIX . Um dos primeiros usuários de impressões digitais para identificação foi Edward Henry, que, durante sua estada no Indian Civil Service, introduziu a identificação dos trabalhadores da construção da estrada de ferro através de impressão digital, com a finalidade de impedir que cada trabalhador recebesse mais de um pagamento. Hoje, os principais usuários de sistemas de identificação por impressões digitais são as entidades policiais do mundo todo [NEW 99].

As impressões digitais de suspeitos tradicionalmente eram coletadas utilizando-se uma tinta especial e um cartão com dez divisões, uma para a impressão de cada dedo. Mas, em lugar da utilização de tinta, sistemas disponíveis atualmente permitem o registro de impressões digitais eletronicamente – estes sistemas são conhecidos como “live-scan” – e as imagens das impressões digitais podem ser impressas diretamente no cartão padrão quando necessário. Desde o final dos anos 60, o FBI (US Federal Bureau of Investigation) automatizou o processo de checagem de impressões digitais de cenas de crime com as mantidas em seus registros [NEW 99] .

A partir dos anos 80, inovações nas áreas tecnológicas de computadores pessoais e scanners ópticos possibilitaram que a utilização de impressões digitais se tornasse ferramenta prática em aplicações não criminais. Mais recentemente, dispositivos de leitura de impressões digitais com custo mais baixo e o desenvolvimento de algoritmos de comparação rápidos e confiávies permitiu a maior disseminação desta tecnologia e sua uitlização em diversas áreas.

Existem dois mercados distintos para sistemas automáticos de impressão digital: as aplicações forenses e as aplicações padrão dos sistemas biométricos para autenticação e identificação de indivíduos. O tipo de sistema utilizado para aplicações forenses é bem diferente daqueles de outras áreas de aplicação. Aplicações forenses envolvem a checagem da totalidade, ou parte, de uma impressão digital contra uma grande base de impressões completas previamente armazenadas.

Para aplicações forenses, existem duas atividades primárias que utilizam impressões digitais para propósitos de identificação. A primeira é o processo de coletar impressões de cada um dos dez dedo do suspeito e compará-las com arquivos existentes para identificação e determinar codinomes, detenções anteriores, etc. Este processo é tradicionalmente feito visualmente por técnicos treinados que examinam a impressão digital para determinar seu tipo básico padrão, e a partir desta classificação observar detalhes menores como as terminações e bifurcações das saliências e o número de saliências entre pontos distintos. Os arquivos contendo impressões dos dez dedos correspondentes são então pesquisados manualmente em busca de uma coincidência. Este sistema, apesar de adequado, requer uma considerável capacidade de trabalho humano para obter resultados adequados [NEW 99] .

A segunda atividade em aplicações forenses é a coleta de impressões digitais latentes deixadas na cena do crime e sua comparação com os arquivos de impressões dos dez dedos em busca de uma coincidência. Esta atividade é extremamente complexa para o investigador porque, se o suspeito já não tiver sido identificado de alguma outra forma, o investigador pode não ter noção de por onde iniciar a busca. Adicionalmente, muitas vezes a impressão latente encontrada na cena do crime é somente parcial. Para que uma impressão digital possa ser utilizada como evidência para a Justiça, um certo número de características da impressão digital encontrada na cena do crime deve coincidir com aquelas encontradas na impressão digital do suspeito. Este número de características coincidentes varia de país para país [NEW 99]. Numa típica imagem de impressão digital, existem em média de 30 a 40 *minutiae*. O FBI americano provou que não existem dois indivíduos com mais de 8 *minutiae* coincidentes. Para a Corte de Justiça americana, são consideradas como pertencentes à mesma pessoa impressões digitais com coincidência mínima de 12 *minutiae* [RUG 98] [DOH 98].

Os sistemas utilizados para aplicações forenses (os AFIS - Automatic Fingerprint Identification Systems) são bastante diferentes dos utilizados para aplicações biométricas padrão. Estes sistemas de identificação de impressões digitais executam suas funções automaticamente e sua utilização está bastante difundida nas forças policiais do mundo todo, com o objetivo de aumentar a produtividade e a segurança no processamento de impressões digitais. Estes sistemas operam a partir de uma impressão digital encontrada na cena do crime, ou um novo cartão preparado com a impressão digital do suspeito, comparando-os com cada outro registro de impressões digitais armazenado no sistema. Isto permite a geração de, por exemplo, uma lista com possíveis suspeitos que tenham impressões digitais similares. Para que isto seja possível, os AFIS armazenam a imagem real da impressão digital completa, e não algum template criado a partir da impressão digital [NEW 99].

Por outro lado, os sistemas biométricos utilizados para verificação através de impressão digital utilizam o processo padrão de todos os sistemas biométricos similares,

armazenando a característica biométrica na forma de detalhes específicos extraídos da impressão digital. A recriação da impressão digital original a partir deste template é impossível, o que faz este tipo de sistema ser inútil para aplicações forenses [NEW 99].

4.2 Descrição da característica

O extenso histórico de utilização de impressões digitais para fins de identificação é um bom indicador de confiabilidade que os outros tipos de biométricos ainda não têm. Existe a experiência de um século de utilização em aplicações forenses e centenas de milhões de impressões digitais comparadas pela qual é possível afirmar com alguma autoridade que impressões digitais são únicas e sua utilização para afiançar a identidade de um indivíduo é extremamente confiável [NEW 99].

A formação das impressões digitais na pele dos dedos depende das condições iniciais do desenvolvimento embrionário [OGO 99]. Na área da impressão digital são encontradas diversas representações das características gerais do fluxo das linhas digitais, como arcos, laços e espirais, e características mais dintintivas, como as terminações e bifurcações destas linhas [NEW 99].

Em meados do século XIX, estudos científicos se propuseram a estabelecer duas características críticas das impressões digitais que são verdadeiras até hoje: não existem duas impressões digitais produzidas por dedos diferentes que tenham o mesmo padrão de linhas digitais, e, apesar do tamanho das impressões digitais sofrer alterações durante o processo de crescimento do indivíduo, estes padrões são imutáveis durante toda sua vida. E foram estes estudos que levaram à utilização de impressões digitais para identificação criminal, primeiro na Argentina em 1896, então na Scotland Yard em 1901, e em outros países no início do século XX [OGO 99].

As linhas que fluem em vários padrões através da pele dos dedos são chamadas *saliências* e os espaçoes entre estas saliências são *vales*. A configuração destas saliências são comparadas entre uma impressão digital e outra para verificar se estas impressões são coincidentes ou não. Impressões digitais são normalmente comparadas a partir de uma (ou ambas) de duas aboradagens associadas às suas características e que são descritas abaixo.

A forma mais geral de classificação de impressões digitais é através da comparação de seu padrão global. Este padrão é determinado pelo o fluxo de linhas através da impressão digital e são basicamente classificados em arco, laço e espiral. Estes padrões podem ser vistos na Figura 4.1. Algumas impressões digitais podem não ser classificadas em nenhuma classe, ou ainda ter atributos de diversas classes [UNI 98]. Diferentes esquemas de classificação podem categorizar as impressões digitais em até em torno de 10 classes diferentes [OGO 99] [KAL 96].

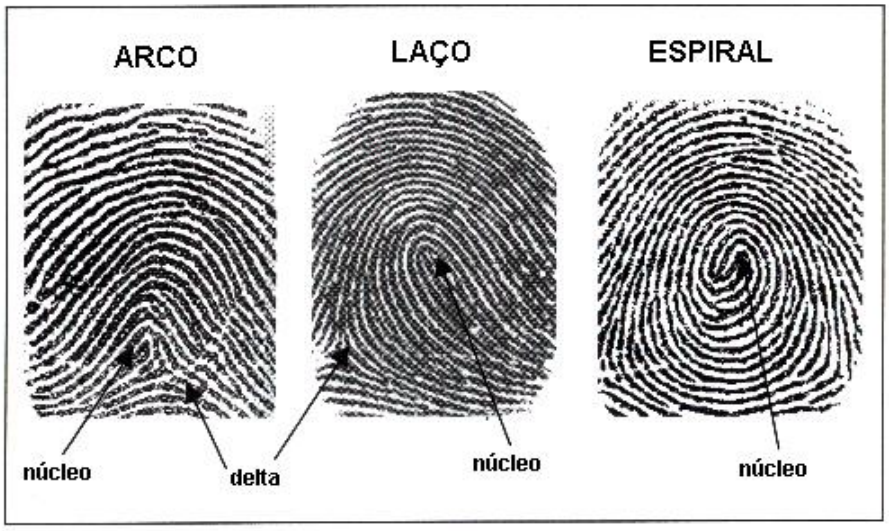

Figura 4. 1 - Padrões de impressão digital

A mais microscópica das abordagens é a utilização de *minutia*. Os dois tipos de *minutiae* encontrados em uma impressão digital são a terminação e a bifurcação, como mostra a Figura 4.2. As terminações são encontradas em pontos onde a linha da impressão digital inicia ou termina. A bifurcação acontece no ponto em que uma linha única se subdivide em duas ramificações, numa junção em forma de Y. Para fins de comparação, os sistemas biométricos que utilizam *minutia* atribuem a cada uma valores como tipo (terminação ou bifurcação), localização (coordenadas x e y), e direção [OGO 99], entre outros.

Algumas vezes ainda duas outras características podem ser consideradas no processo de comparação de impressões digitais: o *núcleo* e o *delta*. O núcleo pode ser entendido como o centro do padrão da impressão digital. O delta é um ponto único onde três padrões se desviam. Estas características também podem ser vistas na Figura 4.1. As localizações do núcleo e do delta podem ser utilizadas como auxílio à orientação de duas imagens de impressão digital para comparação posterior, mas estas características não estão presentes em todas as impressões digitais.

Figura 4. 2 - *Minutiae*: terminação e bifurcação

Existem ainda outras características através das quais impressões digitais poderiam ser comparadas. Alguns sensores, por exemplo, são capazes de reconhecer poros na pele dos dedos e existem estudos sobre a utilização de sua localização para comparação da mesma forma que são utilizadas as *minutiae*.

4.3 Funcionamento do sistema

4.3.1 Aquisição da imagem

A imagem da impressão digital pode ser capturada de duas formas: através de um dispositivo de captura específico (live-scan) (Figura 4.3) ou por meio da digitalização de uma impressão digital previamente impressa.

Figura 4.3 - Exemplo de dispositivo de captura de impressão digital

(Sony Fingerprint Identification Unit – FIU-001/500)
(Fonte: I/O Software Inc. [IOS 00])

A digitalização de uma impressão digital já impressa não deveria ser utilizada em sistemas biométricos de verificação que utilizam impressão digital, uma vez que a principal finalidade destes sistemas é reconhecer um usuário no momento em que ele se apresenta ao sistema. Este processo somente teria sentido no momento de geração do template e, ainda assim, a imagem seria deteriorada pelo próprio processo original de captura, com utilização de tinta, e pelo processo de digitalização. Este processo, então, só é realmente válido para cadastramento de indivíduos em sistemas AFIS. Os sistemas biométricos de verificação utilizam dispositivos de captura de imagem em tempo real.

Nos dispositivos ópticos de captura, uma luz laser ilumina a impressão digital posicionada numa superfície de vidro, e a reflectância desta luz é capturada por uma câmera digital. A quantidade de luz refletida vai depender da altura das saliências, da profundidade dos vales e da oleosidade da pele que está em contato com o vidro. A luz que passa através do vidro e incide nos vales não é refletida, e a luz que incide nas saliências que estão em contato com a superfície do vidro (mais precisamente, na oleosidade contida nas saliências, que vai funcionar como um selo entre a saliência e o vidro) é refletida [OGO 99].

Fibras ópticas também foram propostas para capturar imagens de impressões digitais. Um feixe de fibras ópticas é posicionado perpendicularmente à superfície do dedo, iluminando o dedo e detectando a reflexão da luz para construir a imagem. Microprismas que mudam de posição quando em contato com a pele do dedo também foram propostos [OGO 99].

Sensores de temperatura também podem ser utilizados e consideram o diferencial de temperatura entre as saliências que tocam a superfície do dispositivo e os vales, que se encontram mais distantes. Em sensores de ultrasom, a imagem é formada através da captura de sinais ressonantes pelo receptor. Este tipo de sensor é menos afetado por sujeira e acúmulo de oleosidade do que os sensores ópticos.

4.3.2 Processamento da imagem

A imagem utilizada para extração das características da impressão digital deve ser a melhor possível, para que a coincidência entre duas impressões digitais possa ser corretamente avaliada. Após a captura da imagem, algum tipo de processamento de imagem deve ser realizado, com o objetivo de minimizar possíveis erros inerentes a este processo.

A imagem da impressão digital é um dos tipos de imagem com maior probabilidade de apresentar elementos não pertinentes à própria característica. Estes ruídos na imagem acontecem porque nossos dedos são nossa forma direta de contato com o mundo exterior na maioria das tarefas que executamos rotineiramente, e as extremidades dos dedos facilmente ficam sujas, ressecadas, úmidas, com cortes ou cicatrizes, enrugadas ou desgastadas. A fase de processamento da imagem é utilizada para reduzir os ruídos causados por estas alterações e melhorar a definição das linhas da impressão digital, ressaltando as saliências contra os vales [OGO 99].

A primeira operação executada na imagem é a aplicação de um filtro para a correção do fluxo das linhas da impressão digital. Existe uma característica muito útil nas impressões digitais que é a redundância das linhas paralelas. Mesmo que haja descontinuidade em algumas linhas em particular, é possível analisar uma pequena área em torno destas linhas e determinar seu fluxo. Utiliza-se esta redundância de informação para projetar um filtro, que é aplicado a cada pixel da imagem. Baseado na orientação das linhas em torno de cada pixel, a aplicação do filtro corrige a orientação das linhas no pixel em questão, orientando-as segundo a orientação das linhas da mesma localização. Isto significa que qualquer ruído na imagem que acarrete numa suposta diferença de orientação das linhas da impressão digital será virtualmente ignorado.

Após o processo de melhoria da imagem e redução de ruídos, a próxima operação realizada na imagem é a binarização. Apesar de as linhas da impressão digital se apresentarem na imagem em várias gradações de intensidade na escala de cinza, sua informação é essencialmente binária: são linhas contra o fundo. A informação da imagem deve então ser simplificada para esta representação binária para facilitar o processamento subsequente. A operação de binarização da imagem pega uma imagem em vários tons de cinza e retorna como resultado uma imagem binária. A imagem é

reduzida da intensidade original de 256 (pixels de 8 bits) para 2 (pixels de 1 bit) [OGO 99].

Diferentes imagens de impressões digitais não possuem as mesmas características de contraste, tornando o processo de binarização complexo. O contraste pode ainda variar dentro de uma mesma imagem, como, por exemplo, quando o dedo é pressionado com mais intensidade no centro. Desta forma, não é possível determinar um valor único na escala de cinza a partir do qual a informação é considerada saliência ou não. Para equacionar este problema, é determinado um valor limite adaptativamente às intensidades dos tons de cinza da imagem, e a partir dete valor são comparados todos os pixels, determinando se ele estaria ou não representando uma saliência.

A última operação de processamento da imagem normalmente realizada antes da detecção de *minutiae* é o estreitamento das linhas da impressão digital. Este processo reduz a largura da linha a um único pixel e vai facilitar a posterior detecção das terminações e bifurcações. Métodos de estreitamento eficientes conseguem reduzir a largura das linhas mantendo sua conectividade e minimizando o número de informações artificiais introduzidas devido ao próprio processo. Estes informações artificiais são compostas basicamente por falsas bifurcações com ramificações muito curtas, que são na verdade causadas por descontinuidade nas linhas devidas ao processo de estreitamento, e são removidas através do reconhecimento da diferencça entre *minutiae* legítimas e falsas no estágio de extração das características.

As operações de processamento de imagem são operações que geralmente consomem muito tempo, o que faz com que muitos sistemas sejam projetados para não executar estas operações com o objetivo de alcançar resultados de comparação mais rápidos. Esta não é uma solução recomendável, uma vez que os resultados das operações subsequentes depende da qualidade da imagem resultante. A supressão de operações para melhorar a imagem obtida pode acarretar em degradação nos resultados das comparações, resultando em um possível aumento do número de falsas rejeições e fazendo com que o usuário tenha que apresentar a amostra mais vezes.

4.3.3 Extração das características

As *minutiae* da impressão digital são encontradas a partir da imagem com largura das linhas reduzida, no estágio de extração das características. As terminações são encontradas nos pontos onde as linhas terminam, e as bifurcações são encontradas em junções de três linhas [OGO 99].

Aparentes *minutiae* adicionais são encontradas devido ao ruido da imagem original ou às informações artificias introduzidas durante as operações de processamento da imagem. Estas características adicionais podem ser eliminadas utilizado-se limites determinados empiricamente. Por exemplo, uma ramificação com tamanho muito inferior a um determinado comprimento deve ser eliminada porque é possivelmente ruído. Duas terminações muito próximas, em direções opostas, indicam possivelmente uma descontinuidade de uma linha devido a cicatriz, ruído ou ressecamento da pele. Terminações nos limites da impressão digital são eliminadas porque são, na verdade, o contato da impressão digital com o dispositivo de captura.

Para cada *minutia* válida encontrada são determinados atributos, que podem ser classificação da *minutia* (terminação ou bifurcação), posição (coordenadas x e y), e orientação da terminação ou bifurcação [OGO 99]. O resultado da fase de extração de características é o template, composto por uma lista das *minutiae* acompanhada de valores para seus atributos.

4.3.4 Comparação

A principal dificuldade para a comparação de duas impressões digitais é o alinhamento de suas *minutiae*. Uma das primeiras formas para facilitar a comparação é a utilização do conceito de vizinhança. Grupos de *minutiae* vizinhas são identificados na impressão digital, normalmente 2 a 4 *minutiae* por vizinhança, e cada uma dessas vizinhanças é comparada contra possíveis vizinhanças de outra impressão digital [OGO 99].

Cada uma das *minutiae* de uma vizinhança está localizada a uma certa distância e orientação relativas das outras, e também possui suas próprias informações de tipo e direção. Todas estas informações são comparadas, e se a comparação resultar em apenas pequenas diferenças entre as duas vizinhanças comparadas, elas são consideradas coincidentes. Este procedimento é feito exaustivamente para todas as combinações possíveis de vizinhanças e, se forem encontradas tantas vizinhanças coincidentes quanto necessário, estas impressões digitais também serão consideradas coincidentes. Para o processo de comparação deve-se levar em conta que a pele é uma superfície elástica, de forma que as distâncias e direções relativas entre as *minutiae* podem variar.

O processo de comparação de todas as combinações de vizinhanças possíveis entre duas impressões digitais em geral consome muito tempo, e métodos adicionais foram propostos para alinhar as impressões digitais e reduzir o número de comparações. Um método comum, que é o mesmo utilizado para comparação visual, é localizar o núcleo e o delta e alinhar as impressões digitais com base nestas características.

4.4 Limitações da tecnologia

A qualidade da impressão digital varia de acordo com o gênero, cor da pele, ocupação e idade do indivíduo. Mulheres normalmente têm impressões digitais menos definidas que as dos homens. A leitura das impressões digitais de pessoas com pele mais clara pode ser feita com mais facilitade, tornando-se tão mais difícil quanto mais escura for a pele do indivíduo [NEW 99].

O processo de envelhecimento torna a pele dos dedos mais rígida. Pessoas mais jovens em geral têm a pele mais macia, tornando-se necessário que o dedo seja pressionado contra o dispositivo de leitura com mais intensidade para conseguir uma imagem melhor. Os sistemas devem ser capazes de lidar com estas variações de pressão contra os dispositivos.

A condição geral das mãos também afeta a performance do sistema [POL 97]. Algumas atividades manuais podem fazer com que as saliências da impressão digital sejam desgastadas ou sofram danos. Produtos químicos ou abrasivos e desgaste na pele da ponta dos dedos podem fazer com que a impressão digital se torne tênue e de difícil

leitura pelos dispositivos. Indivíduos com ausência de dedos obviamente não poderão ser verificados por estes sistemas.

Sujeira, oleosidade, umidade e ressecamento da pele podem obscurecer detalhes mais delicados. Para trabalhadores manuais isto pode ser um empecilho para a boa performance do sistema. Impressões digitais latentes, ocasionadas por resíduos de oleosidade deixados na superfície do sensor por uma impressão digital previamente apresentada, também podem confudir o sistema. Sistemas que utilizam ultrassom para a aquisição da imagem da impressão digital podem solucionar este problema.

A forma com que o usuário interage com o dispositivo também pode afetar a performance do sistema. Pressão exagerada do dedo contra o dispositivo de leitura pode causar distorções na imagem [ROE 98]. O posicionamento do dedo no dispositivo de forma muito diferente daquela em que o usuário foi originalmente registrado também pode fazer com que a impressão digital não seja comparada corretamente.

Em ambientes de trabalho onde é necessária a utilização de luvas, como laboratórios químicos, fábricas e hospitais, a utilização de sistemas de leitura de impressõs digitais, dependendo da situação, pode se tornar extremamente inconveniente, pois os dedos não estarão constantemente disponíveis para a apresentação da amostra ao sistema [POL 97].

Finalmente, pela sua utilização bastante difundida em aplicações forenses, a utilização de impressões digitais para fins de identificação poderia estar acompanhada do estigma de criminalidade, causando resistência por parte do público em geral. A utilização cada vez maior deste tipo de sistema em aplicações fora da área criminal pode ter diluído esta preocupação e a tendência é que este preconceito venha a diminuir.

4.5 Proteção contra fraudes

Existem várias formas possíveis de a segurança de um sistema de verificação por impressão digital ser comprometida. A apresentação de um dedo amputado de um usuário autorizado - o método preferido pelos filmes de horror - é a forma mais pueril de tentativa de reconhecimento fraudulenta [NEW 99]. Métodos mais avançados de fraude incluem a criação de modelos realistas dos dedos ou a utilização de uma fina camada de algum material reproduzindo uma impressão digital legítima colocada por sobre o dedo de um usuário não autorizado.

Alguns sistemas incorporam mecanismos que possibilitam a verificação de que o que está sendo apresentado ao sistema é um dedo real, com tecido vivo. Estes mecanismos avaliam característcas como o calor do corpo, a capacitância da pele e o nível de oxigênio na ponta dos dedos [NEW 99].

5 Geometria da Mão

5.1 Introdução

Antropologistas sugerem que a raça humana sobreviveu e se desenvolveu devido ao grande tamanho do nossos cérebros e aos nossos polegares opostos. A mão humana é versátil e nos permite segurar e arremessar objetos, e criar e manipular ferramentas.

A identificação do indivíduo através da utilização de suas mãos pode se dar através do padrão de veias do dorso das mãos, da impressão de suas palmas, e por características da sua geometria.

As primeiras aplicações para os leitores de geometria da mão foram componentes para controle de acesso físico. Um dos primeiros de todos os sistemas biométricos media os comprimentos dos dedos. Se chamava IdentMat, e foi lancado no início dos anos 70 pela Identimation. Sua produção cessou em 1987.

Apesar de este ser um tipo de sistema biométrico largamente utilizado no mundo todo, pouca bibliografia é encontrada sobre o desenvolvimento de sua tecnologia.

5.2 Descrição da característica

Cada mão humana é considerada única, e suas dimensões físicas contém informações que são capazes de autenticar a identidade de um indivíduo. O comprimento dos dedos, largura, espessura, curvatura e a localização de características podem distinguir cada ser humano de outra pessoa [ZUN 99].

Após o nascimento, as mão humanas são quase exatamente simétricas. Com o crescimento do corpo, as mãos vão sofrendo alterações devidas às proprias alterações no corpo e a fatores ambientais. O fato de uma pessoas se tornar canhota ou destra, por exemplo, faz com que uma mão seja ligeiramente maior que a outra. A mão favorecida normalmentente é mais suscetível a danos, por ser a mão mais utilizada para as atividades rotineiras.

O formato da mão, depois de uma certa idade, não sofre grandes alterações. As mãos de pessoas mais jovens, especialmente crianças, se modificam mais rapidamente devido ao crecimento do corpo, e as mão de pessoas mais velhas também sofrem alterações devidas ao prórprio processo de envelhecimento, e a algumas doenças, como artrite. Alterações de peso também acarretam mudanças no formato da mão, como no resto do corpo.

5.3 Funcionamento do sistema

Vários métodos são conhecidos e utilizados para efetuar medidas e avaliar a geometria das mãos. Estes métodos geralmente estão em uma de duas categorias: mecânica ou detecção do cotorno da imagem. Atualmente, os sistemas biométricos que utilizam a

geometria da mão estão baseados em detecção do cotorno da imagem através de leitores ópticos.

Os leitores de geometria da mão utilizam uma câmera digital e diodos de emissão de luz, com espelhos e refletores, para capturar imagens em preto e branco da silhueta da mão. Os leitores não registram detalhes da superfície da mão, ignorando impressões digitais, linhas e cicatrizes. Combinando um espelho lateral e um refletor, a parte óptica do sistema produz duas imagens distintas, uma do topo e outra lateral, o que torna possível obtenção de informacões tri-dimensionais da mão [ZUN 99]. Uma exemplo destas imagens pode ser visto na Figura 5.1.

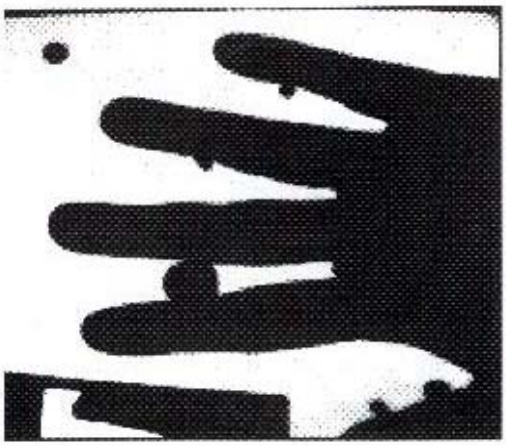

Figura 5. 1 - Imagem da silhueta da mão

No sistema mais difundido no mercado, o ID3D da Regognition Systems Inc. [REC 99], o processo de criação do template solicita que o usuário apresente sua mão ao leitor três vezes, tomando um imagem diferente a cada vez que a mão é posicionada no dispositivo. Leituras múltiplas permitem que sejam capturadas imagens da mão em posições ligeiramente diferentes. A partir destas imagens, o sistema registra 96 medidas da mão do usuário em cada imagem, calculando matematicamente médias destas medidas, e criando um template de 9 bytes. O sistema completo ID3D é mostrado na Figura 5.2.

Para o posicionamento correto da mão no dispositvo, de forma a permitir a tomada de uma imagem correta, o sistema possui guias, na forma de pinos projetados da superfície da sua placa. Estes pinos vão ajudar o usuário a posicionar sua mão corretamente [OGO 99]. No sistema de leitura de geometria da mão produzido pela Identification Systems Dermalog, o posicionamento da mão é livre [DER 99].

Alguns sistemas permitem a utilização de ambas as mãos para a tomada das imagens, mas os dispositivos comerciais de verificação de geometria da mão normalmente são projetados para a utilização da mão direita com a palma para baixo. Mas, como estes sistemas capturam somente informações do formato da mão, e não detalhes de sua

superfície, é possível cadastrar o usuário com a mão esquerda com a palma para cima, considerando que a geometria de cada mão é normalmente uma imagem espelhada da outra mão.

Figura 5. 2 - ID3D HandKey Reader

(Fonte: Recognition Systems Inc. [REC 99])

5.4 Limitações da tecnologia

Idealmente, o posicionamento da mão dispositivo durante o registro e a verificação devem ser idênticos. O posicionamento do dispositivo em diferentes alturas alteram a posição relativa do corpo e da mão, podendo acarretar alterações no formato da mão tomado pelo sistema. Realizar o registro com o dispositivo em determinada altura e a verificação em outra pode causar diferença suficiente no formato da mão para que o usuário seja rejeitado pelo sistema. Assim, o leitor utilizado para o registro do usuário deve ter a mesma altura que o utilizado para sua verificação. Da mesma forma, a posição relativa do corpo pode causar influência no formato da mão registrado pelo sistema. Se o usuário estiver frequentemente de pé no momento da sua verificação, é aconselhável que seu cadastramento também seja feito na mesma posição [OGO 99].

Durante o processo de tomada de imagens, acessórios como anéis e pequenas bijuterias não são entendidos pelo sistema como fazendo parte da geometria da mão, uma vez que as medidas são em geral tomadas nos nós dos dedos. Mas anéis largos utilizados

eventualmente podem causar erros na leitura da geometria da mão [POL 97]. Sujeira, gordura, cicatrizes e outras características superficias não afetam esta leitura.

Grandes alterações de peso entre uma leitura e outra podem fazer com que o usuário autorizado seja rejeitado pelo sistema, uma vez que o sistema não acompanhou o processo gradativo de alteração de peso e consequentemente não realizou a atualização dos templates.

Pessoas com mãos reumáticas, artrite ou doenças como mal de Parkinson quase sempre encontram dificuldades na utilização do sistema, tanto por problemas na própria identificação correta da geometria da mão quanto no posicionamento correto da mão no leitor.

A falta de um ou dois dedos geralmente não se torna um problema, porque de uma maneira geral os dispositivos podem trabalhar tomando medida de apenas quatro ou três dedos. Mas pessoas com amputações das mãos ou de todos os dedos da mão, ou ainda com defeitos de nascença que acarretem dificuldade de posicionar a mão no dispositivo devem ter outros meios de verificação disponíveis [OGO 99].

Os sistemas biométricos que utilizam geometria da mão têm em geral boa aceitação por parte dos usuários. A única excessão parece ser no mercado japonês, onde os usuários têm resistência em tocar, ou colocar a mão, em algum lugar onde outra pessoa já tenha posto a sua [NEW 99].

Estes sistemas não são indicados para base de dados muito grandes, pois o pequeno tamanho do seu template não permite a divisão da base de dados com grande número de registros em um grande número de partições com um pequeno número de registros por partição [RUG 98].

5.5 Proteção contra fraudes

Modelos sofisticados reconstruindo a estrutura óssea da mão de um usuário autorizado poderiam possuir potencial para enganar estes sistemas. Mas, além de terem que contar com a virtual colaboração do usuário autorizado para a execução deste modelo, é improvável que eles possam ser feitos suficientemente reais [NEW 99] [POL 97].

6 Face

6.1 Introdução

A face é o principal componente no processo onde os seres humanos lembram e reconhecem uns aos outros, o que faz com que o reconhecimento da face seja o meio mais natural de identificação biométrica. O reconhecimento de faces é uma das mais notáveis capacidades do cérebro humano, e esta capacidade é desenvolvida durante o período de infância, se tornando essencial em diversos aspectos das relações sociais humanas. Em conjunto com outras habilidades relacionadas, como a percepção e interpretação de expressões faciais, o reconhecimento de faces pelos seres humanos é um processo extremamente complexo e instigante.

Os sistemas biométricos que utilizam reconhecimento de face são não-intrusivos, podendo inclusive operar sem o conhecimento dos usuários. A utilização frequente de câmeras em locais para controle de segurança pode explicar em parte a grande aceitação deste tipo de sistema biométrico. E, na nossa sociedade, onde os indivíduos estão habituados à utilização de fotografias para documentos pessoais, é claro que a identificação pela face seja considerada natural, uma vez que esta é uma forma tradicional de identificação oficial [POL 97].

O reconhecimento de faces, até pouco tempo, não era tratado como uma ciência, e era subjetivo por natureza. Peritos policiais se tornavam artistas e tentavam categorizar diferentes partes da face em conjuntos de padrões que podiam ser reunidos formando uma imagem que poderia ser semelhante à face da pessoa em questão. Este processo, apesar de subjetivo, aborda um dos principais problemas do procedimento computacional para reconhecimento de faces, que é a determinação de quais processos são realizados pelo cérebro humano no momento do recohecimento de uma face.

6.2 Descrição da característica

A capacidade humana de reconhecer faces é uma característica extremamente complexa e instigante que tem sido objeto de muitos estudos.

Apesar de ser impossível, com a tecnologia existente, elaborar máquinas com o poder da capacidade do sistema visual humano, este é um bom ponto de referência para estudos de simulação computacional do reconhecimento de faces. Estudos nesta área realizados por neurocientistas e psiquiatras incluem a própria capacidade humana de reconhecer faces, a modelagem desta capacidade, a aparente modularidade do reconhecimento de faces, a facilidade humana no desenvolvimento desta capacidade, a utilização de características distintivas para o reconhecimento, a degradação da capacidade de reconhecer faces com o avanço da idade, e condições excepcionais que resultam da inabilidde para reconhecer faces, como a prosopagnosia [WEN 99].

Existem evidências que indicam que a capacidade humana de reconhecer faces é um processo dedicado, e não simplesmente uma aplicação do processo geral de

reconhecimento de objetos no cérebro, o que induz a acreditar que os sistemas de reconhecimento de faces também devem ser específicos.

A questão sobre quais características observadas pelos seres humanos são utilizadas no processo de reconhecimento de faces tem sido objeto de muito debate e o resultado de estudos relacionados tem sido utilizado no projeto de algoritmos de alguns sistemas. Crianças pequenas tipicamente reconhecem faces não familiares utilizando características não relacionadas, como óculos, roupas, chapéus e cabelo. Em torno dos 12 anos de idade, estas características são relativamente ignoradas e o foco passa a ser face propriamente. Condições psico-sociais também afetam a capacidade de reconhecer faces [WEN 99].

A emulação da capacidade humana de reconhecimento de faces é o principal objetvo da maioria dos sistemas de reconhecimento de faces.

6.3 Funcionamento do sistema

Os sistemas de reconhecimento de face podem ser utilizados em uma grande variedade de ambientes – de um ambiente totalmente controlado a um absolutamente sem controle. Num ambiente controlado, são tiradas fotografias frontais e de perfil da face, com fundo uniforme e poses idênticas. Estas imagens são comumente chamadas de "mugshots", pois são fotografias tiradas em uma pose fixa e artificial. Cada uma destas fotografias é processada de modo a extrair-se uma subparte dela, a imagem canônica da face. Nesta imagem, o tamanho e a posição da face são aproximadamente normalizados para valores predefinidos e a região de fundo é minimizada. Técnicas que utilizam este tipo de imagem já forma desenvolvidas com sucesso para diversos sistemas de reconhecimento de face [WEN 99].

Mas, de uma maneira geral, o reconhecimento de faces, como o realizado pelos seres humanos em seu cotidiano, acontece em ambientes virtualmente não controlados. Sistemas que reconhecem faces em ambientes não controlados devem em primeiro lugar detectar as faces na imagem. Uma determinada imagem pode ou não conter faces; se elas existirem, sua localização e suas tamanhos devem ser identificados. O reconhecimento de faces em ambientes não controlados é extremamente complexo: mais de uma face pode estar presente na imagem, condições de iluminação podem não ser homogêneas, as expressões faciais podem variar bastante, as faces podem aparecer em diferentes escalas, posições e orientações, características impostas como barba e maquiagem podem esconder características faciais úteis para sua localização e reconhecimento, ou a face pode estar ainda parcialmente encoberta.

A tecnologia de reconhecimento de faces está sendo desenvolvida a partir de diversas áreas distintas, entre elas redes neurais, métrica facial e *eigenfaces*.

Sistemas de reconhecimento de faces que utilizam métrica facial trabalham a partir da determinação de características geométricas da face, como distâncias e ângulos entre pontos como os cantos dos olhos, as extremidades da boca, narinas e queixo, e a relação entre estas medidas. A atividade mais crítica neste processo é a normalização adequada da imagem. As características devem ser normalizadas de alguma forma para que sejam independentes de posição, rotação e escala no plano da imagem. Algoritmos

desenvolvidos [BRU 93] consideram como base a localização dos olhos na imagem para sua normalização, aproveitando sua determinação para estipular o eixo de simetria da face. A partir deste ponto, é possível ajustar a escala e rotação da face, e ainda localizar seus outros componentes geométricos.

Recentemente, estudos vêm sendo realizados no sentido de categorizar faces de acordo com o seu grau de adequação num conjunto de *eigenfaces*, obtidos através da análise matemática denominada *local feture analisys* (LFA). Este mecanismo é baseado na consideração de que todas as imagens faciais podem ser sisntetizadas a partir de um conjunto fixo e conhecido de características. Em outras palavras, as imagens faciais podem ser decompostas em pequenos subconjuntos de características, que são chamadas *eigenfaces*, e que podem ser entendidos como os componentes principais das imagens originais. Cada face pode ser associada a um grau de adequação a cada um de do conjunto de *eigenfaces* definidos, e é possível analisar a face a partir de somente os 40 *eingenfaces* com maior pontuação, garantindo 99% de precisão. Este processo é relativamente semelhante ao realizado por peritos policiais para a elaboração de retratos falados, com a diferença de que a informação é derivada da análise computacional de uma imagem digital.

6.4 Limitações da tecnologia

Apesar de evolução na tecnologia de reconhecimento de faces, a maior parte dos sistemas ainda sofre do mesmo problema básico: as fotografias tomadas no momento do cadastramento apresentam o indivíduo em uma pose artificial. É extremamente difícil realizar uma comparação válida e qualquer outra imagem que não seja também um "mugshot". Adicionalmente, estes sistemas muitas vezes não estão preparados para lidar com alterações angulares na posição da face ou expressões faciais diferentes daquelas utilizadas durante o processo de cadastramento.

Uma vez que estes sistemas utilizam imagens da face obtidas a partir de luz visível, eventualmente características da face poderão não ser distinguíveis em função de más condições de iluminação.

Gêmeos idênticos ou pessoas extremamente parecidas podem confundir o sistema e causar falsa aceitação. Características impostas, como barba, estilo da cabelo e óculos também podem confundir o sistema e causar falsa rejeição.

A face é uma característica humana que pode variar bastante, inclusive pelo próprio processo gradativo de crescimento do corpo. Os templates devem ser atualizados com frequência para acompanhar estas mudanças.

6.5 Proteção contra fraudes

Idealmente, os sistemas de reconhecimento de face deveriam ser projetados para ser sufucuentemente robustos contra o reconhecimento equivocado de gêmeos idênticos ou pessoas extremamente parecidas.

Formas adicionais de fraudar o sistema poderiam incluir a apresentação de fotografias, máscaras ou modelos artificiais da cabeça de um usuário autorizado.

Testes para verificar se a face apresentada é uma face real são realizados a partir da solicitação de pequenos movimentos faciais. O sistema solicita que o usuário pisque os olhos ou mova os lábios, obtendo duas imagens, uma antes e outra durante o movimento. Estas imagens são comparadas e é possível verificar se o usuário foi capaz ou não de realizar estes movimentos. É possível ainda, como teste de validade da face apresentada, a obtenção de imagens de perfil, o que também invalidaria a apresentação de fotografias ao sistema.

7 Íris

7.1 Introdução

Mesmo os dois olhos de uma mesma pessoa são considerados únicos. Além de distintos, os padrões apresentados pelo olho humano são considerados estáveis durante toda a vida do indivíduo, estão protegidos do ambiente externo, e são afetados por apenas algumas doenças. Por causa de sua conexão direta com o cérebro, o olho humano é uma das primeiras partes do corpo a se deteriorar após a morte do indivíduo [NEW 99] [ROE 98].

Duas partes do olho humano podem ser utilizadas para fins de identificação por diferentes sistemas biométricos: a íris e a retina.

O fato de cada íris ter uma textura extremamente rica em detelhes e ter um padrão único, mesmo entre gêmeos idênticos ou entre os dois olhos do mesmo indivíduo, foi observado pelos oftalmologistas americanos Leonard Flom e Aran Safir [NEW 99].

A textura complexa da íris é considerada a característica biométrica que apresenta maior número de formas de variação entre indivíduos [DAU 99]. É também considerada extremamente estável durante a vida do indivíduo, e impossível de ser alterada cirurgicamente sem causar prejuízos à visão [POL 97]. Sua imagem pode ser registrada à distância sem contato físico com o usuário.

Todos os sistemas de reconhecimento de íris comercialmente disponíveis estão baseados em algoritmos patenteados por John Daugman para a empresa americana IriScan Inc. [IRI 99]. O primeiro sistema de leitura de íris foi lançado comercialmente em 1995 por esta companhia. Outras companhias, incluindo Sensar e Oki, iniciaram estudos para o desenvolvimento de sistemas de leitura da íris baseados nas técnicas desenvolvidas pela IriScan [NEW 99].

7.2 Descrição da característica

A íris é um órgão interno do olho, situado após a córnea e o humor aquoso. É composta de tecido conectivo elástico, cuja morfogenia pré-natal se completa durante o oitavo mês de gestação. Este tecido consiste de ligamentos pectíneos, que se aderem na forma de uma estrutura entrelaçada, formando estriamentos, processos ciliares, folículos, anéis, sulcos, um halo, algumas vezes pontos, vasculatura e outras características.

Durante o primeiro ano de vida do indivíduo, células cromatóforas muitas vezes alteram a cor da íris, mas as evidências clínicas disponíveis indicam que o padrão trabecular em si é estável durante a vida do indivíduo. Pelo fato de a íris ser um órgão interno do olho, é imune ao ambiente externo exceto pela capacidade da pupila de reagir a estímulos luminosos.

Existem algumas variações em função da quantidade de detalhes detectáveis da íris em função de variação étnica ou cor dos olhos, mas mesmo olhos extremamente negros

apresentam riqueza de detalhes quando sua imagem é feita utilizando-se raios infravermelhos [DAU 99].

Apesar de a similaridade visível entre gêmeos idênticos demonstrar a penetrância genética de, por exemplo, a aparência geral da face, comparações entre íris geneticamente idênticas (de olhos de uma mesma pessoa ou de gêmeos idênticos) revelam que a textura da íris é uma característica de fenótipo, não de genótipo. A cor os olhos possui alta penetrância genética, mas os detalhes texturais são não-relacionados e independentes mesmo em pares geneticamente idênticos [DAU 99].

7.3 Funcionamento do sistema

Inicialmente, o sistema captura uma imagem monocromática do padrão da íris através de uma câmera de vídeo padrão. Modelos antigos da IriScan requeriam um posicionamento do olho bem próximo ao dispositivo, mas modelos atuais permitem uma distância média olho-lente de 30 centímetros. A partir da imagem capturada da íris, é gerada uma representação matemática – denominada IrisCode – que se transforma num template de 256 bytes [NEW 99] .

Para identificar exatamente a íris na imagem, é necessário primeiro localizar precisamente seus limites interno e externo, e detectar e excluir a presença das pálpebras, se houver.

Então, é definido um sistema de coordenadas que mapeia o tecido da íris de forma a ser invariante a mudanças de constrição na pupila, ao tamanho geral da imagem da íris, ao zoom da câmera e à distância entre o olho e a câmera. Este sistema de coordenadas é pseudo-polar e não considera que os limites interno e externo da íris sejam concêntricos, uma vez que a pupila não está localizada no centro da íris. O sistema de coordenadas compensa automaticamente a deformação elástica da íris em função da dilatação da pupila [DAU 99].

O padrão da íris é então codificado num “IrisCode” de 256 bytes. O IrisCode definido para qualquer olho é invariante para translações e alterações de dimensões, inclusive para alterações do diâmetro da pupila em relação ao da íris. Mas rotações na íris, devidas à inclinação da câmera ou da cabeça do indivíduo, produzem alterações no IrisCode. Desta forma, todas as comparações entre íris precisam ser repetidas para uma faixa de rotações relativas, considerando depois somente a melhor coincidência [DAU 99]. Uma imagem do isolamento da íris e seu IrisCode poode ser vista na Figura 7.1.

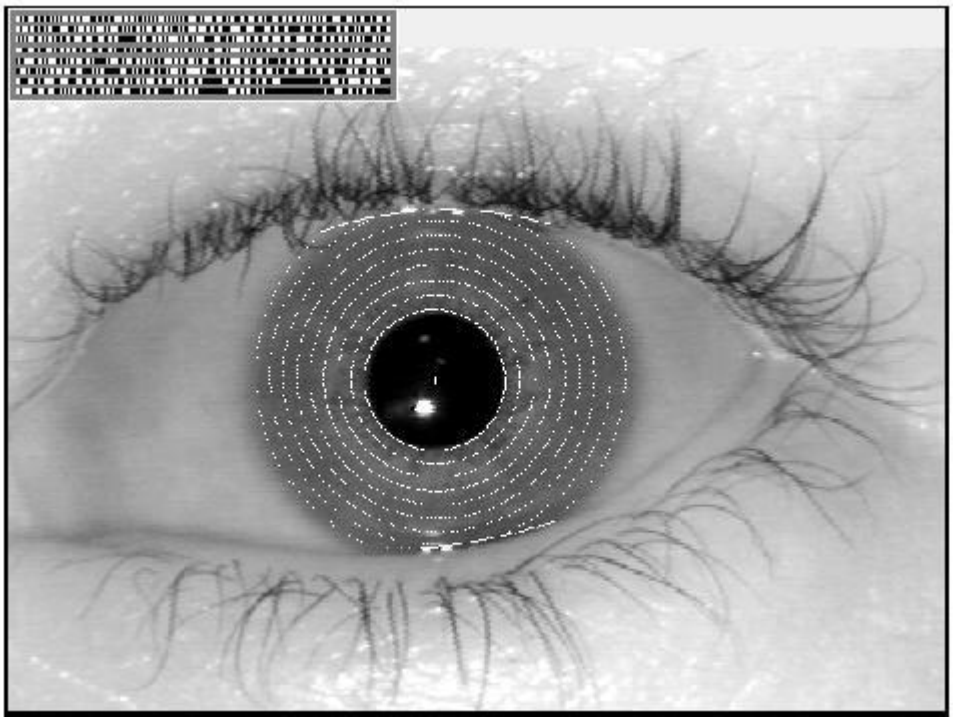

Figura 7. 1 – Isolamento da íris e IrisCode resultante
(Fonte: IriScan Inc. [IRI 99])

7.4 Limitações da tecnologia

Segundo estudos, tipicamente algo em torno de 10% dos bits de um IrisCode divergem quando uma amostra cadastrada no sistema e uma nova amostra são comparadas, devido a fatores como resolução da imagem, foco, movimento do olho, detalhes encobertos pelas pestanas, sujeira em lentes de contato ou ruído da câmera, por exemplo. Além disso, em função da espessura não-uniforme da íris, sua elasticidade também não é uniforme, e mesmo modelos que consideram as deformações no padrão da íris em função de grandes dilatações ou contrações da pupila não são totalmente corretos. Em dilatações extremas a iris pode apresentar ainda dobras radiais em lugar de deformações elásticas. Estas deformações podem acarretar falsa rejeição de um usuário [DAU 99].

Existe uma crença popular de que alterações na aparência da íris refletiriam o estado de saúde de vários órgãos do corpo, ou até mesmo a personalidade do indivíduo, seu humor ou seu futuro. Estas afirmações estariam embasadas numa ciência chamada iridologia. Mas estudos médicos consideram a iridologia uma fraude.

Existe base científica para somente duas formas de alteração na aparência da íris. A primeira ocorre logo após o nascimento, quando células cromatóforas estabelecem a cor dos olhos do bebê; até que isto aconteça, muito bebês têm olhos de cor aparente azul. Adicionalmente, considera-se que alguns tratamentos para glaucoma com drogas

envolvendo prostalgina foram mencionados como causando alterações na cor da íris, mas este fenômeno ainda não está devidamente documentado na literatura médica.

De qualquer forma, alterações na cor da íris são irrelevantes para o método de reconhecimento da íris que utiliza somente seu padrão analisado a partir de imagens monocromáticas feitas com iluminação infravermelha. A base de dados de imagens de íris obtida para estudos por oftalmologistas [DAU 99] cobrem um período de 25 anos, e não revela qualquer alteração relevante nos padrões das íris de cada indivíduo. Algumas alterações na cor foram percebidas, mas é possível que tenham sido causadas por alterações no processo fotográfico [POL 97].

7.5 Proteção contra fraudes

Existem várias formas de se verificar se o que está sendo apresentado ao sistema é uma íris real, viva, e não, por exemplo, uma íris falsa impressa em uma lente de contato, ou uma fotografia de uma íris.

Uma forma óbvia de se realizar esta verificação é determinar a razão entre o diâmetro da íris e o diâmetro da pupila, em situações de alteração na intensidade da luz ou mesmo sob iluminação constante. Para a realização deste teste, pode-se forçar a pupila a se tornar maior ou menor através de alterações randômicas programadas no nível de iluminação, com um tempo de resposta da pupila constante de em torno de 250 mseg para contração e 400 msec para dilatação. Mas, mesmo sem qualquer alteração programada na iluminação, o desequilíbrio normal entre os sinais de excitação e inibição do cérebro para a enervação do músculo da pupila produz pequenas oscilações. Uma vez que os algoritmos devem determinar os limites da pupila e da íris, é possível observar estas oscilações e verificar que se trata de uma íris genuína [DAU 99].

Testes adicionais para excluir a utilização de fotografias ou vídeos podem ser feitos determinando movimento das pálpebras. É possível ainda examinar reflexos de luz no globo ocular, ligando e desligando pequenas fontes de luz infravermelha em sequências randômicas e diferentes posições. Este procedimento vai criar reflexos correspondentes na córnea de um olho vivo, o que não seria possível acontecer no caso da utilização de, por exemplo, uma fotografia [DAU 99]. Outros testes involvem ainda a assinatura espectral característica de um tecido vivo numa iluminação infravermelha.

Finalmente, existem lentes de contato que têm impressos padrões de íris falsos, com o propósito de modificar a cor aparente dos olhos. Estas lentes de contato ficam posicionadas na superficie externa da córnea, e não na parte interna do olho, permitindo sua detecção visual. Além disso, a íris impressa não sofre qualquer distorção quando a pupila sofre alterações no seu diâmetro, como acontece com uma íris viva. Adicionalmente, o próprio processo de impressão da falsa íris cria uma assinatura característica que pode ser detectada matematicamente [DAU 99].

8 RETINA

8.1 INTRODUÇÃO

A identificação através da retina é um método automático que proporciona uma identificação verdadeira da pessoa pela aquisição de uma imagem de uma porção interna do olho de um indivíduo, que deve cooperar com o sistema para sua aquisição [HIL 99].

O olho compartilha o mesmo ambiente estável do cérebro e entre as características físicas utilizadas em sistemas biométricos, o padrão vascular da retina é considerado dos mais estáveis. Em função de sua localização interna, a retina é protegida de variações causadas pela exposição ao ambiente.

Os sistemas de reconhecimento de retina estiveram sob patentes americanas licenciadas para a empresa americana EyeDentify Inc. [EYE 99]. O conceito de reconhecimento da retina também estava sob proteção de patente até 1995. Uma vez que esta patente já expirou, outras empresas poderão ter interesse em desenvolver novas tecnologias para o reconhecimento da retina, o que não ocorreu até então. Alguns subsistemas da tecnologia de reconhecimento de retina, como interface com o usuário e alinhamento/ fixação, ainda estão sob proteção de patentes [HIL 99].

A EyeDentify foi fundada em 1976 a partir da idéia de conceber um dispositivo simples para a identificação de indivíduos utilizando a retina. A pesquisa inicial analisou e modificou diversos dispositivos ópticos (câmeras de fundo de olho) na tentativa de se obter imagens da retina que pudessem ser utilizadas para identificação. Mas estas câmeras necessitavam de um alinhamento do olho extremamente preciso, requerendo grande habilidade por parte do usuário ou a assistência de um operador. Além disso, estas câmeras requeriam iluminação intensa e eram extremamente complexas e caras.

Os mais antigos experimentos com dispositivos de identificação de retina utilizavam luz visível, e a quantidade de luz necessária para iluminar a retina era muitas vezes desconfortável para o usuário. Foram então realizados experimentos utilizando comprimento de onda infravermelhos. Este comprimento de onda é invisível para o olho humano e elimina a necessidade de iluminação intensa da retina, o que, além de ser incômoda para o usuário, poderia causar contração da pupila e consequente redução na quantidade de luz detectada [HIL 99].

O primeiro protótipo funcional foi contruído em 1981, e diversos algoritmos de extração das características da retina foram avaliados. O primeiro sistema de reconhecimento de retina foi lançado pela EyeDentify em 1985. A maior parte das unidades iniciais foram vendidas para estabelecimentos militares e outros que requeriam alta segurança que estes sistemas oferecem.

A EyeDentify alega que até o momento não foi reportado qualquer caso de falsa aceitação com seus sistemas [NEW 99]. Alguns autores consideram que este fato pode ser devido ao alto valor limite para a comparação entre templates imposta pelo sistema mas, ainda segundo o fabricante, o valor adotado pelo sistema pode ser mínimo.

8.2 Descrição da característica

A retina funciona para o olho como um filme para a câmera. Ambos detectam a luz incidente na forma de uma imagem que é focalizada por uma lente, e a quantidade de luz que chega à retina é determinada pela abertura da pupila. A retina é localizada na parte posterior interna do globo ocular, e o sangue alcança a retina através de veias que saem do nervo óptico. Logo atrás da retina se encontra um conjunto de veias chamado vasculatura coroidal [HIL 99]. A estrutura do olho humano pode ser observada na Figura 8.1.

Figura 8. 1 - Estrutura do olho humano

A idéia de que os vasos sanguíneos da retina poderiam ser utilizados para identificar indivíduos foi publicada no New York State Journal of Medicine em setembro de 1935 pelos doutores Carleton Simon e Isidore Goldstein, que, durante estudos de doenças dos olhos, descobriram que cada olho possuía seu padrão vascular único, e publicaram um artigo sobre o uso de fotografias da retina para identificação de pessoas baseada no seu padrão vascular [HIL 99]. A singularidade da retina foi provada nos anos 50 pelo dr. Paul Towers em sua invensticação sobre irmãos gêmeos. Ele considerou que, de quaisquer duas pessoas, gêmeos idênticos teriam a mior probabilidade de ter padrões vasculares de retina semelhantes. Mas os estudo de Tower concluíram que, de todas as características comparadas entre gêmeos, o padrão vascular da retina apresentou a menor similaridade [NEW 99].

Na verdade, quando se fala de padrão vascular da retina, está sendo utilizada uma expressão familiar mas não totalmente correta. Por exemplo, os produtos da EyeDentify sempre utilizaram luz infrevermelha para iluminar a retina, que é essencialmente transparente para este comprimento de onda. A maior parte das informaçõs relevantes para a identificação do indivíduo é refletida pelo vasculatura coroidal, na região localizada logo atrás da retina. Esta área também é referenciada por oftalmologistas como “fundo do olho”, ou fovea.

8.3 Funcionamento do sistema

O dispositivo utilizado para obtenção da imagem da retina funciona de forma similar a um retinoscópio, o aparelho utilizado por oftalmologistas para exame de fundo de olho. Sua fonte de luz é projetada no interior do olho do indivíduo e a luz refletida é detectada.

A representação da retina é derivada da tomada de imagem de uma região anular. Esta imagem é processada de forma a ser normalizada em relação à luz refletida pela retina e detectada pelo sensor. Variações nesta luz refletida podem ocorrer devido à não uniformidade do feixe de luz no ponto em que ele entra no olho, e a variações no tamanho da pupila, que vai influenciar diretamente na quantidade de luz refletida detectada pelo sensor [HIL 99].

Para garantir que a região correta da retina será iluminada pelo feixe de luz, o posicionamento do olho deve estar correto e um alvo de alinhamento/fixação é apresentado ao usuário. O dispositivo contém um orifício para onde o usuário deve olhar para alinhar seu olho a partir deste alvo óptico, composto por uma série de círculos. Conforme o usuário move o olho, os círculos se tornam mais ou menos concêntricos. O alinhamento correto é alcançado quando os círculos se tornam absolutamente concêntricos.

Com o olho corretamente alinhado com o dispositivo de leitura, um feixe de luz infra-vermelha ilumina a retina. A fonte de luz deve ser próxima ao infravermelho e não visível pelo usuário, e o feixe de luz projetado na retina deve ser uniforme. A energia infravermelha é absorvida mais rapidamente pelos vasos sanguíneos do que pelo tecido ao redor, e uma câmera captura uma imagem padrão a partir da luz refletida pelos vasos sanguíneos alcançados pela luz infravermelha. Um exemplo de imagem gerada por este processo é apresentado na Figura 8.2.

Usuários que utilizam óculos devem removê-los antes de utilizar o sistema. Este procedimento deve ser executado por duas razões: reflexos da superfície das lentes podem interferir no sinal adquirido, e distorção na imagem da retina pode acontecer se os óculos não estiverem na mesma posição do rosto a cada tomada de imagem. Se o usuário utiliza o sistema usando óculos, é possível que reflexo das lentes interfira e seja considerado como a representação da retina, e não a imagem da retina propriamente, resultando numa assinatura muito simples que poderia ser duplicada. Lentes de contato não precisam ser removidas, mas alguns tipos podem ser problemáticos e causar erros na assinatura se qualquer parte do contorno da lente estiver na região da pupila enquanto é realizada a tomada da imagem.

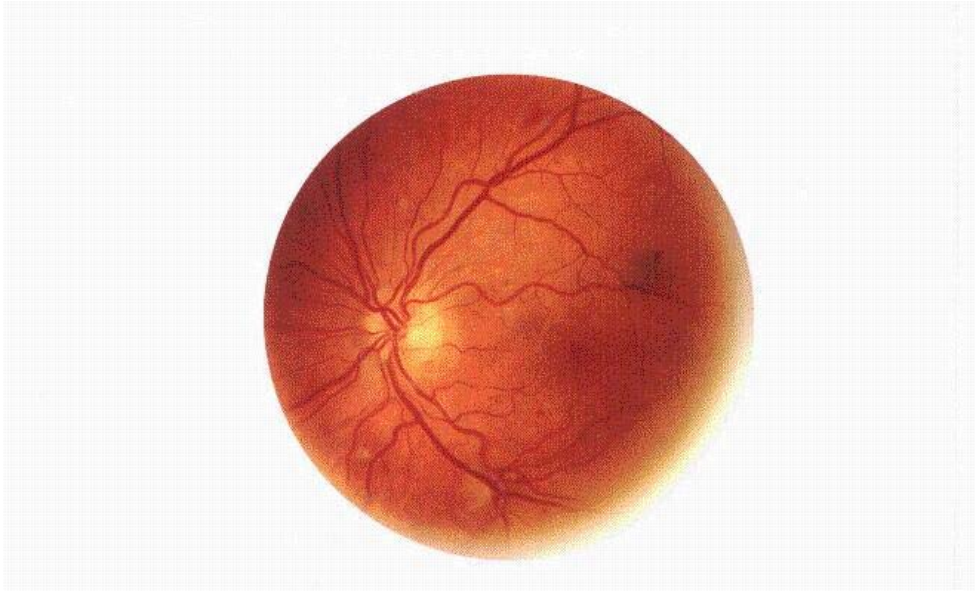

Figura 8. 2 - Imagem gerada no processo de leitura da retina
(Fonte: EyeDentify Inc. [EYE 99])

8.4 Limitações da tecnologia

A imagem da retina apresenta variação muito pequena quando adquirida sob condições corretas. Algumas condições podem trazer o aumento destas variações, acarretando eventual falsa rejeição. Problemas no alinhamento e fixação do olho e distância incorreta entre o olho e a câmera estão entre elas. A abertura insuficiente da pupila também pode acarretar variações na imagem: a função da pupila é regular a quantidade de luz que chega à retina, e ambientes com iluminação intensa, como ambientes externos à luz do dia, podem fazer com que a pupila se contraia até um tamanho tão pequeno que não permita a aquisição da imagem. Obstrução no caminho óptico entre a retina e a câmera, como extremidades de lentes de contato, óculos ou ainda sujeira nas lentes da câmera também interferem na aquisição da imagem. Finalmente, a luz ambiente pode invadir a câmera e interferir na imagem adquirida.

Uma vez que óculos precisam ser removidos no momento da tomada da imagem da retina, pessoas com altos graus de astigmatismo podem ter dificuldade em focalizar os pontos do alvo de alinhamento da câmera, fazendo com que a pupila fique fora da área de operação do dispositivo.

Os sistemas de reconhecimento de retina de um modo geral não são bem aceitos pelo público. Isto acontece basicamente por dois motivos. O primeiro é o cuidado natural que as pessoas têm com seus olhos. Apesar de nada indicar que a incidência de luz infravermelha no interior dos olhos possa trazer algum eventual prejuízo à visão, o medo de se ter este feixe de luz direcionado ao interior do olho faz com que muitas pessoas sejam resistentes ao sistema. O segundo é que estes sistemas perdem muito em

ergonomia se comparados a outros sistemas biométricos. O posicionamento correto, a visualização do alvo e o alinhamento do olho são tarefas que exigem muita concentração do usuário.

8.5 Proteção contra fraudes

Os sistemas biométricos que utilizam a retina são relativamente difíceis de ser enganados. Em função de sua ligação direta com o cérebro, o padrão de veias da retina muda rapidamente após a morte do tecido, o que faria a terrificante idéia da utilização de um globo ocular extraído de um usuário autorizado impraticável.

Uma outra opção de tentativa para fraudar reconhecimento pelo sistema seria através da utilização de algum mecanismo de criação de um falso olho que pudesse recriar as características do olho de um usuário autorizado. Esta falsificação deveria ter o mesmo sistema óptico do olho original, para refletir a retina da mesma forma, e lentes capazes de focalizar e refletir o feixe de luz. Adicionalmente, deveria possuir um sistema de alinhamento e fixação que orientasse o falso olho em torno dos eixos X e Y e o posicionasse corretamente sobre estes eixos, encontrasse uma posição no eixo Z que posicionasse o olho à distância correta da câmera e só permitisse sua rotação em torno deste eixo dentro do limite de rotação permitido pelo algoritmo do sistema [HIL 99].

9 Voz

9.1 Introdução

A voz é considerada a forma mais comum de comunicação entre os seres humanos. Existem estudos que provam que bebês são capazes de reconhecer a voz materna ainda no útero, e podem reconhecer este mesmo padrão de voz após o nascimento. Muitos animais são capazes de reconhecer sua família e diferenciar amigos de inimigos através de seus sons naturais característicos. A natureza produziu uma enorme variedade de sons para permitir demarcação de território, reconhecimento e camuflagem. Pássaros, morcegos e golfinhos possuem características especiais que permitem ainda o reconhecimento de indivíduos. Esta mesma riqueza de sons pode ser encontrada também na voz humana.

O processamento da fala é um campo diverso com muitas aplicações. Os sistemas de reconhecimento que analisam a fala podem ser divididos em três categorias, cada uma extraindo informações específicas diferentes. A primeira é o reconhecimento automático da fala, onde o objetivo é identificar o conteúdo da fala, como palavras e expressões. A segunda é a identificação de idiomas. Este tipo de identificação é extremamente complexo em função da dificuldade de se definir características únicas que que possam ser representativas de um idioma específico, e ainda pela existência de diferenças entre os locutores e os sotaques. A terceira é o reconhecimento de locutor [ADA 97].. Os sistemas que realizam reconhecimento de locutor focalizam as características que produzem a fala, e não no som ou na pronúncia das palavras, e estas características dependem principalmente da constituição física do indivíduo. É este o tipo de reconhecimento utilizado pelos sistemas biométricos que utilizam a voz como característica. Apesar de os seres humanos poderem utilizar estas características naturalmente para identificar alguém, o processo automático de identificação de locutor não é simples [POL 97].

9.2 Descrição da característica

A fala é um sinal produzido como resultado de diversas transformações ocorridas em diversos níveis diferentes: semântico, linguístico, articulatório e acústico. Diferenças nestas transformações resultam em diferenças nas propriedades acústicas do sinal de voz. As diferenças entre locutores são resultado de uma combinação de diferenças anatômicas inerentes ao trato vocal e de hábitos de fala adquiridos por cada indivíduo. Em sistemas de reconhecimento de voz, todas estas diferenças podem ser utilizadas para discriminar locutores.

Existem duas fontes de características específicas do indivíduo na produção da fala: físicas e adquiridas. O formato do trato vocal é um importante fator físico distintivo da fala. O trato vocal é geralmente considerado como o órgão produtor da fala acima das cordas vocais, incluindo a faringe, a cavidade oral (anterior ao véu palatino e limitada pelos lábios, língua e palato), e a cavidade nasal. O trato vocal de um adulto do sexo masculino tem em média 17 centímetros de comprimento [CAM 99].

Conforme as ondas acústicas atravessam o trato vocal, sua frequência é alterada por ressonâncias devidas às suas características fisiológicas. Cada palavra articulada pode ser decomposta em partes menores como sílabas, fonemas, ou outras unidades de som similares. Estes sons têm diversas frequências dominantes, chamadas formantes. Estes formantes podem ser considerados como um conjunto de ressonâncias específicas de um determinado som vocal. Os formantes se mantém constantes para uma determinada unidade de som, ou segmento. Cada segmento tem três ou quatro modulações dominantes, e o conjunto destas modulações é conhecido como espectograma vocal.

Mesmo que duas pessoas articulem exatamente a mesma palavra, o espectograma sonoro será diferente e único para cada pessoa. Esta diferença se torna mais perceptível se o tamanho da palavra aumenta ou se a amostra consiste de maior número de palavras, ou ainda se as pessoas articulam palavras diferentes.

9.3 Funcionamento do sistema

Os sistemas de reconhecimento de locutor podem ser classificados em texto-dependentes ou texto-independentes. Os sistemas texto-dependentes requerem que o usuário articule a mesma frase durante seu registro no sistema e no momento da aquisição da nova amostra. Os sistemas texto-independentes vão reconhecer o usuário independente do que ele disser durante a aquisição da nova amostra o teste. Sistemas texto-independentes, apesar de mais complexos, têm a vantagem de ser mais convenientes para o usuário, uma vez que ele não precisa memorizar qualquer frase específica, mas geralmente é necessária uma amostra da fala maior para que haja reconhecimento confiável. Sistemas texto-dependentes podem utilizar frases menores e ainda apresentam a segurança adicional de que o impostor deve descobrir a frase utilizada no cadastramento do usuário.

Alguns sistemas permitem ainda que o usuário escolha sua própria frase, não havendo restrições em relação à linguagem utilizada ou vocabulário permitido. Além do benefício psicológico trazido por esta escolha, as frases escolhidas pelo usuário tendem a ser mais simples de serem memorizadas, e a linguagem e o vocabulário livres tornam quase impossível que um impostor descubra a frase escolhida pelo usuário.

O sinal produzido pela fala é analógico e contínuo. Para que possa ser processado pelo sistema, o sinal deve estar representado de forma digital. Um microfone ou telefone podem ser utilizados para converter a onda acústica em um sinal analógico, que, após filtragem, é amostrado para formar um sinal digital através de um conversor analógico/digital. Normalmente, em aplicações locais de verificação de locutor, o canal analógico se resume ao microfone, seu cabo e a filtragem do sinal. Nesta situação, o sinal digital resultante pode ser de alta qualidade, sem distorções causadas pela transmissão do sinal analógico através de, por exemplo, linhas telefônicas [CAM 99].

O espectograma vocal é basicamente armazenado como uma tabela de números, onde a presença de cada frequência dominante em cada segmento é expressa como uma entrada binária nas colunas da tabela. Uma vez que todas as entradas da tabela podem ser 1 ou 0, cada coluna pode ser lida como um número binário, e o conjunto destas colunas para cada palavra forma seu código único que vai permitir a identificação do usuário

9.4 Limitações da tecnologia

A fala, por ser uma característica comportamental, não proporciona uma verificação tão precisa quanto as características biométricas físicas. A voz do indivíduo pode sofrer alterações em função de diversos fatores físicos, emocionais e ambientais. Estes fatores são importantes porque, independente de quão precisos sejam os algoritmos de reconhecimento da fala, estas alterações podem prejudicar sua performance. Além disso, é possível que o usuário altere a produção de sua fala conforme o seu desejo.

Os sistemas de reconhecimento de locutor podem ser projetados com alguma robustez contra pequenas alterações na voz humana, como sutis alterações diárias e pequenos resfriados. Mas estados emocionais extremos, cansaço, influência de bebidas alcóolicas, anestesia dental ou problemas de saúde que afetem intensamente o trato vocal podem alterar as características da fala produzida, interferindo na performance do sistema. Obviamente, pessoas que não sejam capazes de produzir a fala não estão aptas a utilizar o sistema.

Variações no canal analógico, como a utilização de diferentes microfones para registro do usuário e aquisição da nova amostra, diferente disposição do microfone e problemas acústicos no ambiente, como ruídos, podem causar interferência na qualidade do sinal adquirido.

Adicionalmente, o processo natural de envelhecimento traz alterações no trato vocal, modificando a produção da fala. Os templates devem ser atualizados periodicamente para minimizar este problema.

9.5 Proteção contra fraudes

A reprodução de uma voz previamente gravada pode ser fraudulentamente apresentada ao sistema em aplicações não vigiadas. Mas gravadores de som típicos produzem gravações de baixa qualidade que são sujeitas a distorções não-lineares, facilitando a identificação de impostores. Sistemas de gravação de som digitais de alta qualidade não introduzem distorções significantes, e podem ser aceitos por sistemas de reconhecimento de voz.

Uma forma de minimizar o risco de aceitação de uma gravação é a utilização de múltiplas frases pelo sistema. O usuário seria registrado a partir de uma série de frases e, durante a apresentação da nova amostra ao sistema, este solicitaria ao usuário uma ou mais das frases em ordem randômica. Para fraudar o sistema, o impostor deveria ter em seu poder gravações de todas as frases, e na ordem correta, em um período de tempo muito curto [NEW 99] [CAM 99] .

10 SISTEMAS BIOMÉTRICOS EM DESENVOLVIMENTO

Muitos conceitos diferentes têm sido discutidos nos últimos anos no meio acadêmico e entre membros da indústria de sistemas biométricos para definir quais características do ser humano poderiam ser utilizadas para identificar um indivíduo. Como foi mencionado no Capítulo 3, qualquer característica humana pode virtualmente ser base de um sistema biométrico, desde que apresente basicamente as propriedades de universalidade, singularidade, estabilidade a longo prazo e coletabilidade. Obviamente nem todas as características biométricas apresentarão todas estas propriedades, mas algumas podem ser direcionadas para um público específico que esteja adaptado a elas.

Alguns sistemas biométricos de tecnologia emergente ou em desenvolvimento são descritos a seguir.

10.1 Assinatura

A verificação dinâmica de assinatura é baseada no fato de que assinar é uma ação de reflexo, não influenciada por controle muscular deliberado [POL 97] e que, observando-se uma assinatura completa, é impossível determinar como ela foi feita. A essência da verificação dinâmica de assinatura é que, diferente da verificação manual, a comparação é realizada com base na forma com que a assinatura armazenada como template e a nova amostra foram feitas, e não a partir de uma imagem estática das assinaturas. O tipo de informação que é coletada do processo de execução da assinatura varia de acordo com o sistema de cada fabricante, mas os dados capturados normalmente incluem fatores como o tempo utilizado para executar a assinatura, velocidade, direção, pressão e ângulo da caneta, número de vezes que a caneta saiu do papel e os instantes no tempo em que isto ocorreu. Alguns sistemas observam quão similar a nova amostra da assinatura deve ser da original; outros possuem ainda alta precisão mesmo que o usuário sublinhe sua assinatura ou não utilize alguma das letras. [NEW 99].

Existem dois tipos de dispositivos que capturam as características da assinatura. O primeiro utiliza placas com superfícies digitalizadoras que capturam as informações (Figura 10.1). A maior parte dos sistemas de verificação dinâmica de assinatura utiliza estes dispositivos, que são periféricos padrão, e os fabricantes somente precisam desenvolver o software que analisa e compara os dados. Outros sistemas utilizam canetas especiais para capturar as informações.

Figura 10. 3 – Dispositivo para captura de assinatura

(Fonte: PenOp Inc. [PEN 98])

A repetibilidade da assinatura nestes sistemas deve ser relativamente constante. Assinaturas alteradas com muita frequência, mal de Parkinson, indivíduos sob influência de bebidas alcóolicas ou drogas podem afetar a performance do sistema.

10.2 Termograma facial

A termografia, que é a utilização de câmeras sensíveis ao espectro infravermelho, permite a identificação de um indivíduo a partir de imagens termográficas da sua face ou outras partes do corpo [PRO 99].

Os termogramas humanos são afetados por alterações na temperatura ambiente, por ingestão de substâncias que sejam vaso-constritoras ou vaso-dilatadoras, inflamações, obstrução das artérias, derrame cerebral, e outras condições físicas. Estas variações de temperatura podem ser mapeadas e utilizadas para diagnósticos de monitoração para tratamentos médicos.

Quando o objetivo é somente a identificação do indivíduo, a temperatura do corpo não é diretamente utilizada. Os dados térmicos são analisados de forma a tirar proveito de informações anatômicas que não variam com estas alterações. Os termogramas faciais apresentam os mesmos padrões de vasos sanguíneos independente da temperatura aparente.

Os padrões térmicos observados pela câmera infravermelha derivam do padrão de vasos sanguíneos sob a pele, que transportam sangue quente para todo o corpo. Mesmo gêmeos idênticos possuem termogramas diferentes [TEC 99].

Cirurgias plásticas podem realizar alterações na aparência geral do corpo, extraindo pele, redistribuindo gordura ou removendo cicatrizes, mas geralmente não alteram a aparência geral do termograma a não ser que os vasos sanguíneos sejam reposicionados sob a pele. Nestes casos, deixariam incisões tão profundas que, além de possivelmente lesionarem os nervos faciais, seriam detectáveis pela iluminação infravermelha. Por

isso, é considerado possível que uma pessoa altere cirurgicamente seu padrão vascular, mas o termograma vai ter evidências de que este procedimento foi realizado.

10.3 Dinâmica de digitação

A tecnologia de dinâmica de digitação verifica a identidade de um indivíduo a partir de seu ritmo de digitação. Cada pessoa desenvolve seu próprio ritmo quando está digitando e, nos tempos da telegrafia, os operadores conseguiam identificar uns aos outros somente por este ritmo. O objetivo desta tecnologia é desenvolver um sistema que possa monitorar continuamente, por exemplo, os usuário de um computador particular, e detectar se alguma outra pessoa está utilizando o computador no lugar da pessoa inicialmente autorizada no sistema. O monitoramento constante é uma atividade difícil; o ritmo de digitação pode variar, por exemplo, se a pessoa está cansada, sob impacto emocional ou sob efeito de bebida alcoólica.

A maior parte dos sistemas disponíveis atualmente somente verifica o usuário quando ele solicita acesso ao sistema, no momento em que ele digita sua senha. A avaliação da dinâmica de digitação inclui, além do próprio tempo utilizado para digitar a senha, o tempo que cada tecla permaneceu pressionada e o tempo gasto no movimento de uma tecla para outra [NEW 99].

10.4 Geometria da orelha

Os sistemas que utilizam o formato da orelha como base para reconhecimento de indivíduos ainda não têm suas especificações totalmente definidas. Na verdade, estudos ainda estão sendo realizados com a finalidade de garantir que o formato da orelha é uma característica única e estável.

A técnica de identificação utilizando a geometria da orelha foi desenvolvida por A. Iannarelli, e é baseado em 12 medidas de distâncias entre pontos específicos da orelha do indivíduo, a partir de uma imagem em tons de cinza do seu perfil [BUR 99]. Estes medidas são apresentadas na Figura 10.4.

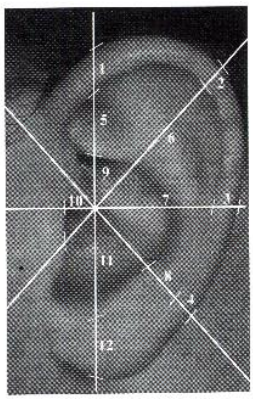

Figura 10. 4 – Medidas da geometria da orelha

Estes sistemas poderiam ser utilizados como fonte suplementar para reconhecimento de indivíduos. Por exemplo, um sistema projetado para reconhecimento de faces possui todo o hardware necessário para capturar e computar as características da geometria da orelha.

10.5 Odor

Estudos em desenvolvimento tentam provar que a utilização do odor do corpo como característica em sistemas biométricos é viável. As substâncias químicas que produzem o odor do corpo são emitidas por todos os poros e podem ser analisadas a partir, por exemplo, o dorso da mão do indivíduo. Normalmente estes sistemas utilizam sensores distintos para registrar cada substância química presente no odor, e o resultado encontrado por cada sensor é utilizado para gerar o template. Variações na temperatura, umidade e condições emocionais acarretam alterações no odor produzido pelo corpo, mas ainda não foram realizados estudos suficientes para avaliar o impacto destas alterações nos sistemas biométricos que utilizam esta característica [NEW 99].

10.6 Sistemas biométricos multi-modais

Sistemas biométricos multi-modais são sistemas que utilizam uma combinação de duas ou mais características biométricas no mesmo sistema. A razão mais relevante para a combinação de diferentes modalidades de características biométricas é o aumento da precisão no reconhecimento dos usuários. Isto somente pode ser realizado quando as características são estatisticamente independentes [BRU 93].

Existem outras razões para combinar diferentes características biométricas em um mesmo sistema. Uma delas é fato de que um tipo específico de característica pode ser mais apropriado para determinada aplicação do que outro. Por exemplo, em um banco, o usuário pode ser registrado a partir de sua impressão digital e sua voz; para a utilização normal em agências e caixas eletrônicos o usuário seria autenticado por sua impressão digital, e para acesso a operações bancárias pelo telefone seria autenticado por sua voz. Uma outra razão para a utilização de sistemas biométricos multi-modais é a preferência do público alvo considerado. Ainda no mesmo exemplo do banco, o caixa eletrônico poderia oferecer autenticação através de impressão digital, voz ou face, e ao usuário seria permitido escolher a que melhor lhe conviesse [HON 99].

Pode ser necessário, ainda, atender com alguma outra característica uma população que não esteja apta a utilizar uma característica específica. Isto já é feito em sistemas não automatizados como, por exemplo, com a utilização de impressão digital no lugar de assinatura para pessoas analfabetas.

11 Testes e Certificação de Sistemas Biométricos

O principal indicador da qualidade de um sistema biométrico são as suas taxas de falsa rejeição e falsa aceitação. Considerando todas as outras propriedades relevantes para a adequação de um determinado sistema biométrico a uma aplicação específica, as taxas de erro produzidas por este sistema vão possibilitar a consideração sobre quão seguro e acurado é o sistema em distinguir usuários legítimos de usuários não autorizados.

Na grande maioria dos casos, a única informação disponível para a avaliação geral de um sistema ou dispositivo biométrico é o seu folheto comercial. As indicações de performance reais, de uma maneira geral, são conhecidas somente pelo próprio fabricante a partir de possíveis testes executados internamente.

Para poder dizer definitivamente que um produto tem, por exemplo, uma taxa de falsa aceitação de 0,001%, o fabricante deveria ter realizado pelo menos 100.000 verificações, preferencialmente utilizando uma pessoa diferente para cada verificação. O que acontece normalmente é que muitos fabricantes realizam pequenos testes e extrapolam estes resultados para calcular suas taxas de erros [NEW 99].

Mesmo que testes reais tenham sido executados pelo fabricante, a determinação da performance no mundo real é um problema complexo [CAM 99a]. Estes testes normalmente são realizados em laboratório, em ambiente e condições controlados, sem a influência de condições ambientais adversas, como calor ou umidade [ROE 98]. Ou seja, as taxas de erros obtidas nos testes estariam sendo medidas a partir de condições não realistas e poderiam não ser válidas para determinado dispositivo em determinada aplicação.

Além disso, o próprios valores das taxas de falsa rejeição e falsa aceitação não são facilmente interpretados, porque diversos fatores podem influenciar seu resultado:

- Estas taxas são intimamente relacionadas e, normalmente, existe algum parâmetro que pode ser ajustado de forma a diminuir a falsa aceitação e aumentar a falsa rejeição ou vice-versa. Ou seja, as taxas informadas pelo fabricante estão relacionadas a algum valor limite que teoricamente poderia ser alterado, consequentemente modificando as taxas de erro.

- Os valores podem ser determinados através de protocolos de teste tipo "uma-tentativa" ou "três-tentativas", por exemplo. Estes protocolos indicam o número de vezes que o usuário pode apresentar sua amostra ao sistema antes que este decida pela sua aceitação ou rejeição. O aumento do número de tentativas pode melhorar a taxa de falsa aceitação sem deteriorar a taxa de falsa rejeição [ROE 98].

- Em algumas situações a taxa de falsa rejeição pode ser ocasionada por algum pequeno grupo que tenha dados biométricos instáveis, resultado de uma escolha equivocada da população de teste. Nestes casos, este grupo deveria ser excluído da população de teste, ou ter apenas um número de indivíduos que fosse representativo na população real.

- As taxas de erros dependem muito da interação do usuário com o sistema. Usuários treinados realizam melhor as tarefas que usuários sem treino. As intenções do usuário também vão interferir nas taxas de erro: dificilmente um usuário da população de teste não estará disposto a colaborar com o sistema, o que pode não ser verdade em aplicações do mundo real.

Para que os resultados estatísticos apresentados sejam avaliados corretamente, devem ser acompanhados por informações detalhadas referentes ao processo de elaboração e execução dos testes. O tamanho da população-amostra, a descrição desta população e a descrição do teste devem ser fornecidos.

O tamanho da população-amostra deve conter informações como o número de indivíduos, o número de registros para cada indivíduo, e o número de coincidências ou não-coincidências possíveis na base de dados.

A descrição da população deve conter os tipos de indivíduos incluídos na amostra, como o número de crianças, jovens e idosos, o número de homens e mulheres, os tipos de atividades executadas pelos indivíduos, e qualquer outra informação que seja relevante para aquele tipo de sistema biométrico. Por exemplo, para o teste de um sistema de reconhecimento de geometria da mão, o número de idosos poderia ser relevante, uma vez que um grande número de falsas rejeições poderia estar ocorrendo em função de doenças reumáticas ou degenerativas.

Finalmente, o teste como um todo deve ser detalhadamente descrito. Por exemplo, se os usuário foram treinados ou não, se a tomada de dados era ou não supervisionada por um operador, se o sistema possuia feedback para a captura da característica, onde e em que condições os testes foram realizados e quais os componentes do sistema estavam envolvidos no teste. Adicionalmente, uma informação de particular interesse é de por quem o teste foi conduzido. O ideal é que testes sejam realizados e seus resultados apresentados por entidades isentas, confiáveis e com capacidade e autoridade para realizá-los.

Os resultados de testes obtidos não podem ser comparados se foram determinados em condições diferentes. Comparações entre resultados somente podem ser consideradas válidas se os testes foram realizados sobre a mesma base de dados e sob as mesmas condições [OGO 99].

Diversas entidades estão se direcionando para testes, certificação e criação de padrões para tecnologias biométricas, organizando-se através de conferências, congressos e seminários, com o objetivo de compartilhar conclusões de pesquisas e divulgar resultados obtidos. Entre estas entidades estão o US Biometric Consortium [BIO 98], a Europen Association for Biometrics, a Association for Biometrics [ASS 98] e o Biometric Consulting Group (BioConsulting), entre muitos outros.

A International Security Computer Association (ICSA), entidade independente americana, desenvolveu um programa de certificação para produtos biométricos [INC 99]. Como produto entende-se qualquer dispositivo de aquisição da característica, componente de software ou sistema integrado submetido pelo fabricante para certificação. Todos os produtos são certificados a partir dos mesmo critérios. O objetivo

principal deste programa é inicialmente nivelar os produtos para garantir sua operabilidade e taxas de erros básicas. As taxas de erro encontradas para cada produto não são divulgadas, e somente os produtos que atinjam taxas de falsa aceitação e falsa rejeição menores que 4,5 % recebem a certificação.

Este tipo de procedimento é importante porque dá ao público usuário de sistemas biométricos um padrão de avaliação seguro e isento. Hoje, a meta da comunidade científica é permitir que este público tenha ferramentas e resultados de testes confiáveis para auxiliar os usuários na seleção e utilização das tecnologias biométricas de uma maneira segura e correta.

12 Utilização

Apesar de o principal objetivo deste trabalho ser apresentar os sistemas biométricos como forma de individualização de usuários para controle de acesso em ambientes informatizados, na vida prática existem diversas outras situações onde é necessária a identificação de uma pessoa na nossa sociedade: Este usuário já foi visto antes? Esta pessoa é funcionário desta companhia? Este indivíduo é cidadão deste país?

Sistemas biométricos encontram aplicação em todas as áreas onde seja nercessário verificar a identidade de pessoas, e começam a substituir as formas tradicionais de verificação.

12.1 Controle de acesso lógico

A informatização das empresas permitiu a manutenção de documentos sem o armazenamento de papel, de forma eletrônica, e se tornou necessário desenvolver mecanismos para a proteção desta nova forma de documentação [NEW 99]. A utilização de sistemas biométricos para segurança em sistemas informatizados foi o estímulo original para a realização deste trabalho.

A maior parte dos dispositivos biométricos pode ser facilmente conectada a computadores pessoais como periféricos, permitindo sua utilização somente por usuários autorizados, através de atividadres simples como logon em redes e acessos a arquivos e serviços através de listas de controle de acesso.

O aumento do número de transações on–line através da Internet demanda um aumento na proteção dos dados que trafegam pela rede. As tecnologias de criptografia normalmente utilizadas para este fim são baseadas em chaves, e chaves apresentam os mesmos problemas que as senhas em geral. A segurança no gerenciamento de chaves é análoga à do gerenciamento de senhas, com a dificuldade adicional de que chaves são ainda mais difíceis de serem memorizadas. A proteção destas chaves pode ser feita a partir da proteção de seu arquivo no local de armazenamento através de acesso biométrico; ou ainda em smart–cards com o mesmo tipo de acesso.

A relação entre criptografia e biométricos também leva a tecnologias mais elaboradas, como a utilização do dado biométrico no processo de geração de chaves.

12.2 Controle de acesso físico

Controle de acesso físico foi a primeira utilização para a maioria dos sistemas biométricos, começando em instalações com necessidade de alta segurança e, com a evolução e redução de preços dos sistemas biométricos de uma maneira geral, para aplicações mais simples, como residências e estabelecimentos comerciais. Aplicações de controle de acesso continuam sendo o principal mercado para sistemas biométricos, e este mercado é dominado por sistemas que utilizam a geometria da mão, seguidos de perto por sistemas de verificação de locutores.

Recentemente, eventos importantes divulgaram os sistemas biométricos para o público em geral. Em 1996, durante os Jogos Olímpicos de Atlanta, dispositivos de leitura da geometria da mão foram utilizados para controle de acesso à Vila Olímpica. Também desde 1996 três parques temáticos da Walt Disney utilizam a geometria dos dedos para controlar visitantes com ingressos para temporada.

Em paralelo ao controle de acesso, sistemas biométricos também têm sido utilizados para aplicações de controle de presença e horário. Este tipo de controle substitui o cartão de ponto por leituras de características biométricas, automatizando o processo e diminuindo o risco de fraudes trabalhistas.

12.3 Sistemas bancários

A maior parte dos bancos ao redor do mundo está atenta ao desenvolvimento dos sistemas biométricos para aplicações bancárias, mas muito poucos realmente implementaram sua utilização.

Sistemas bancários são considerados uma aplicação extremamente sensível, pois a concorrência entre as instituições financeiras é grande, e qualquer pequena insatisfação do correntista pode fazer com que ele mude sua conta para outro banco. Por isto, a escolha do sistema biométrico para atender este público deve ser bastante cuidadosa.

Sistemas biométricos podem ser utilizados para evitar fraudes e facilitar as operações em todas as infraestruturas bancárias existentes – sistema tradicional de caixas, caixa eletrônico e home–banking. Através da utilização de um telefone, do computador do banco e de um sistema de reconhecimento de locutor, por exemplo, o correntista poderia realizar transações como movimento de dinheiro e consultas.

Mas correntistas não são os únicos usuários potenciais de sistemas biométricos no sistema bancário; funcionários do próprio banco também podem ser verificados para a execução de tarefas críticas.

12.4 Concessão de benefícios

Qualquer país que conceda benefícios financeiros a seus cidadãos, quando estes estão desempregados, doentes ou aposentados, está sujeito a solicitações fraudulentas de benefícios. A utilização de sistemas biométricos para concessão desses benefícios pode reduzir drasticamente o volume de dinheiro pago a pessoas que solicitaram o benefício mais de uma vez.

Este tipo de procedimento já foi adotado na Espanha. Na tentativa de reduzir os níveis de fraude nos benefícios concedidos a desempregados, a partir de 1996 foi iniciado o processo de fornecimento de samat–cards como forma de identificação para toda a população espanhola. Este projeto, conhecido com TASS [UNI 99], utiliza impressões digitais armazenadas nos smart–cards para garantir a segurança dos pagamentos de seguridade social e acesso a dados pessoais

Outros países, como Estados Unidos e África do Sul, também possuem soluções de seguridade social com a utilização de sistemas biométricos.

12.5 Controle de imigração

Sistemas biométricos podem ser utilizados no controle de fronteiras para verificar visitantes, identificar estrangeiros ilegais e registrar pessoas procurando asilo, por exemplo.

A finalidade dos sistemas de controle de visitantes é permitir que pessoas que visitam o país com frequência utilizem um sistema de controle de passaporte rápido e automático que elimine a verificação manual do documento por oficiais de imigração. Os Estados Unidos possuem um projeto neste sentido, chamado INSPASS (Immigration and Naturalization Services – Passenger Accelerated Service System) [HAY 99], que atende passageiros aéreos., utilizando geometria da mão. Outros países, como Canadá, Alemanha e Singapura, seguiram o exemplo e estão desenvolvendo projetos similares.

12.6 Aplicações legais

Diversas aplicações legais encontram utilização para sistemas biométricos. Esquemas de identificação nacional, eleições e controle carcerário estão evoluindo em muitos países através da utilização destes sistemas.

Sistemas de larga escala para identificação da população de um país normalmente utilizam alguma forma de documento para identificar o indivíduo. Mas o documento em si não pode, na verdade, provar realmente a identidade de uma pessoa. Os esquemas biométricos para identificação em larga escala resolvem este problema, mas infelizmente encontraram muita resistência nos primeiros países onde foram implementados, sob a alegação de que o Estado estava violando a privacidade de seus cidadãos.

Uma outra aplicação importante para sistemas biométricos é o controle de votação, impedindo fraude tanto durante eleiçõoes quanto em votações em entidades governamentais. Jamaica, Colômbia e Venezuela já possuem esquemas de votação protegidos por sistemas biométricos.

Aplicações criminais também encontram segurança a partir de sistemas biométricos. O controle de acesso em prisões, identificanndo e permitindo diferenciar entre prisioneiros e visitantes e carcereiros, permite o controle exato de quem deixa a prisão num determinado momento, além de permitir o rastreamento da movimentoação de prisioneiros. Outra aplicação seria o controle de pessoas condenadas à prisão domiciliar.

13 Conclusão

O objetivo deste trabalho foi mostrar que as tecnologias biométricas têm evoluído rapidamente e que deixaram a exclusividade das pesquisas de laboratório e dos filmes de ficção científica para uma grande variedade de aplicações efetivas no mundo real.

Todas as transformações trazidas pela era da informação estão revolucionando rapidamente a forma como as pessoas interagem com os sistemas informatizados, e a cada dia aumenta o número de ações eletrônicas, no lugar do papel e lápis ou face a face. Este crescimento das transações eletrônicas resulta numa maior demanda por uma identificação e autenticação de usuários rápidas e confiáveis.

Embora a abordagem tradicional de autenticação de usuários esteja baseada primariamente em senhas e eventualmente em cartões, este tipo de autenticação muitas vezes falha em dar o grau necessário de segurança que as aplicações demandam. Não existe forma absoluta de garantir que o usuário detentor do cartão ou senha é realmente o usuário autorizado, ou se é alguém que obteve o cartão ou senha fraudulentamente. Estas tecnologias menos seguras identificam somente um cartão ou um código numérico. Sistemas biométricos identificam pessoas, e por esta razão oferecem uma ferramenta de segurança mais efetiva. Não é impossível conseguir acesso fraudulento através de um sistema biométrico, mas o esforço despendido para que isso ocorra faz com que seja realmente bem próximo do impossível.

Ainda assim, um esquema de segurança é tão seguro quanto seu ponto mais fraco, de modo que um sistema completo de proteção deve ser projetado em torno do sistema biométrico. Por exemplo, impostores devem ser impedidos de inserir seus próprios templates na base de dados para que sejam considerados usuários autorizados, e canais de comunicação devem ser protegidos contra manipulação indevida.

Teoricamente, qualquer característica física ou comportamental poderia ser utilizada como base para um sistema biométrico, desde que todos os indivíduos possuíssem a característica, que ela tivesse valores diferentes para quaisquer dois indivíduos, que fosse estável a longo prazo e que fosse possível de ser medida. Diversas características vêm sendo estudadas mas muito poucas estão efetivemente em operação; o mais difícil sempre é comprovar a capacidade de a característica ser única entre os indivíduos.

Apesar da evolução dos sistemas biométricos, a determinação de suas medidas de performance ainda é motivo de debate. Fabricantes apresentam medidas de falsa aceitação e falsa rejeição que na maior parte dos casos refletem somente resultados de testes limitados em ambientes controlados. Entidades isentas e com capacidade técnica comprovada devem passar a ser responsáveis pela realização de testes e da divulgação de sua metodologia e seus resultados.

Atualmente, as informações técnicas disponíveis sobre sistemas biométricos estão bastante dispersas em uma variedade de livros, jornais, relatórios técnicos e proceedings de conferências. Os sistemas biométricos estão apenas no início de sua disseminação como tecnologia para o público de uma maneira geral. Mas acredita-se que estes

sistemas se tornarão um componente significativo para a identificação de pessoas, em função do amadurecimento de suas tecnologias fundamentais, da diminuição dos preços dos sensores e sistemas biométricos como um todo, e da própria divulgação destes sistemas. As pessoas começam a ficar cientes das capacidades e limitações desta tecnologia, e a desconfiança de que sistemas biométricos ameaçam a privacidade do indivíduo começa a desaparecer.

Os sistemas biométricos são uma tecnologia ainda repleta de potencialidades e estão no início do seu processo de desenvolvimento,. Não existe prova absoluta de que qualquer sistema biométrico utilize alguma característica física ou comportamental que seja realmente única e que possa distinguir sem sombra de dúvidas um indivíduo de outro; mas, de todas as formas de autenticação conhecidas até o momento, somente os sistemas biométricos podem garantir, mesmo que com alguma pequena probabilidade de erro, que você é realmente você mesmo.

Anexo A – Resumo Comparativo

TABELA A.1 – TABELA COMPARATIVA – CARACTERÍSTICAS BIOMÉTRICAS

TABELA A.2 – TABELA COMPARATIVA – SISTEMAS BIOMÉTRICOS

Anexo B – Experimento : Reconhecimento de Faces

B.1 Introdução

Testar e validar um sistema biométrico é tarefa extremamente complexa, como já foi avaliado no Capítulo 11. Para realizar testes que realmente tenham algum resultado significativo e que efetivamente meçam a performance de um determinado sistema biométrico, seria necessária a utilização de uma base de dados sufucientemente grande, derivada de uma população-amostra representativa, com inclusão e avaliação de todas as possíveis variáveis que pudessem estar presentes na operação normal do sistema. Avaliações confiáveis são resultado de estudos e testes realizados por instituições idôneas capacitadas para este fim.

Os testes aqui apresentados têm como objetivo simular a operação de um sistema biométrico baseado em reconhecimento de faces, a partir de um pequeno grupo de usuários e em ambiente controlado. Este experimento tem caráter exclusivamente ilustrativo.

B.2 Descrição do software

A ferramenta utilizada para realizar este experimento de reconhecimento de faces foi a versão de demonstração do software FaceIt, da Visionics Corporation [FAC 98]. O FaceIt é um software que possui a capacidade de realizar automaticamente detecção de faces, isoladas ou múltiplas, mesmo em cenas complexas, acompanhando a movimentação da face e isolando-a do fundo. Após a determinação da face, o software está apto a gerar seu template e a realizar as funções necessárias para o reconhecimento do usuário.

B.2.1 – Detecção de faces

O FaceIt foi projetado para comparar imagens faciais frontais. Variações rotacionais de até 15º em qualquer direção são assimiladas pelo software. De 15 a 35 graus de variação é possível haver perda de qualidade na capacidade de comparação do software, e a partir de 35 graus esta degradação de performance é bastante expressiva.

A detecção de faces é possível desde que seja identificada a presença de um par de olhos na cena. A função de detecção de faces do FaceIt procura constantemente por faces na cena apresentada. Quando um objeto semelhante a uma face fica visível, o software utiliza seu conjunto de algoritmos de reconhecimento de padrões para determinar se realmente existe uma face presente. Estes algoritmos são capazes de detectar com precisão a presença simultânea de múltiplas faces na mesma cena (Figura B.1) e determinar sua posição exata.

Quando a face é detectada, sua imagem é isolada do fundo da cena e processada para compensação de dimensões, iluminação, expressão e variação angular. A representação da face resultante deste processo é submetida à análise matemática denominada *local*

feature analisys (LFA), descrita no Capítulo 6, resultando na geração do template para aquela face.

Figura B.1 - Identificação de múltiplas faces em uma cena

B.2.2 – Níveis de segurança

A versão do FaceIt utilizada possui três níveis de segurança básicos, relacionados a valores de falsa aceitação obtidos através de estudos realizados pela Visionics em grandes bases de dados. Estes níveis de segurança servem como orientação para o administrador do sistema, e seus valores são apresentados na Tabela B.1 :

NÍVEL DE SEGURANÇA	TAXA DE FALSA ACEITAÇÃO (%)
BAIXO	0,4
MÉDIO	0,04
ALTO	<0,01

TABELA B.1 – NÍVEIS DE SEGURANÇA BÁSICOS NO FACEIT (FONTE: VISIONICS CORP.)

O software permite ainda que o valor de pontuação limite seja configurado para algum valor específico, permitindo que o grau de segurança seja determinado pelo

administrador do sistema. A opção de configuração dos níveis de segurança é apresentada na Figura B.2.

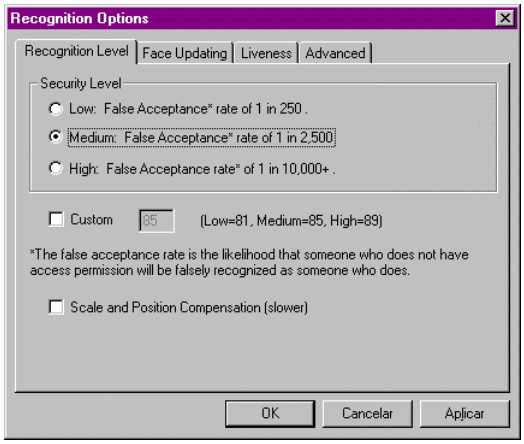

Figura B.2 – Configuração dos níveis de segurança no FaceIt

B.2.3– Atualização de templates

É possível configurar o FaceIt para que a atualização dos templates seja efetuada automaticamente a cada vez que o usuário seja aceito pelo sistema em determinado intervalo de tempo, e desde que a amostra tenha atingido o valor limite mínimo para atualização automática determinado pelo administrador do sistema (Figura B.3). O sistema permite ainda a inserção manual de novas imagens para atualização do template (Figura B.4). Esta opção é recomendada quando há alterações no ambiente da tomada de dados (condições de iluminação, por exemplo) ou no sistema de captura da imagem (alterações da câmera ou placa de vídeo).

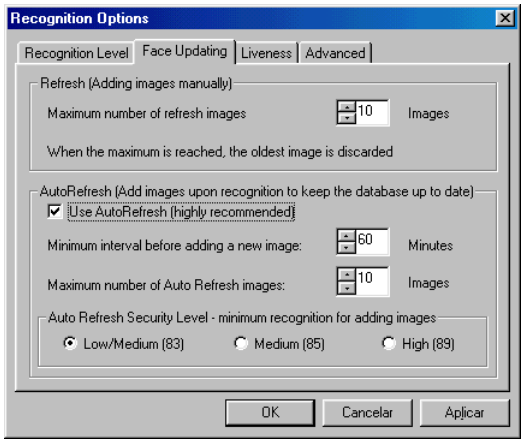

Figura B.3 – Configuração para atualização de templates

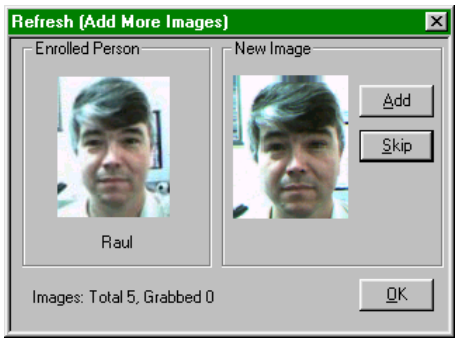

Figura B.4 – Inserção manual de novas imagens para atualização do template

B.2.4 – Teste para prova de vida

O teste para prova de vida é utilizado para determinar se o que foi apresentado ao sistema é a imagem de uma pessoa real, viva, e não, por exemplo, uma fotografia ou uma máscara. O teste para prova de vida ocorre após a identificação da face e antes que o acesso seja liberado. O sistema solicita que o usuário fique inicialmente imóvel, e posteriormente faça pequenos movimentos com a face, como sorrir ligeiramente, piscar os olhos ou erguer as sobrancelhas. As figuras B.5 e B.6 mostram a operação do teste para prova de vida no FaceIt.

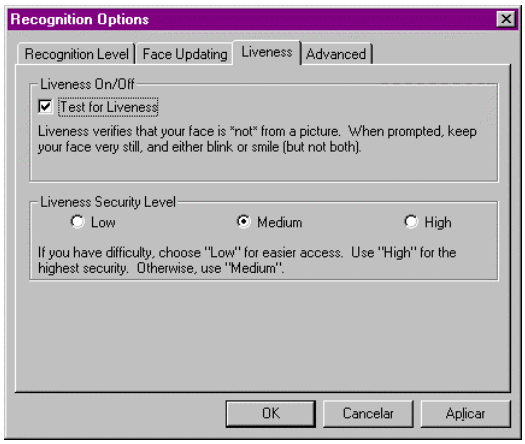

Figura B. 5 - Configuração do teste para prova de vida

Figura B. 6 - Teste para prova de vida em operação

B.2.5 – Operação do sistema

A operação do sistema é bastante simples, tanto para o administrador como para o usuário final. O sistema possui um eficiente esquema de orientação ao usuário para que as imagens da face obtidas para a geração do template tenham a melhor qualidade possível (Figura B.7). Durante o cadastramento, é possível selecionar quais imagens entrarão na composição do template (Figura B.8), tornando o processo de aquisição das imagens mais preciso. Após a geração do template inicial, o software executa um teste de reconhecimento, a partir de movimentos da face e variações de expressão, adicionando ainda mais algumas imagens para a geração do template final (Figura B.9).

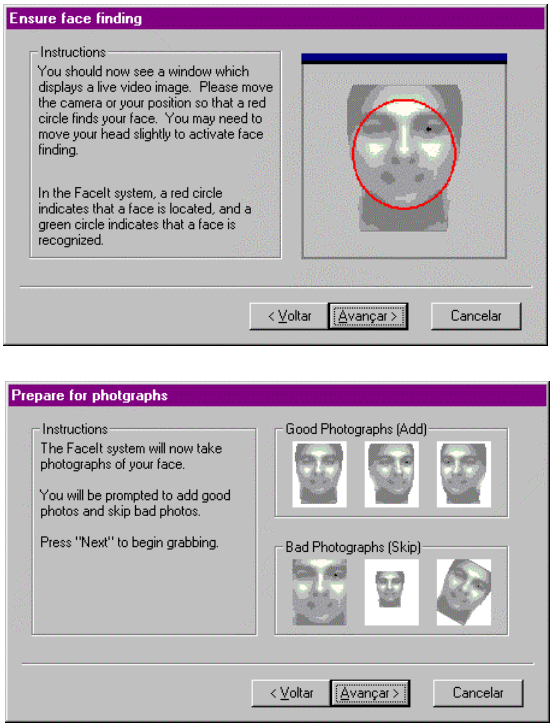

Figura B.7 - Orientação para melhor obtenção de imagens da face

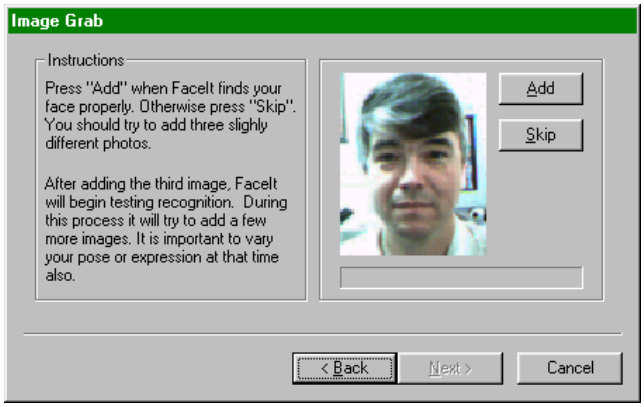

Figura B. 8 - Seleção de imagens iniciais para a composição do template

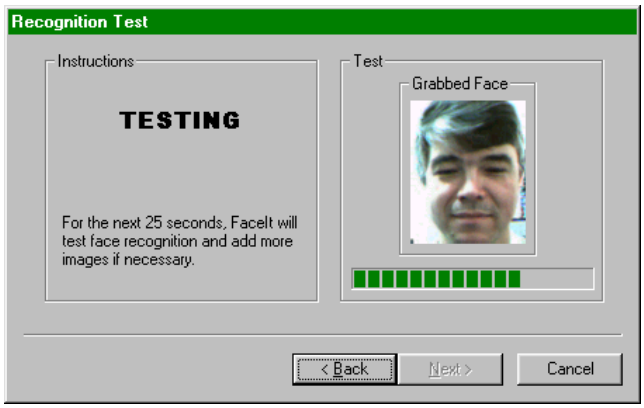

Figura B. 9 - Teste de reconhecimento da face durante o cadastramento

A versão do FaceIt utilizada neste experimento realiza somente a operação de identificação de usuários e, por ser uma versão de demonstração, permite a utilização de somente cinco usuários simultaneamente.

B.3 – Descrição do teste

B.3.1 – População

A população que participou deste experimento foi composta de 29 usuários, todos de pele clara, com idades variando de 19 a 47 anos, sendo 8 do sexo feminino e 21 do sexo masculino. Todos os usuários tinham grau de instrução mínimo de 2º grau completo.

Os usuários foram previamente orientados e treinados, tendo pleno conhecimento do objetivo dos testes e do funcionamento do sistema, e foram também supervisionados

durante todo o processo. Pelo caráter da experiência, os usuários eram não só cooperativos como ansiosos por colaborar.

B.3.2 – Procedimento

O experimento foi executado utilizando-se uma câmera digital Color QuickCam™ da Connectix, com resolução de 640 x 480 pixels para 24 bits de cor, em sala fechada com iluminação controlada.

Cada usuário foi cadastrado e, imediatamente após o cadastramento, verificado pelo sistema, o que garantiu que as condições do ambiente no momento da apresentação das novas amostras fossem exatamente iguais às do momento do cadastramento do usuário. No momento do cadastramento todos os usuários já haviam sido treinados sobre o funcionamento do sistema e sobre como proceder no momento da tomada de dados, sendo que a grande maioria já havia assistido ao processo de cadastramento de outros usuários. O cadastramento foi rigidamente supervisionado, e todas as imagens de cadastro obtidas seguiram os padrões de qualidade sugeridos pelo software.

Durante a apresentação de novas amostras ao sistema para verificação do usuário, modificações intencionais na aparência da face foram inseridas, com o objetivo de observar a incidência de **falsa rejeição** no reconhecimento da face original. Estas alterações incluíram:

- Utilização de óculos;
- variações na expressão facial;
- alterações no contorno da cabeça, através da utilização de acessórios como peruca e gorro, e de modificação no estilo de penteado;
- alterações no contorno da face, através da utilização de cachecol;
- rotação da face.

Para a avaliação da incidência de **falsa aceitação** foram apresentada fotografias frontais dos usuários no formato 3x4.

Como o sistema permite a utilização de apenas cinco usuários ativos simultaneamente e não possui opção de autenticação, para os testes de cada usuário foram escolhidos aleatoriamente mais quatro usuários do mesmo sexo para compor o conjunto de cinco usuários ativos, e os usuários restantes foram bloqueados. A verificação então foi realizada nestes grupos de cinco usuários. Eventualmente um único usuário do outro sexo era incluído no grupo.

O software foi configurado para nível de segurança baixo, o que teoricamente deveria permitir um índice mínimo de falsa rejeição. A opção de atualização automática de templates estava habilitada. A opção de teste para prova de vida estava desabilitada, permitindo a apresentação de fotografias dos usuário aos sistema.

B.4 Apresentação dos resultados

B.4.1 – Apresentação dos resultados

Um resumo dos resultados obtidos neste experimento é apresentado na Tabela B.3. A Tabela B.4 apresenta as ocorrências de falsa aceitação não planejadas registradas durante este experimento. Ambas as tabelas são apresentadas no final deste Apêndice.

B.4.2 – Tabulação dos resultados

A tabulação dos resultados obtidos neste experimento é apresentada a seguir na Tabela B.2.

	Óculos		Expressão facial				Contorno da cabeça						Contorno da face		Rotação da face		Fotografia	
			Sorriso		Outra		Peruca		Gorro		Penteado							
	☺	☹	☺	☹	☺	☹	☺	☹	☺	☹	☺	☹	☺	☹	☺	☹	☺	☹
Usuários	29		29		29		29		29		17		28		29		29	
Total	25	4	14	15	13	16	1	28	2	27	5	12	14	14	12	17	6	23
%	86	14	48	52	45	55	3	97	7	93	29	71	50	50	41	59	21	79
Erro	FR **0,14**		FR **0,52**		FR **0,55**		FR **0,97**		FR **0,93**		FR **0,71**		FR **0,5**		FR **0,59**		FA **0,21**	

Legenda: ☺ - Usuários reconhecidos; ☹ - Usuários não reconhecidos; FR – Falsa rejeição; FA – Falsa aceitação

Tabela B.2 – Tabulação dos resultados.

B.5 Análises e conclusões

A administração e operação do FaceIt é bastante simples. O cadastramento e a tomada de dados supervisionados permitiram que as imagens obtidas fossem de boa qualidade e impediram que erros dos usuários, como mau posicionamento da face ou correção de foco da câmera influenciassem na performance do sistema.

Os sistemas de reconhecimento de face de um modo geral permitem a tomada de dados sem a colaboração do usuário, e este é o caso do FaceIt. O sistema é capar de identificar faces em movimento na cena, com inclinação e alteração de expressão facial sutis, mas obtém melhores resultados se o usuário for cooperativo ou estiver sob supervisão constante, resultando em tomadas de imagens de boa qualidade. Por este motivo, nenhuma das ocorrências de falsa rejeição foi resultado de falha na interação dos usuários com o sistema, uma vez que estes estiveram sob supervisão e orientação constantes.

A aproximação e o afastamento do usuário da câmera foram compensados naturalmente pelo sistema. Apesar disto, grandes aproximações não permitiram correção do foco, acarretando baixa qualidade de imagem e conseqüente não reconhecimento do usuário.

Grandes afastamentos tornaram o tamanho da imagem da face na cena muito reduzido, impedindo que a face fosse localizada. Estes testes não foram considerados na elaboração da Tabela B.3.

Conforme previsto, a utilização de óculos não impediu o reconhecimento dos usuários, desde que as lentes permitissem a visualização dos olhos. Também conforme previsto, alterações na posição da face, dependendo da inclinação, causaram falsa rejeição dos usuários, mas o sistema foi capaz de compensar variações rotacionais pequenas. Variações extremas nas expressões faciais impediram que os usuários fossem corretamente reconhecidos e, em algumas situações, mesmo pequenas variações nas expressões faciais acarretaram falsa rejeição do usuário.

A utilização de peruca e gorro foi quase implacável em sua influência no reconhecimento dos usuários: somente 3% dos usuários com peruca e 7% dos usuários com gorro foram reconhecidos. Este fato nos leva a concluir que estes acessórios alteraram expressivamente o contorno da cabeça, que teria grande importância no aspecto geral da face para o sistema. A alteração do contorno inferior da face, através da utilização de cachecol, também interfere no aspecto geral da face, mas sua influência no ocasionamento de falsa rejeição é menor: 50% dos usuários que utilizaram cachecol foram reconhecidos pelo sistema.

Em função do teste para prova de vida ter sido desabilitado, foi possível a apresentação e aceitação de fotografias dos usuários pelo sistema. Em alguns casos, com fotografia recente e de boa qualidade, o sistema reconheceu a fotografia como um usuário legítimo. O fato de alguns usuários não terem sido reconhecidos por sua fotografias pode ter ocorrido em função da baixa qualidade das fotografias ou por estas fotografias estarem desatualizadas.

Para este experimento, não foi possível a avaliação de algumas variáveis apresentadas por alguns grupos de exceção. Estes grupos podem apresentar características especiais que, mesmo não intencionalmente, afetam a performance do sistema. Estas variáveis estariam presentes na operação normal do sistema, e são descritas a seguir:

Possibilidade de falsa aceitação:

- Irmão gêmeos ;
- pessoas extremamente parecidas .

Possibilidade de falsa rejeição

- Pessoas de pele muito escura, que dificulta a distinção das características faciais;
- envelhecimento natural, após muito tempo sem atualização do template.

Adicionalmente, este experimento não contemplou a avaliação da utilização de máscaras, maquiagem ou qualquer outro recurso que permita a um usuário não autorizado simular a face de um usuário legítimo. Apesar disto, em várias circunstâncias, apresentadas na Tabela B.4, o sistema permitiu que um usuário fosse reconhecido como sendo outro usuário legítimo. As ocorrências não planejadas de falsa aceitação tiveram incidência considerável - pelo menos 11 dos 29 usuários foram reconhecidos como sendo outro usuário em alguma ocasião. Como somente 5 usuários

poderiam ser habilitados simultaneamente, o número de comparações entre usuários foi restrito aos usuários aleatoriamente escolhidos para cada grupo, o que nos faz concluir que a incidência de falsa aceitação teria sido bem maior caso o sistema permitisse a habilitação de todos os usuários simultaneamente.

O fato de o sistema ter sido configurado para nível de segurança baixo teoricamente ocasionaria o menor índice possível de falsa rejeição, que ainda assim mostrou-se bastante significativo e suscetível a variações não muito drásticas na aparência da face. O grande número de falsas aceitações não planejadas também foi resultado desta mesma configuração de nível de segurança. Para que a incidência de falsas aceitações fosse menor, seria necessário aumentar o nível de segurança do sistema, o que tornaria a incidência de falsas rejeições ainda mais crítica

A partir deste experimento, foi possível avaliar que é extremamente simples enganar intencionalmente o sistema, alterando a aparência da face, naturalmente ou através de características físicas impostas, ocasionando falsa rejeição do usuário. Desta forma, este tipo de sistema biométrico não deve ser utilizado quando a intenção é realizar uma identificação negativa, ou seja, garantir que um determinado usuário NÃO é conhecido pelo sistema.

TABELA B.3 – APRESENTAÇÃO DOS RESULTADOS

TABELA B.4 – OCORRÊNCIAS DE FALSA ACEITAÇÃO NÃO PLANEJADAS.

Bibliografia

[ADA 97] ADAMI, André Gustavo. **Sistema de reconhecimento de locutor utilizando redes neurais artificiais**. Porto Alegre: Universidade Federal do Rio Grande do Sul, Instituto de Informática, 1997.

[ALL 99] ALLEN, Carole. **Big brother and the midlife identity crisis**. Disponível em http://www.government.ibm.com/GOV/AIS.nsf/ . Acesso em 29 jan. 1999.

[ASH 99] ASHBOURN, Julian. **Implementing biometric systems**. Disponível em http://www.afb.org.uk/public/ja00002.html . Acesso em 05 nov. 1999.

[ASS 98] ASSOCIATION FOR BIOMETRICS. **Site institucional**. Disponível em http://www.afb.org.uk/ . Acesso em 30 set 1998.

[AUD 97] AUDIO- AND VIDEO-BASED BIOMETRIC PERSON AUTHENTICATION – INTERNATIONAL CONFERENCE, 1., 1997, Crans-Montana, Suiça. **Proceedings...** Berlin: Springer, 1997.

[BIO 98] BIOMETRIC CONSORTIUM. **Site institucional**. Disponível em http://www.biometrics.org/ . Acesso em 30 out. 1998.

[BIP 99] BIOMETRIC PARTNERS, INC. **About fingerprints**. Disponível em http://www.biometricpartners.com/Finger_Prints/finger_prints.html . Acesso em 11 out. 1999.

[BRU 93] BRUNELLI, R.; POGGIO, T. **Face recognition through geometrical features**. Trento, Itália: Istituto per la Ricerca Scientifica e Tecnologica, 1993.

[BRU 93a] BRUNELLI, R.; POGGIO, T. **Face recognition**: features versus templates. Trento, Itália: Istituto per la Ricerca Scientifica e Tecnologica, 1993.

[BRU 93b] BRUNELLI, Roberto; FALAVIGNA, Daniele. **Person identification using multiple clues**. Istituto per la Ricerca Scientifica e Tecnologica, Trento, Italia. 1993.

[BRU 93c] BRUNELLI, R.; FALAVIGNA, D.; STRINGA, L.; POGGIO, T. **Automatic person recognition by using acoustic and geometric features**. Trento, Itália: Istituto per la Ricerca Scientifica e Tecnologica, 1993. (Relatório técnico 9307-43)

[BUR 99] BURGE, Mark; BURGER, Wilhelm. Ear Biometrics. In: JAIN, Anil. **Biometrics – Personal identification in networked society**. Boston: Kluwer Academic Publishers, 1999. p. 274-285.

[CAM 99] CAMPBELL, Joseph P., Jr. Speaker Recognition. In: JAIN, Anil. **Biometrics – Personal identification in networked society**. Boston: Kluwer Academic Publishers, 1999. p.165-189.

[CAM 99a] CAMPBELL, Joseph P. Jr.; ALVEA, Lisa A.; DUNN, Jeffrey S. **Government Applications and Operations**. Disponível em http://www.biometrics.org/REPORTS/CTSTC96/ . Acesso em 04 nov. 1999.

[COB 96] COBB, Stephen. **The NCSA guide to PC and LAN security**. Nova York: McGraw-Hill, 1996.

[COM 98] COMPUTER-BASED PATIENT RECORD INSTITUTE. **Glossary of terms related to information security in computer-based patient record systems**. Disponível em http://www.cpri.org/docs/glossary.html . Acesso em 28 maio 1998.

[DAS 98] DAVIES, Simon G. Touching big brother - how biometric technology will fuse flesh and machine. **Information Technology & People**, [S.l.], v. 7, n. 4, 1994. Disponível em http://www.privacy.org/pi/reports/biometric.btml . Acesso em 29 jul. 1998.

[DAU 99] DAUGMAN, John. Recognizing persons by their iris patterns. In: JAIN, Anil. **Biometrics – Personal identification in networked society**. Boston: Kluwer Academic Publishers, 1999. p. 103-121.

[DAV 99] DAVIS, Ann. **The body as password**. Disponível em http://www.wired.com/wired/5.07/biometrics.html . Acesso em 30 nov. 1999.

[DER 99] IDENTIFICATION SYSTEMS DERMALOG. **Site comercial**. Disponível em http://www.dermalog.de/ . Acesso em 30 set. 1999.

[DOH 98] DOHERTY, Kate. **Is it really you?** Disponível em http://www.securitysolutions.com/category/corporate/biometrc.htm . Acesso em 27 jul. 1998.

[EYE 99] EYEDENTYFY INC. **Site comercial**. Disponível em http://www.eyedentify.com/.. Acesso em 05 mar. 1999.

[FAC 98] VISIONICS CORPORATION. **Site comercial**. Disponível em http://www.visionics.com/ . Acesso em 24 ago. 1998.

[FED 85] FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION 112. **Password Usage**. 1985. Disponível em http://www.nist.gov/itl/lab/fips/ . Acesso em 20 fev. 1998.

[FED 91] FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION 190. **Guideline for the use of advanced authenttication technologies**. 1991.Disponível em http://www.nist.gov/itl/lab/fips/ . Acesso em 20 fev. 1998.

[GAL 98] GALLAGHER, Patrick R. **Guide to understand identification and authentication in trusted systems**. National Computer Security Center. Disponível em http://bilbo.isu.edu/security/isl/idenauth.html . Acesso em 20 fev. 1998.

[HAY 99] HAYS, Ronald J. **INS Passenger Accelerated Service System (INSPASS).** Disponível em http://www.biometrics.org/REPORTS/INSPASS.html. Acesso em 07 nov. 1999.

[HEN 97] HENDRY, Mike. **Smartcard security and applications**. Boston. Artech House, 1997.

[HIL 99] HILL, Robert "Buzz". Retina identification. In: JAIN, Anil. **Biometrics – Personal identification in networked society**. Boston: Kluwer Academic Publishers, 1999. p. 123-141.

[HON 99] HONG, Lin; JAIN, Anil K. Multimodal Biometrics. In: JAIN, Anil. **Biometrics – Personal identification in networked society**. Boston: Kluwer Academic Publishers, 1999. p.328-344.

[INC 99] INTERNATIONAL COMPUTER SECURITY ASSOCIATION. **ICSA Commercial Biometric Certification Program V 1.01**. Disponível em http://www.icsa.net/services/consortia/cbdc/program.shtml . Acesso em 20 jan. 1999.

[INT 99] INTERNATIONAL BIOMETRIC INDUSTRY ASSOCIATION. **Site institucional.** Disponível em http://www.ibia.org/ . Acesso em 01 set. 1999.

[IOS 00] I/O SOFTWARE INC. **Site Comercial**. Disponível em http://www.iosoftware.com/ . Acesso em 02 jan. 2000.

[IRI 99] IRISCAN INC. **Site Comercial.** Disponível em http://www.iriscan.com/ . Acesso em 02 jan. 1999.

[JAI 98] JAIN, A. K.; PRABHAKAR, S.; ROSS, A. **Biometrics-based web access**. EUA: Michigan State University. 1998. (TR98-33).

[JAI 99] JAIN, Anil; HONG, Lin; KULKARNI Yatin. **A multimodal biometric system using fingerprint, face and speech**. Trabalho apresentado na International Conference on Audio- and Video-based Biometric Authentication, 2., 1999, Washington.

[JAI 99a] JAIN, A. K.; BOLLE, R.; PANKANTI, S. Introduction to biometrics. In: JAIN, Anil. **Biometrics – Personal identification in networked society**. Boston: Kluwer Academic Publishers, 1999. p. 1-41.

[KAL 96] KALLE, Karu; JAIN, Anil. Fingerprint classification. **Pattern Recognition**, [S.l.],.v.29, n.3, p.389-404.

[KAU 95] KAUFMAN, Charlie. **Network security**: private communication in a public world. New Jersey. Prentice Hall PRT, 1995.

[LAB 96] LABAN, James. **Privacy issues surrounding personal identification systems**, [S.l.:s.n.], 1996.

[MCC 98] MCCHESNEY, John - host. **Your eyeball, please**: tired: passwords; wired: biometrics. Disponível em http://www.hotwired.com/synapse/hotseat/97/34/transcript2a.html. Acesso em 01 jul. 1998.

[MCD 94] MCDONALD, Jared. **Biometric authentication**. Nova Zelândia, Universidade de Otago, 1994. Disponível em http://spook.otago.ac.nz:800/members/jared/research/Honors/ . Acesso em 02 abr. 1998.

[MIR 98] MIROS INC. **Site comercial**. . Disponível em http://www.miros.com/ . Acesso em 24 ago. 1998.

[NAL 99] NALWA, Vishvjit S. Automatic on-line signature verification. In: JAIN, Anil. **Biometrics – Personal identification in networked society**. Boston: Kluwer Academic Publishers, 1999. p. 143-163.

[NEW 99] NEWMAN, Emma; BUNNEY, Calum; MEARNS, Carolan. **The biometrics report 1999**. New York: SJB Services, 1999.

[NUG 99] NUGER, Kenneth P. **Biometric applications**: legal and societal considerations. Disponível em http://www.engr.sjsu.edu/biometrics/private.html . Acesso em 24 nov. 1999.

[OGO 99] O´GORMAN, Lawrence. Fingerprint verification. In: JAIN, Anil. **Biometrics – Personal identification in networked society**. Boston: Kluwer Academic Publishers, 1999. p. 43-64.

[PAN 99] PANKANTI, Sharath; JAIN, Anil K.; ROSS; Arun**. A prototype hand geometry-based verification system**. Trabalho apresentado na International Conference on Audio- and Video-based Biometric Authentication, 2., 1999, Washington..

[PEN 98] PENOP INC. **Site comercial**. Disponível em http://www.penop.com/ . Acesso em 21 jul. 1998.

[POL 97] POLEMI, Despina. **Biometric techniques**: Review and evaluation of biometric techniques for identification and authentication, including an appraisal of the areas where they are most applicable. Athens: Institute of Communication and Computer Systems, National Technical University of Athens, 1997.

[PRO 99] PROKOSKI, Francine J.; RIEDEL, Robert B. Infrared identification of body parts. In: JAIN, Anil. **Biometrics – Personal identification in networked society**. Boston: Kluwer Academic Publishers, 1999. p. 191-212.

[RAT 95] RATHA, Nlini; CHEN, Shaoyun; JAIN, Anil. Adaptive flow orientation based feture extraction in fingerprint images. **Pattern Recognition Journal**, [S.l.], v.28, p.1657-1672, 1995.

[REC 99] REGOGITION SYSTEMS INC. **Site comercial**. Disponível em http://www.recogsys.com/ . Acesso em 23 fev. 1999.

[ROB 98] ROBACK, Ed. **Identification and Authentication**. NIST Computer Security Handbook, draft. Disponível em http://bilbo.isu.edu/security/isl/hk_i&a.html . Acesso em 20 fev. 1998.

[ROE 98] ROETHENBAUGH, Gary. **Biometrics explained**. Disponível em http://www.icsa.net/services/consortia/cbdc/explained.htm . Acesso em 31 mar. 1998.

[ROE 99] ROETHENBAUGH, Gary. **ICSA Biometric Buyer's Guide**. Disponível em http://www.icsa.net/services/consortia/cbdc/bg/ . Acesso em 20 jan. 1999.

[RUG 98] RUGGLES, Thomas. **Comparison of Biometric Techniques**. The Biometric Consulting Group. Disponível em http://www.biometric-consulting.com/bio.htm . Acesso em 01 jul. 1998.

[TEC 98] TECNOLOGY RECOGNITION SYSTEMS, INC. **Site comercial**. Disponível em http://www.betac.com/trs/ . Acesso em 28 jul. 1998.

[THE 99] THE BIOMETRIC CONSULTING GROUP. **Site institucional**. Disponível em http://www.biometric-consulting.com/ . Acesso em 22 out. 1999.

[TYL 99] TYLER, Christopher; MILLER, Richard. **Computational approaches to face recognition**. Disponível em http://www.ski.org/CWTyler_lab/ARVO/FaceRecog/FaceRecog.html . Acesso em 30 out 1999.

[UNI 98] UNISYS. **BioWare Glossary**. Disponível em http://www.marketplace.unisys.com/bioware/glossary.html . Acesso em 26 ago. 1998.

[UNI 99] UNISYS. **BioWare - Social sevices solution profiles**: Spain plays it smart with smart cards. Disponível em http://www.marketplace.unisys.com/bioware/tass.html. Acesso em 07 nov. 1999.

[VER 98] VERITEL CORPORATION. **Site comercial**. Disponível em http://www.veritelcorp.com/ . Acesso em 15 jul. 1998.

[WAY 99] WAYMAN, James L. **Fundamentals of biometric technologies**. U.S. National Biometric Test Center, College of Engeneering, San Jose State University. Disponível em http://www.engr.sjsu.edu/biometrics/testing.html . Acesso em 07 nov. 1999.

[WAY 99a] WAYMAN, James L. **"Degrees of freedom" as related to biometric device performance**. U.S. National Biometric Test Center, College of Engeneering, San Jose State University. Disponível em http://www.engr.sjsu.edu/biometrics/freedom.html . Acesso em 07 nov. 1999.

[WEN 99] WENG, John J. Face recognition. In: JAIN, Anil. **Biometrics – Personal identification in networked society**. Boston: Kluwer Academic Publishers, 1999. p. 65-86.

[ZUN 99] ZUNKEL, Richard L. Hand geometry based verification. In: JAIN, Anil. **Biometrics – Personal identification in networked society**. Boston: Kluwer Academic Publishers, 1999. p. 87-101.