UNIVERSIDADE FEDERAL DE SANTA CATARINA
PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO

Juliano Fontoura Kazienko

Assinatura Digital de Documentos Eletrônicos Através da Impressão Digital

Dissertação submetida à Universidade Federal de Santa Catarina como parte dos requisitos para a obtenção do grau de Mestre em Ciência da Computação.

Prof. Ricardo Felipe Custódio, Dr.
Orientador

Florianópolis, Fevereiro de 2003

Assinatura Digital de Documentos Eletrônicos Através da Impressão Digital

Juliano Fontoura Kazienko

Esta Dissertação foi julgada adequada para a obtenção do título de Mestre em Ciência da Computação, área de concentração Sistemas de Computação e aprovada em sua forma final pelo Programa de Pós-Graduação em Ciência da Computação.

Prof. Fernando Ostuni Gauthier, Dr.
Coordenador do Curso

Banca Examinadora

Prof. Ricardo Felipe Custódio, Dr.
Orientador

Prof. Carlos Roberto De Rolt, Dr.

Prof. Clovis Torres Fernandes, Dr.

”Ó abismo de riqueza, de sabedoria e de ciência em Deus! Quão impenetráveis são os seus juízos e inexploráveis os seus caminhos! Quem pode compreender o pensamento do Senhor? Quem jamais foi seu conselheiro? Quem lhe deu primeiro, para que lhe seja retribuído? Dele, por ele e para ele são todas as coisas. A ele a glória por toda a eternidade! Amém.” ROMANOS 11,33-36.

Para meus pais, Albino e Edla, que me conduziram desde cedo ao maravilhoso mundo do saber.

Agradecimentos

À Polícia Civil Catarinense, instituição à qual pertenço, que me serviu de forma definitiva para a construção deste trabalho. Especialmente, ao setor Perícia Criminalística da Delegacia Regional de Polícia de Chapecó/SC, onde fui recebido com amizade e coleguismo. Agradeço à Perita Criminal Marli Canello Modesti pelas várias oportunidades em que conversamos acerca das impressões digitais.

Ao meu chefe, Delegado Eduardo Pianalto de Azevedo, por compreender a necessidade de me ausentar em determinados momentos, e aos demais colegas de trabalho que, de uma forma ou outra, colaboraram para a realização deste projeto.

À Polícia Federal, na pessoa do Sr. José Carlos Nedel Fagundes, Papiloscopista da Polícia Federal, que desde o nosso primeiro contato se mostrou receptivo e entusiasmado com o tema desta dissertação.

Ao colega de equipe Felipe Pompeo Pereira, por sua importante companhia na realização das atividades de pesquisa e desenvolvimento.

Ao professor orientador, Dr. Ricardo Felipe Custódio, pelo seu companherismo e incentivo na realização desta dissertação de mestrado. Nesse período ímpar da minha vida, tive acesso ao mundo da ciência pelas mãos de uma pessoa dinâmica, inteligente e, acima de tudo, um grande amigo. Tenha certeza, professor, que, apesar das limitações, esforcei-me ao máximo para corresponder-lhe à altura.

Aos estimados amigos Maria Anésia e Dalsin dos Santos, pessoas maravilhosas. Conhecê-los é uma dádiva divina que guardo no coração.

Aos meus pais, explicação das minhas maiores conquistas.

A Deus, por nos permitir todas as realizações.

Sumário

Lista de Figuras

Lista de Tabelas

Lista de Siglas e Operadores

AC Autoridade Certificadora

AFIS *Automated Fingerprint Identification System*

ANSI *American National Standards Institute*

AR Autoridade de Registro

ARID Análise e Reconhecimento de Impressões Digitais

BAI *Biometric Associates Inc.*

BO Boletim de Ocorrência

BOES Boletim de Ocorrência Eletrônico Seguro

BSP *Biometric Service Provider* ou Provedor de Serviço Biométrico

CEFET-PR Centro Federal de Educação Tecnológica do Paraná

CD-ROM *Compact Disk - Read Only Memory*

CSP *Cryptographic Service Provider* ou Provedor de Serviço Criptográfico

D Deciframento

DOC Documento ou mensagem eletrônica

E Cifração

FBI *Federal Bureau of Investigation*

FD Fórmula Datiloscópica

FIPS *Federal Information Processing Standards*

FIR *Fingerprint Identification Record*

G Gerador de um par de chaves: uma pública; outra privada

H(DOC) ou H(M) Incidência de uma função de resumo sobre um documento ou mensagem eletrônica

H(senha) Resumo de uma senha entrada no momento da autenticação

H(senha1) Resumo de uma senha armazenado no cartão

HASH Resumo

ICP Infra-estrutura de Chave Pública

ICP-Brasil Infra-estrutura de Chaves Públicas Brasileira

ID Certificado digital do usuário

ITU *International Telecommunication Union*

ITU-T *ITU Telecommunication Standardization Sector*

K_R Chave privada de criptografia assimétrica

K_S Chave de sessão de criptografia simétrica

K_U Chave pública de criptografia assimétrica

M Documento ou mensagem eletrônica

MD5 *Message Digest 5*

NFIS *Nist Fingerprint Image Software*

NIST *National Institute of Standards and Technology*

NSA *National Security Agency*

PGP *Pretty Good Privacy*

PIN *Personal Identification Number*

PKI *Public Key Infrastructure*

RAM *Random Access Memory*

RSA Rivest-Shamir-Adelman

S Assinatura Digital

SSP/SC Secretaria da Segurança Pública de Santa Catarina

SSP/SP Secretaria da Segurança Pública de São Paulo

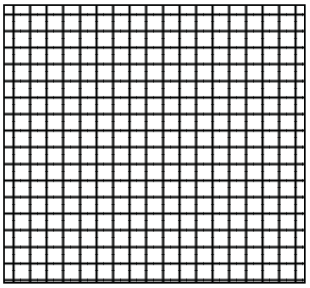
template1 *Template* de impressão digital armazenado no cartão

template2 *Template* de impressão digital adquirido no momento da autenticação

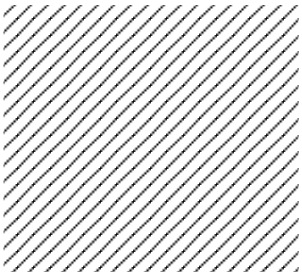
V Verificação da assinatura digital

$\|$ Concatenação

Lista de Símbolos



1. Sensor de impressão digital baseado em *chips* de silício



2. Indicação da incidência de uma cifra

Resumo

O objetivo geral desta dissertação é utilizar a impressão digital para a verificação da identidade do usuário quando da assinatura de documentos eletrônicos. A impressão digital possui características únicas que permitem estabelecer a identidade de uma pessoa. Com esse propósito também foi considerada a técnica para a composição das assinaturas digitais, baseada no uso de criptografia por chave pública. A assinatura digital propicia integridade e autenticidade aos documentos assinados. No entanto, é proposto o uso da impressão digital como forma de aprimorar a segurança do processo de autenticação de usuário durante a assinatura do documento eletrônico. Essa forma de autenticação proposta visa ao gerenciamento seguro da chave criptográfica necessária para assinar documentos e ao fortalecimento da ligação entre esta chave criptográfica e seu proprietário. Propõe-se um sistema seguro para a assinatura de documentos eletrônicos baseado não só no uso de impressões digitais, mas também na utilização de senhas e de cartões. Neste trabalho, é mostrado através de um sistema desenvolvido a viabilidade técnica e prática da assinatura digital de documentos eletrônicos utilizando a impressão digital. A partir daí, propõe-se uma aplicação prática do modelo desenvolvido relativa ao registro de ocorrências policiais da Polícia Civil do Estado de Santa Catarina.

Abstract

The general objective of this dissertation is to use the fingerprint for the verification of the user's identity when of the electronic documents signature. The fingerprint possesses only characteristics that allow to establish the identity of a person. With it purpose also was analyzed the technique for the composition of the digital signatures based on the use of public key cryptography. The digital signature offers integrity and authenticity to the signed documents. However, the use of the fingerprint is proposed as form of improving the safety of the process of user's authentication during the signature of the electronic document. This authentication form proposal seeks to the secure management of the cryptographic key necessary to sign documents and to the strengthen of the connection between this cryptographic key and your owner. This work presents one secure system for the signature of electronic documents based not only in the use of fingerprints, but also in the use of passwords and of cards. In this work, it's shown through a developed system the technical and practical viability of the digital signature of electronic documents using fingerprints. So, is proposed a practical application of the system to Civil Police of the Santa Catarina State.

Capítulo 1

Introdução

O avanço tecnológico tem provocado constantes reestruturações da sociedade. Dentre as evoluções da era da informação, pode-se seguramente destacar a grande rede de computadores - a Internet. Ela liga o mundo de ponta a ponta, facilitando a comunicação interpessoal. Porém, junto com os progressos da ciência surgem os desafios. Uma questão importante é como estabelecer a identidade das pessoas com quem se comunica, especialmente em uma rede tão vasta como a Internet.

O foco de pesquisa desta dissertação é estabelecer um mecanismo que permita aprimorar a identificação de pessoas quando da assinatura digital de documentos eletrônicos usando impressões digitais. Na Seção 1.1, o contexto no qual está inserido o foco de pesquisa deste trabalho é mostrado. Na Seção 1.2, os objetivos desta dissertação são arrolados. Na Seção 1.3, são apresentados os aspectos que motivaram a realização deste estudo. Na Seção 1.4, são apresentadas as metodologias e ferramentas utilizadas e, na Seção 1.5, expõe-se o conteúdo deste trabalho.

1.1 Contexto da Pesquisa

O Laboratório de Segurança em Computação - LabSEC vem desenvolvendo em conjunto com o Laboratório de Informática Jurídica - Linjur, ambos da Universidade Federal de Santa Catarina, um projeto para que seja possível o oferecimento

de serviços equivalentes aos dos cartórios convencionais via Internet. O projeto, denominado Cartório Virtual, está subdividido em vários subprojetos: Sistema de Atendimento ao Cliente (SAC) Seguro, Autoridade de Aviso, Selo Digital, Autoridade de Datação, entre outros. Esta dissertação situa-se dentro da área de Assinatura Digital através da Impressão Digital, conforme ilustrado na Figura 1.1 [BOR 02, DAN 01].

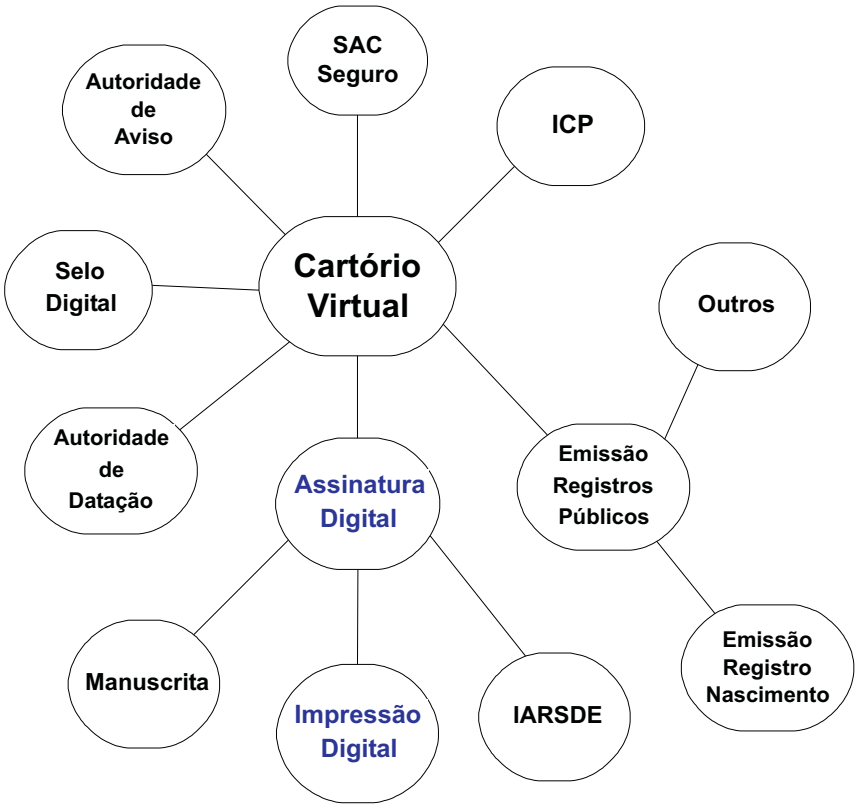


Figura 1.1: Contexto geral do projeto Cartório Virtual.

Neste trabalho, apresenta-se um sistema desenvolvido que usa a técnica de assinatura digital com a finalidade de certificar a origem de uma mensagem eletrônica e garantir a integridade dos dados assinados. Nesses métodos, tem-se um certo grau de confiabilidade, mas que se gostaria de aumentar essa certeza. Daí, a sugestão de usar métodos biométricos, em especial da impressão digital, que é o método biométrico mais difundido e com grande grau de aceitabilidade do seu uso. Vários estudos e aplicações tem sido desenvolvidas acerca do reconhecimento de impressões digitais auxiliado por computador.

A autenticação é, ou deveria ser, parte integrante de qualquer sistema computacional. Saber com ”quem se conversa” é uma importante recomendação que também deveria ser observada no mundo virtual, uma vez que as comunicações de dados são efetuadas, na maioria das vezes, remotamente.

Consciente do importante papel que ocupa a verificação da identidade de pessoas dentro dos sistemas de informação, buscam-se métodos de autenticação na literatura, dentre os quais se destacam os seguintes: assinatura digital, senhas, cartões inteligentes, sistemas biométricos. Neste trabalho, procura-se, através da associação desses métodos, compor um sistema para assinatura de documentos eletrônicos que ofereça uma maior certeza no estabelecimento da identidade de um usuário. Tal sistema proposto é apresentado de maneira detalhada no capítulo 5.

1.2 Objetivos

Esta seção destina-se a apresentação dos objetivos desta dissertação. O objetivo geral é mostrado na Subseção 1.2.1, enquanto os objetivos específicos são mostrados na Subseção 1.2.2.

1.2.1 Objetivo Geral

O objetivo deste trabalho é utilizar a impressão digital para autenticar a identidade do usuário no processo de assinatura digital de documentos eletrônicos.

1.2.2 Objetivos Específicos

São os seguintes os objetivos específicos:

- Revisão da Técnica de Datiloscopia.
- Descrever a tecnologia AFIS.
- Revisão da Técnica de Assinatura Digital.

- Estado atual do reconhecimento de impressão digital no Brasil.
- Descrever os sistemas comerciais e padrões existentes para o reconhecimento automático de impressão digital.
- Descrever o estado da arte em termos de tecnologias de reconhecimento automático de impressão digital.
- Propor um modelo para assinatura digital de documentos eletrônicos utilizando autenticação da identidade do usuário via impressão digital.
- Elaborar protótipo de um sistema computacional para o modelo proposto.
- Estender o modelo proposto visando ao registro de ocorrências policiais, como forma de mostrar uma aplicação prática para o modelo desenvolvido.

1.3 Motivação

É crescente a procura por métodos que proporcionem segurança em computação [LIU 01b]. Isso se deve a inúmeras razões, dentre as quais pode-se citar o furto de informações como o furto do nº do cartão de crédito, violação do sigilo das comunicações de dados, falsificação da identidade e fraudes de toda ordem. Diante desse contexto, há um grande esforço por parte da comunidade científica a fim de incrementar a segurança no mundo digital.

O desenvolvimento do comércio eletrônico é outro fator que contribui para o aumento da demanda por métodos que proporcionem segurança como, por exemplo, a criptografia. Nas transações comerciais através da Internet, torna-se extremamente importante que ocorra a certificação da identidade entre as partes, uma vez que obrigações e direitos para ambas certamente serão gerados a partir da relação comercial eletrônica. Também, é necessário que informações pessoais, como o número do cartão de crédito de um usuário, trafeguem pela rede de maneira confidencial da origem até o seu destino e permaneçam assim.

Outro aspecto atrelado diretamente à autenticação é o controle de acesso a programas de computador e a ambientes físicos. Dessa forma, é possível, através do reconhecimento da impressão digital ou da íris, controlar o acesso a salas de acesso restrito [PHI 00, LIU 01b]. De outra forma, a impressão digital pode ser utilizada em um processo de assinatura digital de mensagens eletrônicas, aprimorando assim a etapa de reconhecimento da identidade do usuário. A literatura científica faz referência ao uso de impressões digitais e cartões inteligentes em um ambiente de assinatura digital de documentos eletrônicos [Iso 01].

A utilização de assinatura digital é importante dentro de um sistema de identificação porque possibilita verificar a origem da mensagem e a sua integridade [STA 99]. Outros métodos de autenticação como, por exemplo, a biometria não permitem por si só verificar a integridade de uma mensagem eletrônica. Por outro lado, existe o problema da personificação de identidades alheias que poderia ser dificultada através do uso de características biométricas em combinação com assinatura digital. Assim ter-se-ia uma maior grau de certeza de que foi realmente um determinado usuário quem assinou uma mensagem eletrônica, uma vez que tenha sido requerida, por exemplo, sua impressão digital para que pudesse efetuar a assinatura de um documento eletrônico.

Para a Polícia Civil, de qualquer estado, é importante a identificação das pessoas pela impressão digital, principalmente para a elucidação da autoria de delitos e investigações criminais. Nesse sentido, a impressão digital vem sendo utilizada há tempos pelos organismos policiais para o estabelecimento da identidade de um indivíduo, por ser uma característica inerente a ele. Esse aspecto contribui para a inserção dos datilogramas no modelo para assinatura digital de documentos eletrônicos apresentado nesta dissertação.

1.4 Metodologias e Ferramentas

Na elaboração deste trabalho, foram realizados levantamentos acerca do uso das impressões digitais. Na Polícia Civil Catarinense, procurou-se detectar seu uso desde a confecção da carteira de identidade até a comparação de impressões digitais

latentes coletadas em locais de crime. Posteriormente, estudou-se o seu uso em alguns órgãos policiais do Brasil e do mundo. Também, buscou-se levantar os padrões existentes para a coleta, armazenamento, classificação e comparação de impressões digitais.

As atividades realizadas podem ser divididas em dois grupos:

- **Levantamento de Soluções**
  - A empresa COMPULETRA Ltda. foi visitada. Sediada na cidade de Porto Alegre/RS, ela oferece diversas soluções na área de biometria [COM 01]. Uma delas é o BioWeb®, produto que serve para a autenticação da identidade de pessoas na Internet por meio da impressão digital, a outra é o BioControl®, que se presta ao controle do acesso físico através de sensores biométricos usados junto a portas e catracas. Na empresa, pôde-se ver sensores de impresões digitais localizados em portas. Também, foi apresentado na oportunidade o serviço de *webmail* proporcionado através do sítio do ”Terra” , para o qual estava sendo implementada a autenticação de usuário via impressão digital. Essa visita permitiu verificar aplicações práticas para o uso de identificação pelas impressões digitais em sistemas de informação, bem como da associação da biometria com a criptografia na elaboração de sistemas seguros.
  - Com a finalidade de adquirir um leitor de impressão digital, foram realizados levantamentos e contatos com diversas empresas fornecedoras do produto. Uma delas foi a empresa JABUR HI-TECH, da qual o LabSEC efetuou a compra de um leitor de impressão digital acompanhado de ferramentas para desenvolvimento de *software*.
  - Foram estudadas ferramentas da área de criptografia visando à criação de um protótipo de sistema para assinatura de documentos eletrônicos através da impressão digital.
- **Contatos Para Uso de Sistemas**
  - Contatos realizados com o Núcleo de Identificação da Superintendência Regional do Departamento de Polícia Federal e com o Instituto de Identificação da

Polícia Civil de Santa Catarina, ambos sediados em Florianópolis/SC. Também, em diversas oportunidades, foram realizados contatos com colegas policiais civis dos setores de Identidade e de Perícia Criminalística da Delegacia Regional de Polícia de Chapecó/SC. Esses contatos permitiram conhecer os processos e sistemas nos quais as impressões digitais fazem parte.

– Foi realizado contato com o Grupo de Imagem do NIST [NIS 01]. Nessa interação, foi recebido gratuitamente um CD-ROM contendo *software* que faz a classificação e detecção de minúcias de imagens de impressões digital. No Apêndice B, aborda-se esse assunto.

– Foi realizado contato com a empresa *Biometric Associates* [ASS 02] a qual forneceu informação a respeito de *smart card* comercializado.

1.5 Conteúdo do Documento

Este trabalho foi organizado de acordo com a estrutura exposta nesta seção. No Capítulo 2, *Impressão Digital*, são apresentadas as técnicas envolvendo a datiloscopia. No Capítulo 3, *Conceitos de Criptografia*, são relacionados os fundamentos da criptografia e a técnica para a assinatura digital. No Capítulo 4, *Sistemas de Impressão Digital*, é descrito o uso de impressões digitais pelos organismos policiais e alguns padrões internacionais relacionados à área. No Capítulo 5, *Assinatura Digital usando a Impressão Digital*, é proposto um modelo para assinatura digital de documentos eletrônicos usando a biometria, além de mostrar-se um sistema relativo a esse modelo proposto. Além disso, pondera-se acerca da segurança dos documentos digitais. No Capítulo 6, *Boletim de Ocorrência Policial*, discorre-se sobre a possibilidade de que se faça o registro de ocorrência policial através da Internet utilizando a técnica de assinatura digital apresentada. No Capítulo 7, são feitas as *Considerações Finais* e conclusões sobre a relevância deste trabalho de pesquisa.

Também são relacionados no final deste documento alguns apêndices nos quais são tratados assuntos de relevância ao tema proposto. No Apêndice A, é abor-

dada a questão da criação de *Dedos Artificiais*. No Apêndice B, descreve-se um programa para processamento de imagens de impressão digital, o *Nist Fingerprint Image Software*, produzido pelo Instituto Nacional de Padrões e Tecnologia dos Estados Unidos.

Capítulo 2

Impressão Digital

Neste capítulo, são apresentadas as formas de autenticação da identidade de usuários. O método de autenticação biométrico é estudado, sendo colocado sobre enfoque a indentificação de pessoas a partir da impressão digital. Ao longo deste capítulo, procura-se estudar os aspectos que tornam possível a identificação de pessoas através dos datilogramas. É em virtude do caráter identificativo da impressão digital que considera-se o seu uso no modelo proposto para assinatura de documentos eletrônicos. É esse cunho identificativo que é estudado minuciosamente neste capítulo.

Na Seção 2.1, mostram-se os métodos de autenticação existentes. Na Seção 2.2, são apresentados aspectos relativos aos sistemas biométricos, seus tipos, algumas aplicações para a biometria, entre outras peculiaridades. Na Seção 2.3, ilustra-se a estrutura da pele humana. Na Seção 2.4, introduz-se a papiloscopia e suas áreas de estudo. Na Seção 2.5, o método de identificação datiloscópico é estudado de maneira detalhada. Na Seção 2.6, são descritos os sistemas automáticos para reconhecimento de impressões digitais. Na Seção 2.7, é realizada a conclusão deste capítulo.

2.1 Autenticação

Autenticação é a verificação da identidade [oC 94]. No contexto desta dissertação, autenticação corresponde a certificação da identidade de usuários [dHF 99].

Procedimentos que envolvem a autenticação estão freqüentemente presentes em nossa vida, seja na verificação da assinatura manuscrita constante em um contrato de locação de imóvel, ou ainda, no caixa eletrônico de um banco, onde o sistema bancário verifica a identidade do cliente para que o mesmo possa efetuar operações com sua conta, entre outras tantas situações do nosso cotidiano.

No âmbito computacional, a atividade de autenticação tem o mesmo sentido. Em ambientes de rede, em virtude dos crescentes ataques às diversas vulnerabilidades dos sistemas, tem-se procurado por métodos de autenticação cada vez mais eficientes. As redes de computadores proporcionam ao atacante ou falsário um certo grau de anonimato, o que, muitas vezes, acaba por estimular o ataque.

Por outro lado, existem mecanismos de segurança projetados para detectar, prevenir e recuperar de ataques à segurança: a criptografia e as funções de resumo de mensagem são exemplos disso [STA 99]. Junto com elas, a biometria pode ser de grande valia quando utilizada para a autenticação de usuário.

Na Tabela 2.1, são relacionados alguns tipos de autenticação existentes dentro da área de segurança. Vale destacar que os métodos baseados em (1) e (2) possuem vulnerabilidades à medida que possibilitam compartilhamento com terceiros, perda, esquecimento etc. Contudo, os métodos baseados em (3) proporcionam um processo de autenticação diferente, com base no que o indivíduo é ou faz, ou seja, algo que lhe está intrinsecamente relacionado [oC 94]. Os tipos (4) e (5) fundamentam-se na idéia de que o usuário deve estar localizado no tempo e no espaço para que seja possível a verificação da sua identidade. O último tipo de autenticação é aquele em que uma pessoa atesta quem você é.

2.2 Biometria

Biometria é o ramo da ciência que estuda a mensuração dos seres vivos. Em especial, entende-se por biometria a medida de características únicas do indivíduo que podem ser utilizadas para reconhecer sua identidade [LIU 01b]. Tais características podem ser tanto físicas como comportamentais. Estas incluem a assinatura manuscrita

Tabela 2.1: Métodos utilizados na verificação da identidade.

Método baseado em	**Exemplo**
1. Informação secreta compartilhada entre as partes	PINs, senhas
2. Algo que você tem, físico, material	Cartões, chaves
3. Algo que você é ou faz - a Biometria	Fala, Íris, Impressão digital
4. Localização temporal	Abertura do cofre de um banco
5. Localização espacial	Em frente à loja X
6. Uma testemunha	Alguém que diz quem você é

e o reconhecimento de voz, aquelas incluem a análise da geometria da mão, impressões digitais, reconhecimento da íris, entre outras.

Cada vez mais, as organizações buscam a utilização de algum tipo de característica biométrica no processo de autenticação da identidade dos usuários. Destaca-se a conveniência no uso de autenticação biométrica, à medida que as características biométricas não podem ser roubadas, emprestadas, esquecidas e dificilmente forjadas; ao passo que na autenticação através das tradicionais senhas de acesso pode acontecer o empréstimo ou mesmo o esquecimento da senha [LIU 01b]. Outra vantagem em relação às senhas é de que as características biométricas são, via de regra, maiores em tamanho. Esse aspecto une a vantagem de se utilizar senhas longas (maior dificuldade em descobri-las) com a simplicidade e rapidez do uso de senhas curtas (memorização) [RAT 01a].

2.2.1 Tipos

A seguir são apresentados alguns tipos de características biométricas usualmente explorados [LIU 01b].

Assinatura manuscrita - Analisa a forma como o usuário assina seu nome. Padrões de assinatura como a velocidade, pressão e formato final da assinatura são levados em

consideração. É um método em que não há a necessidade de contato do usuário com o sistema, por isso é um método não intrusivo. Além disso, é uma forma de autenticação bastante utilizada e conhecida por parte dos usuários.

Face - Toma por base as características faciais. Requer uma câmera digital para a leitura da face.

Geometria da mão - Diz respeito à medida do formato da mão.

Íris - São as características do anel colorido de tecido encontrado ao redor da pupila. Para tanto, usa-se uma câmera convencional, não exigindo contato com a mesma. É bastante preciso, além de ser não intrusivo.

Retina - Envolve a análise da camada de vasos sangüíneos que fica na parte de trás dos olhos. Tal método proporciona alta precisão, porém não possui grande aceitação por parte dos usuários, porque exige que os mesmos tenham contato com o mecanismo responsável pelo escaneamento da retina.

Voz - É baseado na conversão de voz em texto. Tal técnica possui um grande potencial de crescimento na sua utilização, uma vez que não requer nenhum *hardware* específico, a não ser um microfone. A ocorrência de barulho no ambiente pode acarretar distorções significativas na coleta da voz.

Impressão Digital - Consiste na análise feita com base nos desenhos papilares da ponta do dedo. Há grande oferta de produtos desse gênero no mercado, atualmente. Na seção 2.5, esta medida biométrica é detalhada e apresentada.

2.2.2 Aspectos Comparativos

Pode-se comparar os tipos biométricos com base no uso de critérios de avaliação como, por exemplo, facilidade de uso, incidência de erro, precisão, aceitação por parte do usuário ou não-intrusividade, nível de segurança requerido e permanência da característica [LIU 01b, JAI 97]. De uma forma geral, para efetuar a escolha entre esses tipos é necessário que se considere o propósito da aplicação na qual será utilizado

[PHI 00]. Na Tabela 2.2, tem-se uma comparação entre 5 tipos biométricos, considerando os critérios de facilidade de uso, incidência de erro, precisão e aceitação do usuário.

A verificação da asssinatura de próprio punho é bem aceita do ponto de vista que as pessoas utilizam essa biometria há tempos. Ou seja, a assinatura manuscrita é tradicionalmente utilizada para assinar documentos, sendo a mesma passível de verificação no futuro. Essa verificação pode ser oficial ou legal, tal como o reconhecimento de firma realizado por tabeliões, ou até mesmo aquele reconhecimento feito pela própria pessoa, de maneira informal. Essa é uma prática corrente na sociedade moderna.

A permanência da característica biométrica pode ser considerada na comparação entre tipos de biometria. A impressão digital possui alto nível de permanência uma vez que os desenhos digitais, explicados em detalhe na subseção 2.5.2, estão definitivamente constituídos desde o sexto mês de vida fetal [TOC 95], em cada indivíduo, perdurando a vida toda. Por outro lado, a face e a assinatura manuscrita possuem menor permanência, porque tais características podem ser alteradas com maior facilidade.

A aceitação por parte do usuário está diretamente relacionada com a questão da não-intrusividade. Por intrusividade entenda-se o contato físico da pessoa com o sistema biométrico. Em geral, o tipo biométrico menos intrusivo é mais rapidamente aceito pelos usuários [LIU 01b].

A impressão digital tem sido utilizada há tempos para a identificação de pessoas, sendo considerada prova legítima em tribunais de todo mundo, quando reveladas a partir de determinados suportes como o papel e vidro, encontrados em cena de crime, por exemplo [JAI 00].

2.2.3 Taxa de Falsa Aceitação e Falsa Rejeição

Os sistemas biométricos, como outros sistemas, não são perfeitos. Desse modo, são admitidas duas taxas de erro. A FAR *(False Acceptance Rate)*, taxa de falsa aceitação, denota o percentual de impostores que são capazes de acessar o sistema. A FRR *(False Rejection Rate)*, taxa de falsa rejeição, denota o percentual de usuários cadastrados no sistema que não conseguem obter acesso a ele [MAI 99].

Tabela 2.2: Comparação entre alguns tipos biométricos.

Critério de Avaliação	Imp. Digital	Íris	Face	Assinatura	Voz
Facilidade de uso	Alta	Médio	Médio	Alta	Alta
Incidência de erro	Sujeira	Pouca luz	Óculos	Mudança	Ruído
Precisão	Alta	Muito Alta	Alta	Alta	Alta
Aceitação do usuário	Média	Média	Média	Muito alta	Alta

Fonte: Artigo Científico [LIU 01b].

Quanto menores essas taxas mais preciso é o sistema biométrico. Ocorre que essas duas taxas são antagônicas, ou seja, se se desejar tornar mais difícil o acesso de impostores ao sistema, pode-se reduzir a taxa de falsa aceitação. Porém, ao mesmo tempo que o acesso ao sistema fica mais difícil para falsários, também o fica para usuários verdadeiros, ou seja, aqueles cadastrados no sistema. Assim, a redução da taxa de falsa aceitação normalmente implica na elevação da taxa de falsa rejeição, como ilustrado na Figura 2.1, e vice-versa [MAI 99]. Ao centro da figura aparece uma linha pontilhada. É importante perceber que essa linha representa o equilíbrio entre as duas taxas. O ideal é reduzir tanto uma taxa quanto a outra para o nível zero, porém é impossível porque à medida que uma é reduzida a outra é elevada.

Contudo, pode-se ajustar essas taxas de acordo com o nível de segurança desejado. Por exemplo, se se quiser um sistema computacional extremamente seguro contra usuários não cadastrados, pode-se baixar a taxa de falsa aceitação para zero. Porém, os usuários cadastrados no sistema terão problemas para acessá-lo, uma vez que a taxa de falsa rejeição aumentará, possivelmente tendo que tentar o acesso várias vezes para entrar no sistema [MAI 99].

Na Figura 2.1, é apresentado um gráfico que ilustra a relação existente entre as taxas biométricas discutidas.

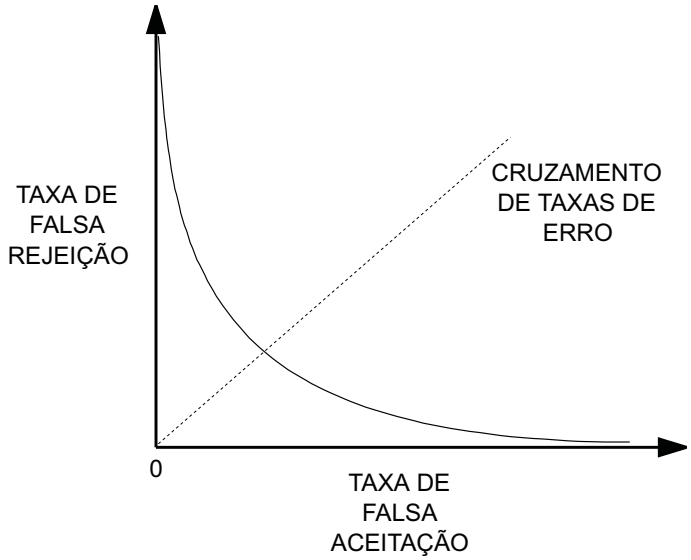


Figura 2.1: Taxas de erro associadas a sistemas biométricos. A linha pontilhada no centro da figura representa o equilíbrio entre as duas taxas. O ideal é reduzir tanto uma taxa quanto a outra para o nível zero, porém é impossível porque à medida que uma taxa é reduzida a outra é elevada.

2.2.4 Verificação e Identificação

As técnicas de reconhecimento por meio das características biométricas podem ser adotadas de duas formas. A primeira e mais simples de ser implementada é a verificação da identidade de um dado usuário, onde a verificação é feita através da comparação com apenas uma referência e o tempo computacional para o confronto é baixo. A outra, que demanda maior tempo de processamento, é a procura pela identificação de alguma pessoa, onde a comparação é realizada com várias referências; o que a torna uma tarefa mais complexa. Por isso, é necessário empregar um algorítmo muito eficiente para que a procura entre, às vezes, milhões de referências, seja realizada no mais curto espaço de tempo possível [MAI 99].

No primeiro caso, o usuário se apresenta como sendo uma determinada pessoa e o sistema confere se ele realmente é ”quem diz ser”. Assim, se o confronto for positivo, o usuário terá acesso ao que é restrito. Sistemas deste tipo são chamados de 1-1 (um para um), pois o dado biométrico apresentado pelo usuário é simplesmente checado com o que foi registrado no banco de dados, durante o cadastro desse usuário. Exem-

plos de aplicações desse tipo de sistema basicamente se resumem àquelas que poderiam funcionar com o tradicional esquema nome-de-usuário/senha, como o *login* em redes e aplicativos ou a liberação de travas de portas elétricas de ambientes restritos.

No segundo caso, a identificação de uma pessoa ocorre quando se tem o dado biométrico dela e se faz uma busca num banco de dados, comparando as informações até que se encontre ou não um registro idêntico ao que é procurado, com certa margem de erro inclusa. Sistemas biométricos deste tipo são conhecidos por 1-N (um-para-muitos), pois o dado biométrico de uma pessoa é comparado ao de várias outras pessoas. Eles podem ser aplicados em casos como a identificação de criminosos e suspeitos ou na localização de desaparecidos. Pelo reconhecimento facial, imagens de pessoas em um estádio de futebol, por exemplo, podem ser utilizadas para identificar torcedores que já tiveram passagem pela polícia por motivos de violência dentro e fora do estádio, alertando os policiais para possíveis confrontos. Fotos de pessoas desaparecidas também poderiam ser comparadas digitalmente com registros de instituições sociais e outros arquivos. A identificação é de grande valia para a Polícia que, freqüentemente, precisa confrontar impressões digitais de suspeitos ou mesmo criminosos com inúmeras outras, contidas em uma base de dados [MAI 99].

2.2.5 Aplicações de Sistemas Biométricos

Sistemas biométricos têm sido usados nas áreas de identificação criminal e segurança prisional. Como exemplo, tem-se o Presídio Central de Porto Alegre, onde ocorre a identificação de presos e visitantes através da impressão digital, desde 1997 [dF 01]. Todavia, o uso de tais sistemas não está restrito somente a essas áreas, existindo um grande potencial de uso em diversas aplicações que exijam um melhor controle de acesso tanto a dados quanto a ambientes físicos [JAI 97].

Algumas aplicações de sistemas biométricos são relacionadas a seguir:

- Segurança nas transações bancárias, tal como transferência eletrônica de fundos e transações com cartão de crédito [JAI 97].

- Controle de acesso físico a locais específicos, como o controle de acesso a aeroportos [JAI 97]. No prédio do TIC, acrônimo de Telefônica Internet Data Center, o acesso físico a algumas salas que contêm informações de clientes se dá mediante reconhecimento de íris [BAL 01].

- Segurança em sistemas de informação com acesso à base de dados via *login* [JAI 97].

- Controle de votante, a fim de evitar fraude no momento da votação [JAI 97].

- Controle de funcionários, tal como o da empresa DATAPREV - empresa de processamento de dados da Previdência Social. Os funcionários têm suas identidades autenticadas através de *smart cards* e impressão digital [dF 01].

- Controle de emissão de carteiras nacionais de habilitação - O estado do Paraná possui um sistema automático para controle do processo de habilitação de condutores. Tal sistema, entre outros dados, digitaliza a impressão digital do candidato, sendo que em qualquer parte dos exames a identidade do candidato pode ser verificada, evitando-se fraudes [Det 00, Car 00].

- Assinatura digital - Um consórcio entre empresas nórdicas[1] construiu um sistema para assinatura de documentos eletrônicos calcado em impressões digitais [HOJ 00].

2.3 A Estrutura da Pele Humana

A pele é uma membrana que cobre a parte externa do corpo [eS 01]. Ela constitui-se basicamente de duas camadas: derme e epiderme. A primeira é a parte mais profunda da pele. Na sua superfície estão localizadas as **papilas**, que são pequenos relevos com vasos sangüíneos e corpúsculos do tato. Já a epiderme é uma fina membrana transparente que cobre a derme [JÚN 91].

Outros elementos que podem ser observados na pele são as cristas papilares e o sulcos intercristais os quais são conhecidos por, respectivamente, estrias e vales.

[1] *Precise Biometrics, Miotec e iD2 Technologies.*

Também, existem as glândulas sebáceas e sudoríparas, responsáveis pela excreção de gordura e suor do corpo humano, respectivamente. Outro elemento que vale destacar são os poros[2]. Eles constituem-se em canais por onde o suor é eliminado e se localizam em cima das estrias [JÚN 91].

As papilas podem ser encontradas nas superfícies palmares e plantares [JÚN 91]. Na Figura 2.2, é apresentada a estrutura da pele.

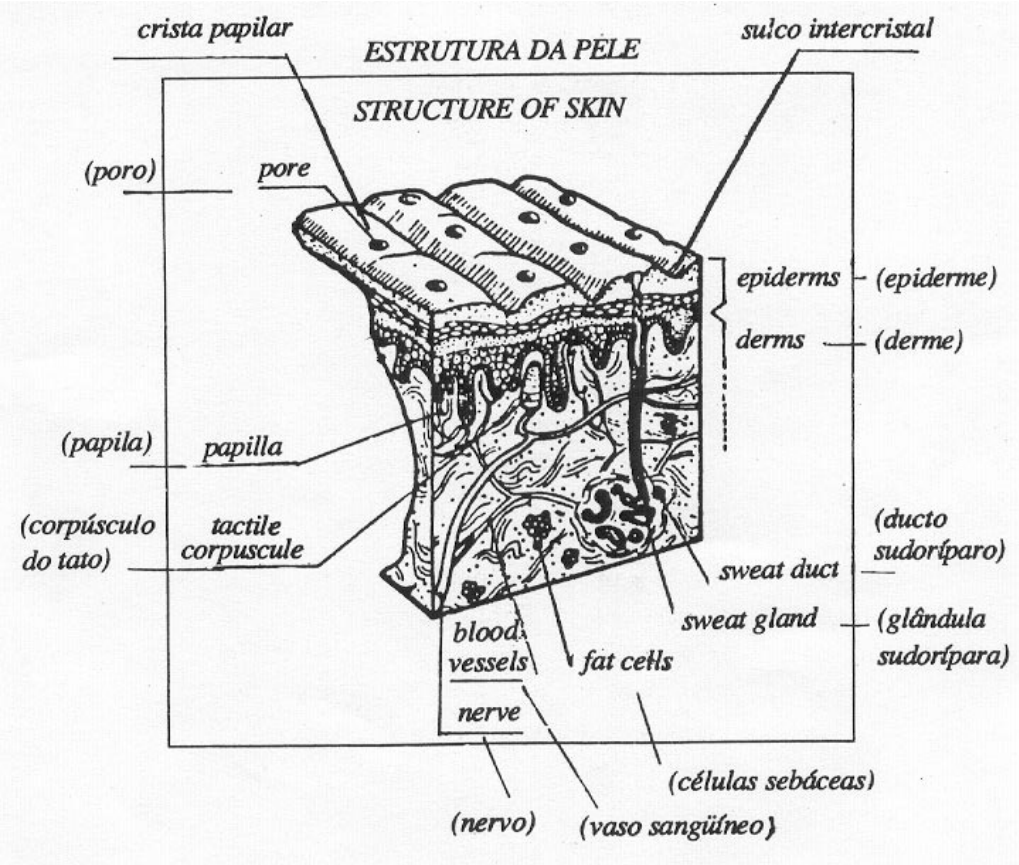


Figura 2.2: Estrutura da pele [JÚN 91].

[2]O pioneiro no estudo sobre os poros foi Arthur Kollman, que qualificou a análise dos poros como um método infalível de identificação [TOC 99]. Arthur publicou um livro informando sobre a possibilidade de classificar os poros. Também, os poros possuem as mesmas propriedades do desenho digital [JÚN 91]. Tais propriedades são apresentadas na subseção 2.5.3.

2.4 Papiloscopia

A papiloscopia, do latim *papilla* = papila e do grego *skopein* = examinar, é a ciência que estuda as impressões papilares e a identificação por meio das mesmas. Ela está dividida nas seguintes áreas: quiroscopia, podoscopia e dactiloscopia [JÚN 91].

A quiroscopia estuda a impressão da palma das mãos, ou seja, as impressões palmares. A palma da mão está dividida em quatro regiões anatômicas, a saber: digital, infradigital, tênar e hipotênar.

A podoscopia estuda a impressão das planta dos pés, que está dividida em cinco regiões anatômicas, a saber: região do grande artelho, região do segundo ao quinto artelhos, região abaixo do grande artelho, região abaixo do segundo ao quinto artelhos e região do calcanhar.

A dactiloscopia estuda as impressões das extremidades digitais.

2.5 Dactiloscopia

A dactiloscopia, do grego *dáktylos* = dedos e *skopein* = examinar, consiste em um método de identificação humana através da impressão digital, também conhecida como datilograma [FED 82]. De uma forma geral, a dactiloscopia divide-se nas três seguintes grandes áreas de atuação [JÚN 91]:

- Dactiloscopia Civil - Trata da identificação para fins civis, como a carteira de identidade.
- Dactiloscopia Criminal - Nesta área encontram-se as três possibilidades seguintes:
  - A identificação do indiciado em inquérito policial, não identificado anteriormente, ou quando houver dúvida ou suspeita sobre sua identidade.
  - A expedição de documentos de idoneidade como o atestado de antecedentes criminais e folha de antecedentes.
  - A identificação de fragmentos de impressões digitais encontradas em locais de crime.

- Dactiloscopia Clínica - Cuida do estudo sobre as perturbações observadas nos desenhos digitais em conseqüência de algumas doenças ou do exercício de certas profissões. Os desenhos digitais são apresentados na subseção 2.5.2.

2.5.1 História

No período pré-histórico, sem nenhuma prova concreta, admite-se que o homem primitivo costumava marcar com a mãos os objetos de seu uso, inclusive a caverna onde morava [TOC 95]. Os cientistas não sabem afirmar se tais marcas possuíam valor identificativo. Alguns autores pensam que tal atitude seja apenas uma manifestação artificial. Para outros estudiosos, o homem primitivo de alguma forma observou a disposição dos desenhos formados na ponta dos dedos, por curiosidade ou não [FED 82].

O período empírico caracteriza-se pelo uso das impressões digitais em processo de legalização de documentos. Em países do oriente, como a China do século VII, tem-se referência do uso de impressões digitais para fins criminais, além de existirem sinais de que conheciam o arranjo dos desenhos papilares. Outra situação é a do divórcio, onde o marido era obrigado a entregar um documento à mulher expondo suas razões para tanto, bem como assiná-lo. Quando era inviável proceder à assinatura, imprimia sua impressão digital no papel [FED 82]. Autoridades no assunto afirmam, porém, que as impressões digitais coletadas naquele tempo eram meros borrões inclassificáveis, sem valor prático algum no estabelecimento da identidade [TOC 99].

Pode-se dizer que o período científico começa em 1686. Nessa data, Marcello Malpighi, um professor de anatomia da Universidade de *Bologna*, Itália, estudou as estrias e as várias figuras formadas por elas, que apareciam na palma da mão. Ele notou que as estrias estavam dispostas em forma de espirais e presilhas na ponta dos dedos, porém, não fez nenhuma referência do seu uso para identificação pessoal [TOC 99].

No ano de 1823, Johannes Evangelist Purkinge, professor de anatomia da universidade de Breslau na Prússia, publicou um trabalho onde analisava a diversidade dos padrões de estrias, especialmente na última falange de cada dedo. Em seu estudo, dividiu esses padrões em nove categorias: (2) do tipo arco, (2) do tipo presilha, (5) do tipo

verticilo. No entanto, não deu praticidade a esse estudo para a identificação de pessoas [TOC 99]. Existem relatos de que Purkinge estudou também os poros da pele [JÚN 91]. Sobre os significados de arco, presilha e verticilo, vide subseção 2.5.4.

No ano de 1858, William Herschel, oficial administrativo britânico e chefe do distrito de Bengala, na Índia, passou a usar impressões digitais em contratos com os nativos. A idéia era amedrontar as partes quanto ao possível repúdio de sua assinatura. Os nativos acreditavam que o contato pessoal com o documento criava uma ligação maior da pessoa com ele do que a própria assinatura manuscrita. Para tanto não havia embasamento científico, porém, calcado na observação, Herschel verificou que os desenhos digitais não mudavam com o passar do tempo [TOC 99].

No ano de 1897, Edward Richard Henry, Inspetor Geral da polícia em Bengala e posteriormente Comissário de Polícia metropolitana de Londres, continuou o trabalho de Herschel. Ele identificou impressões digitais latentes, isto é, impressões digitais obtidas após análise criteriosa de cenas de roubo e homicídio, como pertencentes a um ex-condenado [TOC 99].

Em 1880, Henry Faulds, médico escocês residente em Tóquio, no Japão, escreveu vários artigos publicados na revista inglesa *Nature*, nos quais descreveu suas observações sobre as impressões digitais. Ele defendia o seu uso para detecção criminal e identificação. Faulds recomendou o uso de tinta de impressão como meio de reprodução da impressão digital.

Um importante avanço na área de identificação através da impressão digital foi feito na década de 1880. Nesse período, Sir Francis Galton, antropólogo inglês, estabeleceu um estudo intenso sobre as impressões digitais alertando para a individualidade e permanência das mesmas. Em seu livro *Finger Prints* [TOC 99], publicado em 1882, Galton mostrou cientificamente a suspeita de Hershel: as impressões digitais não mudam durante a vida do indivíduo e duas delas não são iguais, descrevendo o primeiro sistema de classificação para impressões digitais. Com Galton, surgiu o termo minúcia ou detalhes de Galton, que diz respeito às características pelas quais as impressões são identificadas [TOC 99]. Galton publicou seu sistema dactiloscópico adotando 38 tipos de impressões digitais, divididos em três grupos: arcos, presilhas e verticilos [JÚN 91].

Em 1891, Juan Vucetich, Oficial da Polícia Argentina, começou a montar o primeiro arquivo baseado nos padrões de Galton, colocando em efetivo funcionamento o sistema de identificação datiloscópica proposto por ele. Já em 1892, Vucetich fez a primeira identificação criminal através da impressão suja de sangue deixada pelo criminoso em local de crime. Em seu livro, *Dactiloscopia Comparada*, descreveu seu sistema de classificação baseado em quatro tipos básicos de impressões digitais [TOC 99]. O sistema de Vucetich bem como seus tipos fundamentais estão apresentados na subseção 2.5.4.

No ano de 1900, Edward Richard Henry, citado anteriormente, realizou um importante trabalho que se traduziu na publicação do seguinte livro: *Classification and Uses of Finger-Prints*. Nele Henry descrevia o seu sistema de identificação datiloscópica adotando quatro tipos fundamentais para classificação de impressões digitais: arcos, presilhas, verticilos e compostos [JÚN 91].

O sargento John Kenneth Ferrier, do *Scotland Yard Fingerprint Bureau*, ministrou o primeiro curso sobre impressões digitais no Estados Unidos, em 1904. A partir daí, o uso de impressões digitais se alastrou nesse país. Em muitas cidades, núcleos de identificação por impressões digitais foram criados, seguindo-se de condenações onde as impressões digitais serviam como prova judicial [TOC 99].

Em 1918, Edmond Locard escreveu que, em termos de confrontamento de impressões digitais, um número de doze minúcias ou pontos característicos encontrados em duas impressões é suficiente para afirmar que um datilograma corresponde a outro [TOC 99].

De forma geral, no século XX, a identificação pela impressão digital tornou-se reconhecida como prática válida perante a justiça, bem como perante os organismos responsáveis pelo cumprimento da lei. Por volta de 1960, o FBI - *Federal Bureau of Investigation*, a ”Polícia Federal” dos Estados Unidos da América, promoveu grandes esforços no desenvolvimento de sistemas automáticos de identificação através da impressão digital. Vários organismos de cumprimento da lei espalhados pelo mundo também passaram a adotar esses sistemas. Atualmente, o campo de atuação desses sistemas tem transcendido a tarefa de cumprimento legal, sendo amplamente aceitos e uti-

lizados nas mais diversas aplicações civis, tais como controle de votantes e controle de funcionários [JAI 97].

2.5.2 Desenho Digital e Impressão Digital

O desenho digital é a combinação de cristas papilares e sulcos interpapilares localizados na polpa digital [JÚN 91]. A impressão digital ou datilograma é a reprodução do desenho digital. O datilograma possui certos elementos constitutivos que são relacionados a seguir, conforme nomenclatura sugerida por Tavares Jr. [JÚN 91]:

- LINHAS PRETAS - Constituem-se nas linhas impressas do datilograma, correspondendo às cristas papilares.
- LINHAS BRANCAS - Correspondem aos sulcos interpapilares ou intercristas e separam as linhas impressas do datilograma.
- POROS - Pequenos orifícios localizados sobre as linhas impressas do datilograma.
- MINÚCIAS OU PONTOS CARACTERÍSTICOS - São particularidades que ocorrem nas cristas papilares e podem distinguir uma impressão digital da outra. São apresentados em mais detalhes na subseção 2.5.5.
- LINHAS ALBODACTILOSCÓPICAS - São formadas pela interrupção de duas ou mais cristas papilares. Elas ocorrem em razão do enrugamento da pele. Uma observação importante é de que essas linhas não devem ser confundidas com as linhas brancas que correspondem aos sulcos interpapilares.
- DELTA - É um triângulo formado pelas cristas papilares. Tem como principal função determinar o tipo de impressão digital.

2.5.3 Postulados da Dactiloscopia

São aqueles princípios fundamentais que servem de base para a ciência dactiloscópica. Grande parte dos historiadores e especialistas na área admitem apenas os

três primeiros, porém em [RAB 96] e em [TOC 99] são encontradas referências a respeito do item classificabilidade, além dos outros itens: perenidade, imutabilidade e variabilidade.

Perenidade - *Os desenhos dactiloscópicos em cada ser humano já estão definitivamente formados desde o sexto mês de vida fetal, perdurando por toda a vida do indivíduo.*

Imutabilidade - *O desenho digital não se modifica durante toda a existência, podendo sofrer algumas alterações em função de queimaduras, cicatrizes e doenças de pele como a lepra. No entanto, a estrutura anatômica dos desenhos digitais, uma vez formada, não muda.*

Variabilidade - *Os desenhos digitais são variáveis de dedo para dedo e de pessoa para pessoa. Dessa forma, não há possibilidade de se encontrar dois dedos com desenhos digitais idênticos, nem mesmo numa mesma pessoa.*

Classificabilidade - *Apesar de não se encontrar dois dedos com desenhos digitais iguais, e levando em consideração a existência de um número reduzido de tipos fundamentais de impressões digitais onde cada desenho digital se enquadra, é possível classificar o desenho digital em um determinado tipo fundamental.*

2.5.4 Os Tipos Fundamentais de JUAN VUCETICH

Tendo Galton chegado à classificação dos desenhos digitais em quatro tipos, deu por encerrado seu trabalho, sem, no entanto, ter percebido a grande contribuição que havia proporcionado à área de identificação individual [RAB 96].

Mais tarde, através de uma publicação sobre o trabalho de Galton, Juan Vucetich tomou conhecimento dos estudos realizados na área de identificação. A partir daí, ele criou e colocou em efetivo funcionamento um sistema de identificação humana através da impressão digital, ou seja, o sistema dactiloscópico, enfocando, sobretudo, a classificação e o arquivamento das impressões digitais dos geralmente dez dedos das mãos.

Fundamentalmente, para a classificação dos datilogramas, foi adotado o modelo estabelecido por Galton, o qual é descrito a seguir [RAB 96]:

- Desenhos formados por linhas arqueadas e mais ou menos paralelas entre si, chamados por ele de *arch*, ou, arco.

- Desenhos que apresentam, na parte central, linhas dobradas sobre si mesmas em forma de alça ou presilha. A essas atribuiu o nome de *loop*, ou, presilha, as quais dividiu em dois tipos, a saber: ulnar ou cubital e radial, conforme as extremidades livres das alças, na mão considerada, apontassem, respectivamente, para o cúbito ou o rádio do correspondente antebraço.

- Desenhos compostos por linhas enroladas em espiral ou em círculos concêntricos, aos quais deu o nome de *whorl*, ou seja, verticilo.

Com base na classificação apresentada, Vucetich apenas traduziu *arch* para arco, *loop* para presilha e *whorl* para verticilo. Em seguida, notando que nos tipos presilha e verticilo havia um pequeno acidente morfológico, que também fora observado por Galton, denominou-o de delta, cujo significado encontra-se na subseção 2.5.2. Também, estabeleceu que o tipo fundamental seria sempre aquele revelado através do datilograma, independente da mão a que pertencesse e com base principalmente na presença ou ausência do delta. Daí a seguinte conceituação *Vucetichista* para os tipos fundamentais [RAB 96]:

1. **Arco** - Datilograma que não possui delta. As linhas que formam a impressão digital atravessam de um lado ao outro, assumindo forma abaulada.

2. **Presilha Interna** - Apresenta um delta à direita do observador, sendo que as linhas da região do núcleo da impressão digital dirigem-se para a esquerda do observador.

3. **Presilha Externa** - Apresenta um delta à esquerda observador, sendo que as linhas da região nuclear dirigem-se para a direita do observador.

4. **Verticilo** - Tipo dactiloscópico que apresenta normalmente dois deltas, um à esquerda e outro à direita do observador. Outro aspecto é que as linhas da região do núcleo da impressão digital ficam encerradas entre as linhas que se prolongam dos deltas.

Pensando na parte de arquivamento de impressões digitais, Vucetich designou símbolos para cada tipo dactiloscópico. Dessa forma, os símbolos literais A, I, E, e V foram designados, na ordem, para indicar o tipo fundamental das impressões dos polegares. Os símbolos numéricos 1, 2, 3, e 4 foram empregados para designar o tipo fundamental da impressões dos demais dedos da mão [JÚN 91]. Na Figura 2.3, encontram-se os quatro tipos fundamentais com suas respectivas simbologias atribuídas por Vucetich.

Figura 2.3: Os quatro tipos fundamentais de impressões digitais de Vucetich. Associado a cada tipo está o nome e dois caracteres localizados logo acima do datilograma. Essa simbologia é utilizada para representação do tipo fundamental.

Junto a essa simbologia, Vucetich idealizou uma ficha dactiloscópica onde seriam coletadas as impressões digitais dos dez dedos da mão. Essa ficha, uma vez preenchida, receberia o nome de *Individual Datiloscópica*. Nessa ficha, existiam duas fileiras com cinco espaços cada, sendo que na fila superior seria destinada à coleta das impressões digitais dos dedos da mão direita, ou *série*. Na fila inferior, seriam coletadas

as impressões dos dedos da mão esquerda, ou *seção*.

Numa etapa posterior, Vucetich representou os datilogramas de uma ficha *Individual Datiloscópica* através de uma fração ordinária, onde o numerador seria dado pelos símbolos da série ou *Ser*, e o denominador pelos da seção ou *Sec*. A essa representação ele deu o nome de *Fórmula Dactiloscópica*, que é a descrição dos padrões de impressão digital dos dedos das mãos de um indivíduo.

Supondo que uma pessoa tenha seus datilogramas classificados conforme a Tabela 2.3, a *Fórmula Dactiloscópica*, ou *FD*, desse indivíduo é dada pela fração apresentada a seguir:

$$FD = \frac{Ser}{Sec} = \frac{V - 2221}{I - 3333}$$

Através desse processo, com o uso dos dez dedos da mão e com os quatro tipos datiloscópicos distintos, seria possível, em teoria, obter-se 1.048.576 fórmulas diferentes, de acordo com a seguinte demonstração [RAB 96]:

SÉRIE (5 DEDOS)	4 X 4 X 4 X 4 X 4 = 1.024 SÉRIES
SEÇÃO (5 DEDOS)	4 X 4 X 4 X 4 X 4 = 1.024 SEÇÕES
TOTAL	1024 X 1024 = 1.048.576 FDs

Apesar do grande número de teoricamente possíveis fórmulas datiloscópicas, a quantidade de fórmulas dactiloscópicas que ocorrem no campo biológico é mais reduzida. Conforme comprovação estatística, constata-se que, na prática, não se equiparam em freqüência os quatro tipos dactiloscópicos. A freqüência maior é a dos verticilos, seguida das presilhas, e finalmente dos arcos [RAB 96].

Existem variações dos desenhos digitais chamadas de subtipos, que podem ser constatadas em cada tipo fundamental. Tais subtipos possibilitam o desdobramento de individuais dactiloscópicas de mesma fórmula, o que facilita a busca e identificação de indivíduos em grandes arquivos [RAB 96].

Um aspecto interessante de perceber é que os tipos e subtipos datiloscópicos não identificam unicamente um indivíduo, uma vez que as fórmulas datiloscópicas podem repetir-se de uma pessoa para a outra. Dessa forma, tanto o tipo quanto

Tabela 2.3: Esquema de classificação de datilogramas.

Dedo	**Mão direita**	**Mão esquerda**
Polegar	V - Verticilo	I - Presilha Interna
Indicador	2 - Presilha Interna	3 - Presilha Externa
Médio	2 - Presilha Interna	3 - Presilha Externa
Anular	2 - Presilha Interna	3 - Presilha Externa
Mínimo	1 - Arco	3 - Presilha Externa

o subtipo dactiloscópico não são suficientes para a verificação e prova da identidade de um datilograma, somente limitando a busca, em arquivos dactiloscópicos, dentro daqueles indivíduos que possuem mesma fórmula [RAB 96].

De outra forma, existem dois tipos de características mapeados na impressão digital que podem ser mais eficazes na individualização dos datilogramas: as minúcias e os poros. Vale citar o sistema desenvolvido para uso interno pela NSA, Agência Nacional de Segurança dos Estados Unidos, que utiliza poros para comparar impressões digitais. Tal sistema visa explorar a eficácia do uso de poros para comparar automaticamente impressões digitais [ROD 97].

Na subseção 2.5.5, apresenta-se um elemento tradicionalmente utilizado para comparar impressões digitais: as minúcias.

2.5.5 Minúcias

Minúcias, também chamadas de pontos característicos, são pequenas irregularidades ou acidentes morfológicos que ocorrem no desenho dactiloscópico. As minúcias servem para distinguir uma impressão digital da outra, de forma a facilitar a identificação única de um indivíduo.

Segundo Rabello, doze pontos característicos bastam para identificar

uma impressão digital. Ou seja, doze pontos característicos coincidentes em dois datilogramas bastam para fazer prova científica e juridicamente válida, caracterizando, de forma indiscutível, que ambos correspondem ao mesmo dedo [RAB 96].

Outro aspecto é o de que não devam existir pontos discrepantes entre as impressões comparadas. Um ponto discrepante é um ponto característico que se encontra em uma impressão digital, mas não na outra, considerando a sua localização no plano cartesiano [JÚN 91]. Dentre os autores consultados, há um consenso quanto ao número mínimo de pontos necessários para a identificação de um datilograma. Em [TOC 99], [JÚN 91] e [RAB 96] são encontradas referências de que doze é o número mínimo de pontos necessários para a afirmativa de uma identidade. Porém, Tochetto relata que nos Estados Unidos o número mínimo de pontos considerados em uma identificação datiloscópica chegou a sete [TOC 99].

Ao se efetuar a leitura dos pontos característicos, deve-se considerar o movimento do relógio. Ou seja, deve-se tomar por base a orientação da esquerda para direita [TOC 99]. Este aspecto é importante para que se possa identificar corretamente e uniformemente os tipos de minúcias.

A nomenclatura para os diversos tipos de minúcias pode variar entre órgãos de identificação, porém, toma-se por referência o seguinte [TOC 99]:

- PONTO - Um pequeno ponto.
- ILHOTA - Pequena ilha papilar, isolada de outras.
- CORTADA - Proporcional ao dobro da ilhota.
- BIFURCAÇÃO - Linha papilar que em uma dado trecho de seu trajeto se divide em duas.
- CONFLUÊNCIA - Duas linhas papilares que se desenvolvem paralelamente e em determinado ponto se unem, tranformando-se em uma uma só linha.
- ENCERRO - Duas linhas papilares unidas nas extremidades, encerrando um espaço em branco.

- INÍCIO DE LINHA - É a parte onde começa uma linha papilar.
- FIM DE LINHA OU FINAL DE ESTRIA - É a parte onde termina uma linha papilar.
- EMPLAME - União de duas linha papilares por uma terceira linha, no sentido inclinado.

Os vários tipos de minúcias podem ser observados em um datilograma real. Na Figura 2.4, são mostrados quatro tipos de minúcias em um fragmento de impressão digital: final de estria, encerro, bifurcação e ilhota.

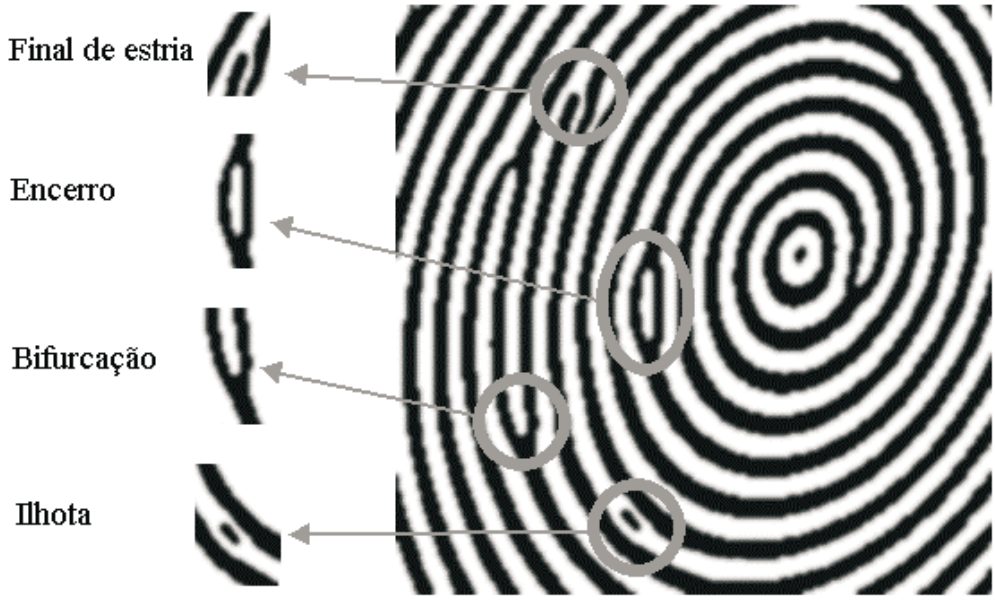


Figura 2.4: Exemplos de minúcias identificadas em um datilograma.

2.6 A Tecnologia AFIS

AFIS é um acrônimo de *Automated Fingerprint Identification System*, ou seja, sistema automatizado de identificação pela impressão digital. Em linhas gerais, tal sistema captura as impressões digitais de uma pessoa para posterior processamento, incluindo comparação entre as impressões obtidas e um banco de dados de impressões

previamente cadastradas [NAV 01]. Tal tecnologia encontra-se amplamente difundida pelo mundo.

Órgãos policiais e de investigação tradicionalmente utilizavam a impressão digital para identificar pessoas através de um processo de análise manual. Sendo assim, a identificação automática através da impressão digital foi idealizada para uso desses órgãos, em função da necessidade de uma maior eficiência e produtividade operacional. O FBI foi um dos pioneiros na proposta e desenvolvimento desses sistemas, aproximadamente no ano de 1960 [JAI 97].

Com o passar do tempo, o AFIS mostrou-se ser uma tecnologia bastante útil e aplicável a várias situações do nosso cotidiano. Dessa forma, aplicações onde a identificação ou a verificação da identidade é necessária foram se constituindo um novo mercado para essa categoria de sistemas. Como exemplo disso, pode-se relacionar o seguinte: o acesso a terminal bancário, acesso a ambientes restritos, sistema de voto eletrônico, entre outros [DOM 97].

A estrutura genérica de um AFIS é apresentada na Figura 2.5. Nela é possível encontrar as partes principais do sistema, ou seja, interface com o usuário, a seleção de um *template* ou molde no caso de verificação, aquisição de imagem, a extração de características, criação do *template*, armazenagem, o confronto ou comparação e a resposta dada pelo sistema.

A interface com o usuário permitirá, dentre outras coisas, que o sistema solicite ao usuário o posicionamento adequado do dedo no leitor de impressão digital. Outra situação é a possibilidade da definição do tipo de consulta aos dados armazenados, isto é, se é uma verificação ou uma identificação de datilograma. Como todo sistema biométrico, um AFIS pode ser configurado para realizar ambas as tarefas. No caso de uma verificação, o usuário poderia indicar por meio da interface sua identidade, para que o sistema pudesse selecionar o *template* adequado para o cotejo.

Na etapa de aquisição da impressão digital existem duas possibilidades. A primeira traduz-se no obtenção da imagem através da coleta convencional de impressões digitais, ou seja, o entintamento do dedo e posterior uso de sensores fotográficos, *scanners*, para a tarefa de digitalização. Na conversão de sistemas manuais para sistema

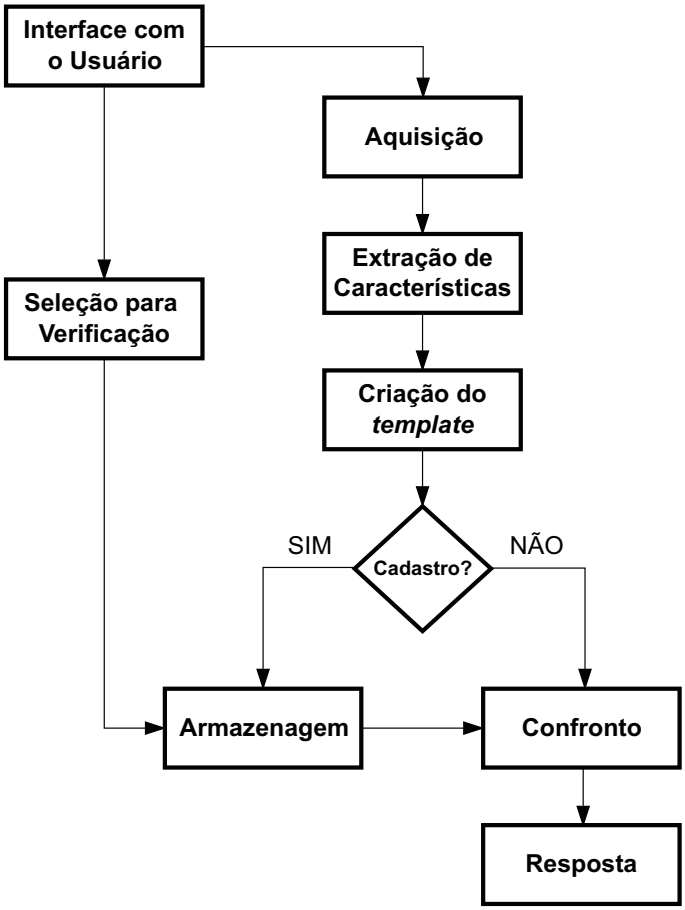


Figura 2.5: A estrutura genérica de um AFIS.

automáticos de cotejo de impressões digitais, essa maneira de aquisição de imagem é utilizada. Além disso, existe a situação de coleta de impressões ocultas em local de crime, onde o processo de aquisição é o mesmo exposto até aqui. A segunda possibilidade é digitalização da imagem com o uso de sensores próprios para leitura dos datilogramas. Assim, através do toque direto do dedo com o sensor, a imagem será criada. Atualmente, existem as seguintes tecnologias de sensores para captura em tempo real de impressões digitais [MAI 99]:

- Óptica, onde uma câmera captura o sinal refletido de um prisma.
- Ultra-som, que é baseado no envio de sinais acústicos em direção ao dedo, detectando o eco ocasionado [BIC 99].

- Microchips de silício, que se divide em três subtipos:
  - Pressionamento. Consiste em detectar a pressão aplicada sobre o sensor e assim capturar a impressão digital.
  - Capacitância. A idéia é capturar as diferentes acumulações de carga criadas pelas estrias e vales da impressão digital.
  - Térmico. Mede a temperatura das estrias quando do contato do dedo com o sensor. Essa temperatura contrasta com a dos vales da impressão digital, uma vez que eles não encostam no microchip.

Para que seja possível a detecção dos pontos característicos, é necessário que a imagem adquirida da impressão digital receba um tratamento. Geralmente, as etapas de tratamento de imagem variam de fabricante para fabricante aparecendo mais ou menos etapas conforme a metodologia empregada para extração de minúcias. Em [FAR 99], propõe-se um algoritmo para extração de minúcias que incide sobre imagens esqueletizadas ou afinadas, sendo as linhas reduzidas à largura mínima de um pixel. Outra abordagem é a extração de minúcias diretamente da imagem em escala de cinza adquirida [MAI 97], isto é, sem que haja previamente os tratamentos de binarização, que é a conversão da imagem adquirida a 256 níveis de cinza em dois níveis: preto e branco, e afinamento de imagem. Já o sistema biométrico ARID, produzido no CEFET-PR, utiliza as seguintes etapas para tratamento de imagem de impressão digital: recorte, mapa direcional, limiarização e afinamento [ANT 02].

O bloco de extração de características consiste em capturar na imagem determinadas particularidades que a individualizam. Dentre as técnicas utilizadas nesse processo, há a possibilidade de reconhecimento de impressões digitais através do uso de redes neurais, procurando-se identificar padrões na imagem da impressão digital, ou seja, as minúcias [LEU 91]. Embora a maioria dos métodos de comparação de impressões digitais utilizem como base as minúcias, há a possibilidade de se comparar impressões utilizando poros ou ambas particularidades [ROD 97].

O *template* ou molde é uma coleção de informações obtidas a partir da impressão digital, sobretudo as minúcias, constituindo-se em um dado numérico gerado

a partir da imagem de uma impressão digital. Nessa representação da impressão digital, pode-se encontrar informações como as coordenadas das minúcias, seu tipo, direção, a distância entre elas etc. Também, é possível dizer que o *template* é uma versão comprimida da imagem da impressão digital, num esquema de compressão com perda de dados, sendo portanto impossível obter-se a impressão digital novamente a partir do *template* [MAI 99]. O tamanho do *template* varia de acordo com a aplicação e com o que se considera da imagem da impressão digital. Assim, identificação e verificação impactam de forma diferente no seu tamanho, requerendo a tarefa de identificação um volume maior de informações. Basicamente, o *template* usado na identificação possui tamanho aproximado de 500 bytes e aquele utilizado na tarefa de verificação varia entre 64 e 400 bytes [IDE 01].

O confronto entre *templates* visa determinar se duas impressões digitais são do mesmo dedo. O que se confronta é o *template* de uma impressão colhida com o *template* de uma impressão armazenada em uma base de dados ou num cartão, por exemplo. Nesse módulo, geralmente é definida uma métrica de similaridade entre as representações das impressões [JAI 97]. Pode-se encontrar referência disso em [ANT 02, NAV 01, RAT 00], onde é relatada a montagem de um grafo descritor de minúcias a partir das informações contidas no *template*. Nesse grafo, é estabelecida uma relação de distância entre tais minúcias, sendo que em uma situação de confronto é analisado o quanto um grafo se parece com o outro.

A partir daí, obtém-se o resultado e as impressões existentes na base de dados são classificadas em três grupos: 1) Seguramente não é essa pessoa, 2) Talvez seja esta pessoa e 3) Seguramente é essa pessoa. O que irá definir o tamanho desses grupos é o parâmetro limiar preestabelecido no sistema, ou seja, a relação existente entre a taxa de falsa aceitação e a taxa de falsa rejeição, discutidas na subseção 2.2.3.

É interessante notar que em casos de identificação, onde ocorre a busca em, quase sempre, uma grande base de dados, são utilizadas rotinas mais complexas de busca. Nesses casos, pesquisas em AFIS tem enfocado não só a análise de minúcias como o uso da classificação de impressões digitais na expectativa de reduzir a quantidade de impressões a serem comparadas, diminuindo assim o tempo de resposta ao

usuário [FAR 99]. Também são encontradas referências com relação ao uso de prévia classificação de impressões digitais em grandes base de dados em [LUM 97]. No caso da verificação, a rotina de busca é mais simples, uma vez que o usuário declara sua identidade, cabendo ao sistema tão somente verificá-la.

Existem vários padrões regulando o formato de dados relativos à impressão digital. O principal é o padrão ANSI/NIST ITL 1-2000, que regula aspectos como tipos de minúcias válidas e quais e quantos são os tipos fundamentais de datilogramas, entre outras tantas peculiaridades para o formato e o intercâmbio de informações de impressões digitais. Um padrão derivado deste último é o EFTS versão 7.0, que é uma implementação do FBI. No Capítulo 4, seção 4.2, esses padrões são detalhados.

2.7 Conclusão

Neste capítulo, foram apresentadas as formas de autenticação da identidade de usuários que vão desde as tradicionais senhas até aos sistemas a biométricos, tão em voga nos dias de hoje.

A escolha de que tipo de autenticação usar deve ser pautada por suas peculiaridades e pelo o ambiente onde será inserido. Muitas vezes, a união de tipos de autenticação diferenciados pode ser vantajosa para se possa aumentar a confiabilidade no processo de autenticação da identidade, considerando que cada forma de autenticação tem prós e contras. Assim, são utilizados cartões, senhas e impressões digitais no modelo que se propõe nesta dissertação, visando autenticar a identidade de usuários durante a assinatura de documentos eletrônicos.

A identificação através dos datilogramas é relevante para este trabalho por tratar-se de uma característica pessoal do indivíduo. O caráter identificativo das impressões digitais e os aspectos que tornam possível essa identificação, conforme ilustrado neste Capítulo, habilitam o seu uso no modelo proposto para assinatura digital de documentos eletrônicos. Tal modelo é apresentado no Capítulo 5 desta dissertação.

Capítulo 3

Conceitos de Criptografia

Neste capítulo, introduz-se uma importante ferramenta que figura na área de segurança em computação: a criptografia. Nesse sentido, além de conceituá-la, pondera-se sobre alguns aspectos relacionados ao seu uso, como os certificados digitais e a Infra-estrutura de chaves públicas. Acima de tudo, é feita uma revisão da técnica para a realização de assinatura digital, segundo a abordagem RSA, que será utilizada no modelo proposto para assinatura digital usando a impressão digital apresentado no Capítulo 5.

Na Seção 3.1, explica-se o significado da palavra criptografia e suas áreas de abrangência. Na Seção 3.2, é abordada a técnica para a realização de assinatura digital e abordam-se também as funções resumo que são usadas na geração dessa assinatura. Na Seção 3.3, são tratados os seguintes assuntos: certificação digital e Infra-estrutura de Chaves Públicas. Na Seção 3.4, concluí-se este Capítulo.

3.1 A Criptografia

A palavra criptografia tem origem grega - *kryptós* = escondido, oculto, obscuro e *graphía* = grifo, escrita - consistindo na arte ou ciência de escrever em códigos, utilizando um conjunto de técnicas que torna o texto incompreensível [dHF 99]. Para cifrar um texto é necessária uma chave a qual possui um certo número de bits. Quanto maior o tamanho da chave, ou seja, quanto maior o número de bits da chave, maior é a

segurança porque o espaço de chaves é aumentado. O número de chaves possíveis é igual a 2^b, onde *b* é o número de bits da chave.

Pode-se classificar as técnicas criptográficas em duas classes, conforme o número de chaves utilizadas no processo de cifrar e decifrar textos: criptografia simétrica e assimétrica. A criptografia simétrica usa uma única chave para cifrar e decifrar uma mensagem. Para tanto, a chave deve ser conhecida pelo emissor e pelo receptor da mensagem. Um dos principais problemas relacionados com esse tipo de criptografia é a distribuição e gerenciamento das chaves, uma vez que elas devem ser mantidas como um segredo entre as partes envolvidas [STA 99].

A criptografia assimétrica, conhecida também por criptografia de chave pública, usa um par de chaves para cifrar e decifrar a informação: a chave pública K_U e a chave privada K_R. Assim, se a chave privada, mantida em segredo, é utilizada para cifrar, então a chave pública, de conhecimento público, deverá ser usada para decifrar, e vice-versa. A criptografia assimétrica foi apresentada em 1976 por Whitfield Diffie e Martin Hellman [DIF 76]. Em 1977, Rivest, Shamir e Adleman desenvolveram um algoritmo assimétrico chamado RSA [RIV 77], tendo por referência as iniciais dos sobrenomes dos autores [STA 99]. Nos últimos tempos, o RSA tem sido a base para a maioria das aplicações que envolvem criptografia assimétrica. Basicamente, a criptografia assimétrica resolveu dois problemas não resolvidos pela criptografia simétrica, ou seja, a distribuição de chaves e as assinaturas digitais [STA 99].

3.2 Funções Resumo e Assinatura Digital

A função resumo traduz-se em uma imagem compacta da mensagem. Comumente, são referidas por ”impressão digital” do arquivo. Esse termo é usado a fim de denotar o caráter identificativo das funções resumo, em analogia às impressões digitais de uma pessoa. Essas funções possuem duas propriedades importantes:

- Não é possível fazer a operação inversa. Em outras palavras, dado um resumo deve ser inviável computacionalmente obter a mensagem original.

- Duas mensagens distintas não devem originar um resumo igual.

Em sua essência, tais funções podem ser usadas para garantir a integridade de uma mensagem. Na Figura 3.1, um modelo de assinatura digital é exposto, onde um usuário *A* utiliza sua chave privada para cifrar o resumo de uma mensagem *M*. O usuário *B* decifra o resumo com a chave pública, K_U, de *A*, obtendo $H(M)$. Calcula um novo resumo com base na mensagem recebida e compara os dois valores. Se forem iguais, a mensagem não foi alterada, caso contrário, houve quebra de integridade. Dessa forma, a integridade da mensagem é garantida. Além disso, a autenticação da origem da mensagem é provida com o uso da criptografia assimétrica, pois o usuário *A* usa a informação pessoal K_R para cifrar o documento.

No esquema da Figura 3.1, o sigilo de mensagem não é provido, porém é possível fazê-lo através da cifragem de *M* com a chave pública do usuário *B*. Posteriormente, este usuário utilizará sua chave privada para decifrar *M*. No entanto, os serviços de sigilo e integridade são opcionais para as assinaturas digitais, sendo os serviços de autenticação, não-reuso e não-repúdio de mensagem os essenciais.

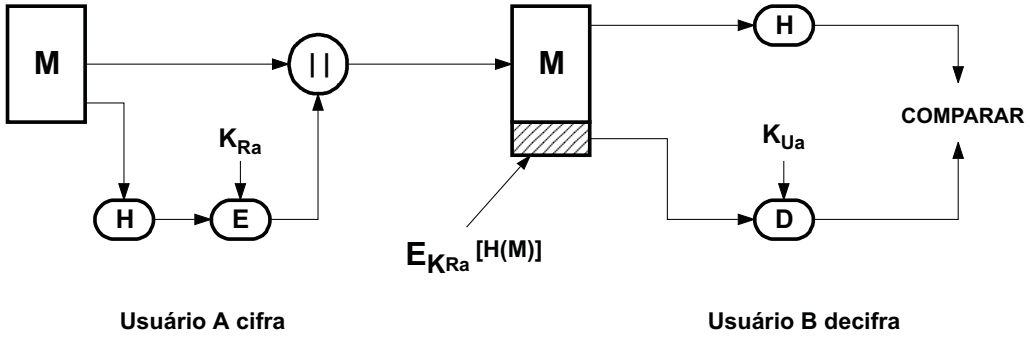


Figura 3.1: Abordagem RSA para assinatura digital de documentos eletrônicos [STA 99].

Dessa forma, a assinatura digital é um código binário que é determinado com base no documento e alguma outra informação associada à pessoa. Ao assinar um documento no papel, o que está efetivamente sendo assinado é o papel, ao contrário da assinatura digital onde se assina a informação. Por outro lado, na assinatura manuscrita em papel há um vínculo direto entre a pessoa e o documento assinado, uma vez que se deixa diretamente no documento uma característica pessoal como a pressão exercida sobre

o papel. A assinatura digital, por outro lado, usa um número, a saber: a chave privada do signatário, para realizar a assinatura do documento e eletrônico, ou seja, a ligação de um número com a pessoa é fraca.

Em situações onde não é completa a confiança entre emissor e receptor da mensagem, alguma coisa a mais que a usual autenticação digital pode ser necessária. Nesses casos, a técnica de assinatura digital pode ser usada na checagem, por exemplo, da autenticidade e integridade das mensagens eletrônicas. As assinaturas digitais devem possuir as seguintes propriedades [STA 99]:

- Possibilitar a verificação do autor, data e hora da assinatura.
- Possibilitar autenticação do conteúdo original da mensagem no momento em que se realizar a assinatura.
- Possibilitar verificação por terceiros, a fim de que se possa resolver disputas.

3.3 Certificação Digital

O certificado digital é um arquivo assinado digitalmente por uma entidade confiável, chamada Autoridade Certificadora (AC). O principal objetivo do uso de tais certificados é o associar uma chave pública a uma pessoa ou entidade, constituindo-se em um meio mais confiável de divulgação de tal chave.

Um formato para certificado bastante aceito é o X.509v3. Trata-se não só de um certificado, mas de uma serviço de autenticação que prevê uma estrutura para o armazenamento e divulgação de certificados. A estrutura do certificado X.509v3 é mostrada na Figura 3.2 [STA 99]. Dados como nome da AC, período de validade do certificado, nome do usuário titular do certificado, chave pública K_U do usuário, além de atributos que podem ser adicionados (foto, permissões de acesso, etc), fazem parte da estrutura. O último campo do certificado é composto do resumo de todos os demais campos, cifrado com a chave privada da AC. Em outras palavras, é a assinatura digital do certificado realizada pela AC, sendo que a chave pública da AC é de domínio público.

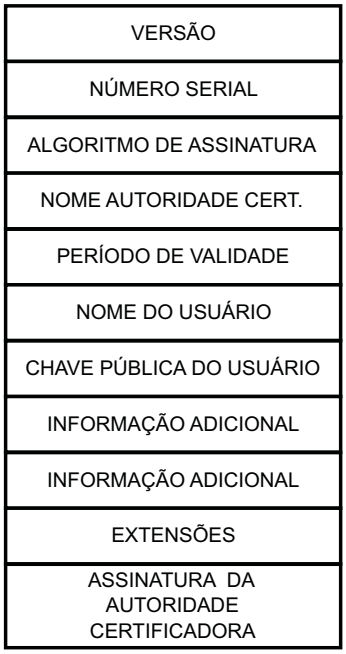


Figura 3.2: Estrutura do certificado digital X.509 Versão 3.

Um outro aspecto relevante é a infra-estrutura necessária para que as operações envolvendo os certificados digitais sejam possíveis. A Infra-estrutura de Chaves Públicas - ICP constitui-se em um conjunto de políticas e procedimentos voltados à operacionalização de um sistema de emissão de certificados digitais baseado em criptografia de chave pública. Alguns serviços de segurança viabilizados por uma ICP são os seguintes: integridade, autenticação e não-repúdio da informação [Hun 01].

Assim como em outros países, o Brasil tomou medidas para regulamentar a ICP no âmbito da legislação federal. Uma medida provisória institui a Infra-estrutura de Chaves Públicas Brasileira - ICP-Brasil, que visa dar validade jurídica aos documentos eletrônicos [BRA 02].

Uma ICP tem papel de fundamental importância para o processo de assinatura digital, possibilitando, por exemplo, a verificação de uma assinatura. No entanto, a sua utilização não garante, por si só, a autenticidade das assinaturas feitas no meio eletrônico. Ou seja, não garante quem realmente usou a chave privada que foi utilizada em dada assinatura. Mesmo que o usuário zele pela integridade e segredo de sua chave privada, um programa malicioso poderá copiá-la, sem que o usuário perceba isso. De

posse da chave, o autor do programa poderá assinar documentos eletrônicos, assim como o proprietário. O problema do gerenciamento de chave é discutido na seção 5.1.

Segundo [Hun 01], os elementos que constituem uma Infra-estrutura de Chaves Públicas são os seguintes:

- Política de segurança.
- Autoridade certificadora.
- Autoridade de registro.
- Repositório de certificado e sistema de distribuição.
- Aplicações de ICP.

Dentre os elementos de uma ICP, pode-se destacar a Autoridade Certificadora (AC), que é uma entidade que emite e revoga certificados digitais. Tais certificados, em última análise, servem para identificar pessoas em uma rede de computadores.

Os certificados podem seguir o padrão X.509, que é um serviço de autenticação recomendado pela ITU-T, prevendo a manutenção de uma base de dados, distribuída ou não, com informações acerca de usuários, como, por exemplo, o certificado digital [STA 99]. Essa base de dados é representada pelo Diretório Público que se destina a manter os certificados e torná-los disponíveis a qualquer um que os procure. Existem outras maneiras pelas quais se pode distribuir certificados digitais, fornecendo suporte à assinatura digital. Uma delas é através de Anúncio Público, como é o caso do PGP. A divulgação e distribuição dos certificados digitais do PGP pode ser realizada através da *home page* do próprio usuário. Porém, o uso de ICP e certificados X.509v3, considerando o conceito de Diretório Público, proporciona maior confiabilidade para a divulgação e distribuição de certificados digitais [STA 99].

A Autoridade de Registro (AR) destina-se a validação ou autenticação da identidade do usuário e a posterior solicitação de emissão do certificado à AC. Assim como a AC, as AR constituem-se em pontos críticos de uma ICP. A qualidade do processo de autenticação dos dados do usuário determina o nível de confiança que pode ser dado aos certificados emitidos [Hun 01].

3.4 Conclusão

Neste capítulo, foram revisados conceitos importantes atrelados à criptografia. Um desses conceitos é o de assinatura digital. Ela é uma ferramenta relevante na construção de sistemas de autenticação seguros porque contribui no processo de identificação de usuários. As assinaturas digitais oferecem autenticação, não-reuso e não-repúdio às mensagens assinadas.

No modelo proposto no Capítulo 5, sugeri-se que seja garantida a integridade da mensagem, como forma de aumentar a confiabilidade no processo de assinatura digital. Com esse propósito, discutiu-se as funções resumo neste capítulo. Conforme apresentado, tais funções podem ser usadas com essa finalidade.

Há muito que se discutir acerca da segurança das assinaturas digitais, uma vez que o sistema apresentado na Figura 3.1, não garante plenamente a autenticação da identidade dos signatários. É importante a busca por mecanismos que superem este problema e, por conseqüência, incrementem a confiança no sistema de autenticação de identidade.

Capítulo 4

Uso de Sistemas de Impressão Digital Para Fins de Identificação

Neste capítulo, apresentam-se sistemas onde as impressões digitais são usadas e os padrões existentes para a permuta de dados relativos a impressões digitais. As experiências práticas envolvendo a utilização de datilogramas para identificar pessoas são relevantes para a definição do modelo proposto no Capítulo 5.

Neste capítulo, foram feitas diversas considerações acerca do uso de impressões digitais. Na Seção 4.1, é fornecido um panorama acerca do uso de sistemas de impressões digitais para fins de identificação, sobretudo aqueles utilizados pelos organismos policiais, os quais tradicionalmente os utilizam em seu cotidiano. Na Seção 4.2, discute-se alguns padrões existentes para a troca de informações de impressões digitais. Na Seção 4.3, são apresentadas algumas tecnologias emergentes na área de verificação através de impressões digitais.

4.1 Uso por Organismos Policiais

Na Subseção 4.1.1, é mostrado o uso de impressões digitais em processos de identificação no Estado de Santa Catarina. Na Subseção 4.1.2, apresenta-se a utilização de datilogramas em sistemas de identificação em âmbito nacional.

4.1.1 No Estado de Santa Catarina

No Estado catarinense, observa-se o uso de impressões digitais para efeitos identificativos. Com efeito, elas são assentadas nas carteiras de identidade que a Polícia Civil, dentro de sua estrutura, emite. Em nossa vida civil, as identidades são freqüentemente utilizadas para identificação perante terceiros.

De acordo com a lei, deve constar na carteira de identidade civil, entre outros, os seguintes elementos identificativos: a identificação do órgão expedidor, armas da República, nome do identificado, foto, assinatura manuscrita, data de nascimento, filiação, naturalidade e impressão digital do polegar direito. Porém, o texto legal parece contemplar de maneira especial a impressão digital. Conforme o trecho a seguir, retirado da lei específica, esse aspecto é percebido: *"Art.8 A carteira de que trata esta lei será expedida com base no processo de identificação datiloscópica."* [Car 83]. Talvez isso traduza a grande importância que a impressão digital tenha nas atividades policiais, pois elas podem ajudar significativamente na descoberta da autoria de um delito ou na resolução de disputas judiciais.

A fim de facilitar a exposição do assunto, esta subseção está dividida em três partes. A Identificação Civil é apresentada no item 4.1.1.1. Aspectos sobre a área de Polícia Técnico-Científica e impressões latentes são mostrados no item 4.1.1.2. A Identificação Criminal é discutida no item 4.1.1.3.

4.1.1.1 Identificação Civil

A carteira de identidade é o documento de identificação civil. Em [Car 83, Dec 83] encontra-se o embasamento legal relativo à validade e expedição da carteira de identidade. Em outras palavras, são aqueles documentos emitidos por unidades da federação e estados membros da República Federativa do Brasil, tendo o status de documento oficial de identidade com aceitação nacional [SAN 01]. A sua confecção tem sido processada da seguinte maneira:

1. A pessoa dirige-se à Delegacia Regional de Polícia ou a um Posto de Identificação na sua cidade. Ela deve apresentar uma documentação para a confecção da car-

teira de identidade, como fotos em tamanho 3x4, comprovante de recolhimento da respectiva taxa, comprovante de residência e sua certidão de nascimento ou de casamento.

2. O próximo passo consiste no cadastramento dos dados da pessoa no sistema computadorizado de controle de identificação estadual. Nesse sentido, são coletados uma série de dados do identificado, como nome, data de nascimento, nome do pai, nome da mãe, altura etc. O referido sistema de controle de identificação é acessado por meio de terminais localizados na Delegacias Regionais do Estado. Além disso, coleta-se a assinatura manuscrita do identificado na cédula de identidade. O controle da emissão e a numeração de tais cédulas são feitos pelo Instituto de Identificação do Estado.

3. A seguir, a ficha Classificação Datiloscópica, apresentada na Figura 4.6, página 64, é preenchida. Nela são coletadas as impressões digitais do dedo polegar, indicador, médio, anular e mínimo, tanto da mão esquerda quanto da mão direita. Tais impressões são coletadas de maneira rolada e pousada [RAB 96]. Além disso, coleta-se a impressão digital do polegar direito na carteira de identidade.

   Destaca-se que a tomada e arquivamento de impressões digitais são feitos manualmente, ao contrário dos demais dados da pessoa que são armazenados através do computador.

4. Finalmente, a Carteira de Identidade é montada e entregue ao identificado. É importante destacar que na parte frontal da carteira aparecem três características biométricas: foto facial frontal, assinatura manuscrita e impressão digital do polegar direito.

De um forma geral, a Polícia tem evoluído do sistema manual para um automatizado, que usa sistemas automatizados de identificação de impressão digital, com o cadastramento e armazenamento de informações pessoais, assim como coleta de impressões digitais através de leitores específicos, fotos digitais e assinaturas manuscritas digitalizadas no momento do cadastro para requisição da carteira de identidade. A Polícia

Civil catarinense, por exemplo, tem empenhado-se na implantação de um sistema automatizado de identificação através dos datilogramas. A utilização de tal sistema, possibilita, entre outras facilidades, consultas de dados da pessoa a partir de sua impressão digital.

4.1.1.2 Polícia Técnico-Científica e Datiloscopia

Quando da ocorrência de um fato criminoso, a perícia policial é acionada, deslocando-se ao local de crime e procedendo ao levantamento de vestígios que possam levar à elucidação do crime, e conseqüente constatação de sua autoria. Dentre esses vestígios, as impressões digitais são alvo de intensa procura em cenas de crime, dado que elas encontram-se muitas vezes ocultas e pouco visíveis nos cenários de crime. Essas impressões ocultas são conhecidas como impressões latentes [RAB 96], as quais são ilustradas na Figura 4.1. Tais impressões são produzidas através de suor e gordura quando do contato dos dedos com determinados suportes.

Figura 4.1: Impressões digitais latentes deixadas em tomada e vidro.

Silva faz referência a três métodos de revelação de impressões latentes, além de informar sobre vários reagentes que podem ser utilizados nesse processo: método sólido, utilizando pós, líquido, faz uso de drogas e substâncias químicas, e gasoso, através de vapores e substâncias químicas [eS 01].

A escolha do pó utilizado no levantamento da impressão digital varia conforme alguns fatores. Um deles é a aderência do pó à superfície e à impressão digital. O pó deve aderir a impressão e não à superfície na qual a mesma se encontra. Outro fator é a cor do pó, que deve ser escolhida de maneira a obter-se um maior contraste fotográfico

possível. Junto com os pós, utiliza-se a fita adesiva translúcida e a fotografia para capturar as impressões [eS 01]. Na Figura 4.2, são mostrados alguns materiais utilizados na revelação de impressões digitais latentes.

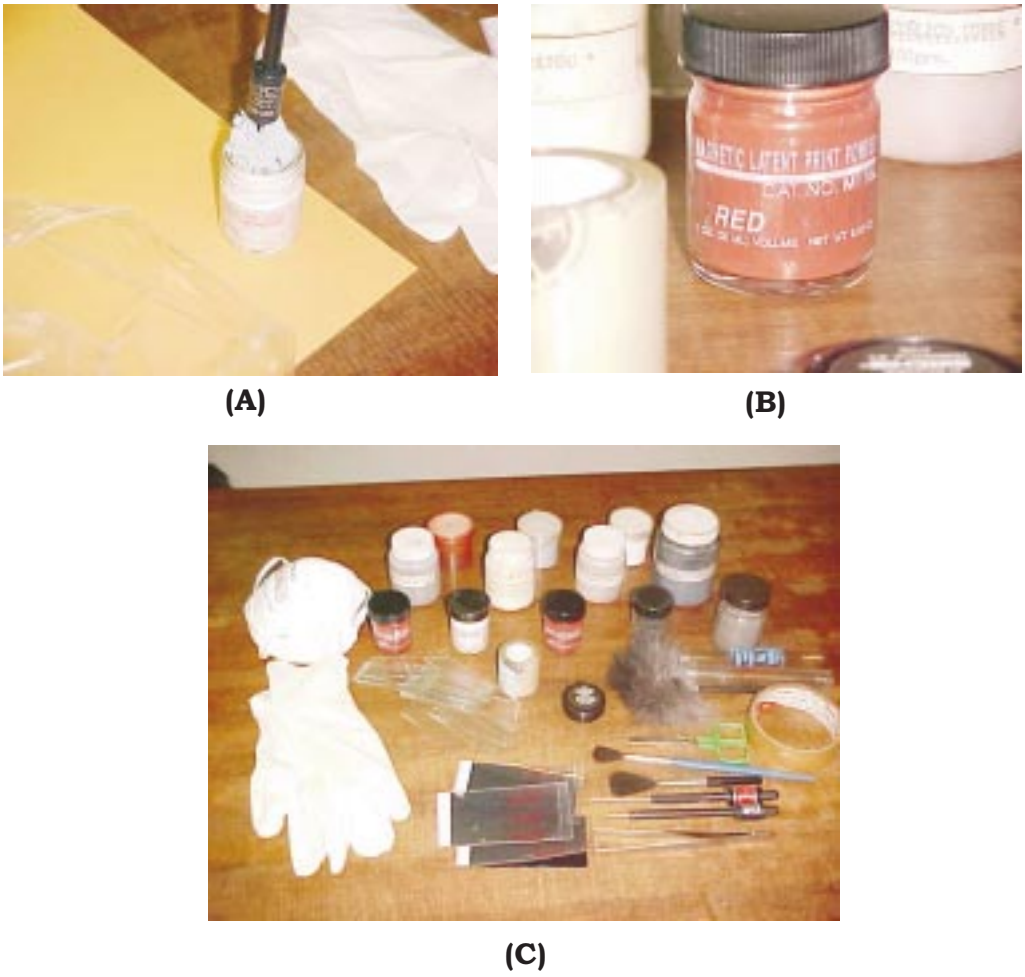


Figura 4.2: (A) Bastão magnético (B) Pó magnético e (C) Materiais diversos utilizados na revelação de latentes, como fita adesiva translúcida, pós, luvas, pincéis, etc.

Uma vez coletada a impressão latente, parte-se para a etapa de análise e confrontação da mesma. Porém, como confrontar a impressão coletada com uma base de dados de milhões de pessoas manualmente?

Por exemplo, o número de indivíduos civilmente identificados no Estado de Santa Catarina é de aproximadamente 5 milhões. Considerando esse número, observando que cada pessoa geralmente possui dez dedos, o número de comparações sobe

para 50 milhões. Em grande parte dos casos, não é possível saber a qual dos dedos da mão corresponde a impressão digital latente. Por outro lado, se considerássemos a existência de uma base de dados relativa apenas à identificação criminal, o número de pessoas identificadas seria bem menor que 5 milhões. Isso tornaria o processo de identificação mais rápido.

Em virtude da ausência de um sistema automático que realize o cotejo de impressões, o qual possibilitaria o confronto com a impressões digitais da base de dados estadual, se faz extremamente necessário a existência de um suspeito para que se possa proceder a comparação.

Apesar de a análise de impressão digital ser feita de forma manual pela Polícia catarinense, existe o interesse em utilizar um sistema automático para confronto de impressões digitais. A solução AFIS usada pelo Estado catarinense relaciona-se especificamente à parte de identificação civil, não abrangendo a área de reconstrução de imagens de impressões latentes, por exemplo. Várias empresas comercializam a solução AFIS em pacotes distintos, ou seja, o AFIS Civil e o AFIS Criminal. Uma dessas empresas é a PRINTRAK [PRI 01].

É no Instituto de Criminalística (IC) que são feitos os cotejos datiloscópicos. Eles ocorrem de acordo com os pedidos encaminhados por parte das delegacias do estado à Diretoria de Polícia Técnico-Científica. Esta diretoria é o órgão ao qual está subordinado o Instituto de Criminalística juntamente com o Instituto Médico Legal e o Instituto de Identificação. Dentre as tarefas realizadas no IC está a comparação de datilogramas, tanto aqueles encontrados em documentos oficiais como a carteira de identidade, prontuário, boletim de ocorrência, quanto os datilogramas latentes. Na Tabela 4.1, pode-se observar a demanda pelo instituto no que concerne exclusivamente ao ramo datiloscópico. Nota-se que, o número de comparações realizadas no período é bastante baixo, considerando que abrangem requisições de confronto partidas de todo o Estado cartarinense.

Tabela 4.1: Comparações dactiloscópicas realizadas pelo Instituto de Criminalística de Santa Catarina no ano de 1999 até o mês de agosto de 2001.

Ano	**1999**	**2000**	**2001**
Número de Comparações	9	20	19

Fonte: Instituto de Criminalística - SC.

4.1.1.3 Identificação Criminal

A identificação criminal é realizada nos casos em que a autoridade policial julgue necessário e em conformidade com lei federal que discorre sobre identificação criminal [lei 00]. Os indivíduos identificados criminalmente são em número bem menor e muitas vezes referem-se apenas àqueles que respondem a inquérito policial.

O formulário apropriado para identificação criminal que associa um indivíduo à prática delituosa é chamado de Boletim Individual. Tal formulário foi criado em dois modelos, sendo que ambos têm a mesma finalidade. Um deles é mais completo, uma vez que é composto pelos seguintes métodos identificativos [ALC 01]: fotográfico, datiloscópico e antropométrico. Este último observa as características morfológicas e cromáticas do indivíduo. Como exemplo de características cromáticas pode-se relacionar a cor do olho, da pele e dos cabelos de uma pessoa. Já as características morfológicas podem ser exemplificadas pelo tipo da fronte, da boca, do rosto e do nariz de um indivíduo [TOC 99]. O outro modelo de formulário, apresentado na Figura 4.7, página 65, é mais simplificado, proporcionando maior praticidade no seu preenchimento. Atualmente, este formulário é mais utilizado, porém é importante salientar que ele não considera os métodos de identificação antropométrico e fotográfico que seriam importantes para a melhor identificação do indivíduo. Outro aspecto é que os dados criminais constantes no Boletim Individual são cadastrados parcialmente em sistema de computador integrado em nível estadual.

No que diz respeito à parte criminal, é importante que as pessoas in-

fratoras da lei sejam identificadas corretamente, sob pena de uma pessoa inocente vir a sofrer medidas repressivas incabíveis por parte das autoridades. Por pessoa inocente entenda-se aquela que não tem efetivamente nenhuma relação com o fato delituoso. Um exemplo disso são os casos em que pessoas acabavam tendo emitidos mandados de prisão contra si ou sendo indiciadas em inquérito policial porque ou perderam ou tiveram seus documentos de identidade roubados, os quais acabaram sendo utilizados por criminosos [BAD 01].

Nesse sentido, no dia-a-dia policial, é necessário que se tenha um cuidado especial com a identificação de pessoas. A seguir, são apresentadas duas situações que podem levar ao erro na identificação. Uma é que, em virtude de preceito legal, muitos infratores se eximem de terem suas impressões digitais coletadas mediante a apresentação de uma carteira de identidade que, em muitos casos, é falsa ou pertence a outra pessoa [CHA 01]. Os delinqüentes costumam utilizar identidades falsas ou de terceiros numa tentativa de acobertarem sua verdadeira identidade em virtude de suas práticas delituosas. Outro aspecto é que se dá maior atenção à verificação da identidade da pessoa através do nome. Ora, sabe-se que os nomes, devido à ocorrência de nomes completos iguais, não identificam unicamente um indivíduo.

Diante de tudo isso, por que não se identifica a pessoa apresentada pela sua impressão digital? Seria isso motivo de grande constrangimento ao identificado? Curiosamente, a impressão digital merece lugar de destaque nas carteiras de identidade estaduais, pena que não ocupe este mesmo lugar em situações de identificação do cotidiano das pessoas: em uma delegacia de polícia, no momento de sacar dinheiro em um estabelecimento bancário, quando da assinatura de um documento eletrônico etc.

4.1.2 Em Nível Nacional

Assim como em Santa Catarina, há um esforço por parte dos Estados brasileiros no tocante à utilização de sistemas de informação civis e criminais mais eficientes. O uso de sistema AFIS é um exemplo disso. No estado do Paraná, a Secretaria de Segurança Pública tem tal sistema implantado há algum tempo [NAV 01]. Outro Estado

é o Mato Grosso, que já iniciou a utilização de sistemas de impressões digitais [CHA 00].

No âmbito do governo federal as perspectivas não são diferentes. A Polícia Federal vem adotanto medidas para a implantação de um sistema automatizado de impressão digital. Segundo informações prestadas pelo diretor do Instituto Nacional de Identificação [dO 01], o AFIS é parte integrante de um grande projeto na área de polícia técnico-científica, em conjunto com o governo francês, chamado PROMOTEC. Os objetivos principais desse projeto são os seguintes:

- Aumento acentuado na resolução de casos criminais pela identificação de impressões latentes deixadas nas cenas de crime.

- Melhoria da capacidade para verificar a identidade de criminoso com uso apenas da impressões digitais.

- Capacidade para confirmar a identidade de estrangeiros em tempo real.

- Melhorar a cooperação internacional em assuntos criminais através da troca de impressões digitais, com a INTERPOL, com sistemas AFIS de outros países na América do Sul e com o resto do mundo.

No Brasil, a questão legal prejudica a tomada de impressões digitais. De fato, o preceito constitucional restringe a identificação criminal aos casos onde a pessoa não apresente uma identificação civil e àqueles específicos [CHA 01]. O preceito constitucional do qual se fala é o inciso LVIII do artigo quinto de nossa carta magna, o qual é disposto a seguir: *"LVIII - o civilmente identificado não será submetido a identificação criminal, salvo nas hipóteses previstas em lei;"* [BRA 94]. Como esta matéria dependia de regulamentação legal, foi criada uma lei que especificou as situações onde se pode realizar a identificação criminal [lei 00]. Já outros países, como Alemanha, França, Noruega e Inglaterra, realizam a coleta de impressões digitais de todos os indivíduos presos, inserindo as mesmas em um banco de dados do sistema AFIS. Alguns países realizam tal procedimento inclusive com suspeitos. No caso de comprovação da inocência as impressões são retiradas do banco do sistema [CHA 01].

Um programa interessante do Ministério da Justiça é o projeto INFOSEG, que tem por objetivo principal a disponibilização e integração, junto às polícias e instituições do judiciário, de dados de inquérito policial, processos judiciais, mandados de prisão, informações penitenciárias, passaportes e veículos em nível nacional. Cabe salientar que uma premissa do projeto é apresentação de fotografia e impressões digitais [JUS 02]. Isso demonstra a preocupação com a identificação criminal no âmbito do sistema.

4.2 Organismos Americanos e a Padronização

Alguns organismos Americanos, policiais e não policiais, têm se destacado no estudo e desenvolvimento de sistemas automáticos para o cotejo de impressões digitais. Pode-se arrolar o *National Institute of Standards and Technology* e o *Federal Bureau of Investigation*, ambos atrelados ao governo americano, como entidades bastante comprometidas com o desenvolvimento tecnológico nessa área.

Hoje, observa-se um grande número de fabricantes da solução AFIS, em junção com um mercado consumidor crescente para essa tecnologia. Objetivando viabilizar a comunicação entre esses sistemas, órgãos governamentais e fabricantes do produto têm buscado estabelecer padrões para o intercâmbio de informações de datilogramas.

Nos parágrafos que seguem, são abordadas três normatizações existentes para o intercâmbio de informações relativas a impressões digitais. A primeira delas é a ANSI/NIST-ITL 1-2000, discutida na Subseção 4.2.1. A segunda, a especificação EFTS 7.0, é abordada na Subseção 4.2.2. Por último, a implementação da INTERPOL, que é apresentada na Subseção 4.2.3.

4.2.1 ANSI/NIST-ITL 1-2000

O padrão ANSI/NIST-ITL 1-2000 é fruto de uma cooperação entre o *American National Standards Institute* (ANSI), *National Institute of Standards and Technology* (NIST), através de seu órgão *Information Technology Laboratory* (ITL) e o *Fe-*

deral Bureau of Investigation (FBI), entre outras agências de cumprimento da lei. Em 1986, tais organismos desenvolveram e adotaram a primeira versão dessa normatização, que especificava um formato de dados para o intercâmbio de imagens de impressão digital e dados relativos a minúcias. Com o passar do tempo, tal normatização sofreu revisões vindo a incorporar outros tipos de imagens e atributos relativos a face, cicatriz e tatuagem [GAR 00, fIS 00, MAC 02]. Embora o padrão leve em consideração esses aspectos, enfoca-se a impressão digital nesta apresentação.

De uma forma geral, este padrão organiza os dados em uma estrutura de arquivos, registros, campos, subcampos e itens de informação. Dentro desses parâmetros, os dados e seus formatos vão sendo definidos. Por exemplo, XXXXYYYY representa uma coordenada (X,Y) onde o valor 12950964 representa a coordenada (1295, 964). TTT representa uma orientação, ou seja, uma ângulo dado em graus [GAR 00].

A norma especifica ainda que as imagens de impressão digital devem ser capturadas por um leitor de impressões ou outro equipamento operando a uma resolução mínima de 500 pontos por polegada com uma tolerância de um por cento desse valor. O valor máximo para resolução não é definido [fIS 00]. No paradigma EFTS encontra-se essa mesma especificação quanto à resolução, inclusive com a tolerância mencionada acima [oI 99a].

Cada padrão leva em consideração tipos e códigos diferenciados para a classificação dos datilogramas. Enquanto a normatização ANSI/NIST prevê um maior número de padrões de classificação, o padrão EFTS codifica basicamente quatro tipos de impressões digitais. Esses tipos são aqueles definidos por Vucetich e esclarecidos na Subseção 2.5.4. Nessas duas normatizações detecta-se a previsão de situações onde a tipificação do datilograma fica dificultada por ocasião de cicatrizes, amputação ou pela incapacidade de estabelercer uma classificação. Na Tabela 4.2, são verificados os padrões de classificação para os datilogramas com as suas respectivas codificações.

Um aspecto importante e devidamente contemplado por esses padrões são as minúcias. São elas que tornam possível a individualização de um datilograma. Dessa maneira, tanto o padrão ANSI/NIST quanto a norma EFTS definem códigos para sua representação. Através da Tabela 4.3, nota-se a existência de uma ligeira diferenciação

Tabela 4.2: Codificação ANSI/NIST e EFTS para a classificação de padrões de impressões digitais.

Padrões de Classificação	**ANSI/NIST**	**EFTS**
Arco (tipo não designado)	-	AU
Arco plano	PA	-
Arco tendido	TA	-
Presilha radial	RL	-
Presilha cubital	UL	-
Verticilo plano	PW	-
Presilha centralizada	CP	-
Presilha dupla	DL	-
Verticilo acidental	AW	-
Presilha inclinada à direita	RS	RS
Presilha inclinada à esquerda	LS	LS
Verticilo (tipo não designado)	WN	WU
Cicatriz	SR	SR
Amputação	XX	XX
Desconhecido ou não classificável	UN	UC

Fonte:[fIS 00, oI 99a, GAR 00].

Tabela 4.3: Codificação ANSI/NIST e EFTS para tipos de minúcias.

Tipo de Minúcia	**ANSI/NIST**	**EFTS**
Final de estria	A	A
Bifurcação de estria	B	B
Trifurcação (ou cruzamento)	C	-
Tipo indeterminado	D	C

Fonte: [fIS 00, oI 99a, GAR 00].

entre a codificação especificada em cada padrão, assim como os tipos de minúcias consideradas. No item 4.2.1.1, são detalhados alguns atributos pertinentes às minúcias, de acordo com a norma ANSI/NIST.

As normas ANSI/NIST e EFTS estabelecem um formato para troca de informações de impressões digitas, inclusive imagens, sem, no entanto, definir padrões para o intercâmbio de *templates* de impressão digital, apresentados na Seção 2.6, que são utilizados para o confronto de datilogramas. Na prática, ocorre que um *template* gerado em um sistema não pode ser confrontado com um *template* gerado por outro [NAV 01].

4.2.1.1 Sistema de Coordenadas das Minúcias

A norma ANSI/NIST prevê uma série de recomendações que especificam a padronização dos seguintes atributos de minúcias: coordenada x, coordenada y e orientação ou ângulo teta θ.

Conforme [fIS 00], a minúcia deve figurar no primeiro quadrante do plano cartesiano. O sistema de mensuração é dado em *unidades*, onde uma unidade é igualada a 0,01mm. Assim, o estabelecimento da ordenada que, na ilustração da Figura 4.3, é de 2500 unidades, pode ser convertida para 25mm ou 2,5cm. Nesse sistema, o valor de x cresce da esquerda para a direita e o valor de y é incrementado de baixo para cima. Tanto os valores de x quanto os valores de y devem variar entre ”0000” e ”5000” unidades, ou seja, de 0 à 5cm. Da mesma forma, a orientação relativa da minúcia é repre-

sentada em unidades, onde cada unidade equivale a 1 grau. As unidades vão de ”0” a ”359” [fIS 00].

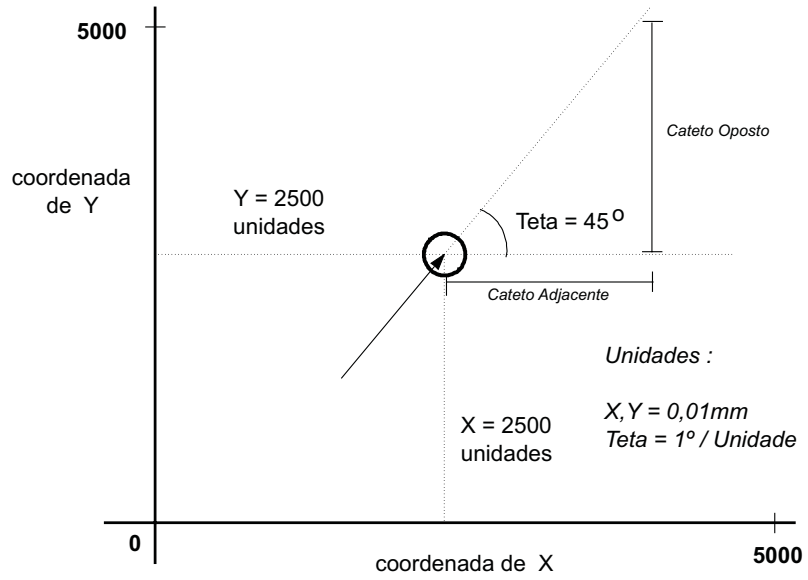


Figura 4.3: Existem três atributos relacionados às minúcias: a coordenada *x*, a coordenada *y* e o ângulo θ. Pode-se observar o primeiro quadrante do plano cartesiano onde um triângulo é formado pelo eixo horizontal com a linha composta pelo prolongamento da direção da estria que compõem a minúcia. Em seguida, o cálculo da tangente do ângulo formado pelas duas retas descritas deve ser feito. A partir daí, basta converter o valor encontrado em graus para encontrar o ângulo θ.

Na Figura 4.3, o sistema de coordenadas de minúcias é exposto. Por meio dela, mostram-se os atributos coordenada *x*, coordenada *y* e ângulo θ no plano cartesiano. Um triângulo retângulo é formado pelo eixo horizontal com a linha composta pelo prolongamento da direção da estria que compõem a minúcia [fIS 00]. A partir daí, define-se a orientação da minúcia através do cálculo da tangente do ângulo [MAI 97] formado pelos segmentos de reta correspondentes às duas retas descritas. Para tanto, é utilizada a seguinte fórmula: $\tan\theta = \frac{cateto\ oposto}{cateto\ adjacente}$. Uma vez descoberto o valor da tangente, é possível encontrar o ângulo correspondente θ na tabela de conversão de tangentes.

No caso da ocorrência de uma bifurcação, o padrão possibilita a inversão lógica para um final de estria. Assim, a orientação da bifurcação é representada como se essa inversão tivesse ocorrido [fIS 00]. Na Figura 4.4, é ilustrada a orientação das minúcias de acordo com os padrões ANSI/NIST e EFTS.

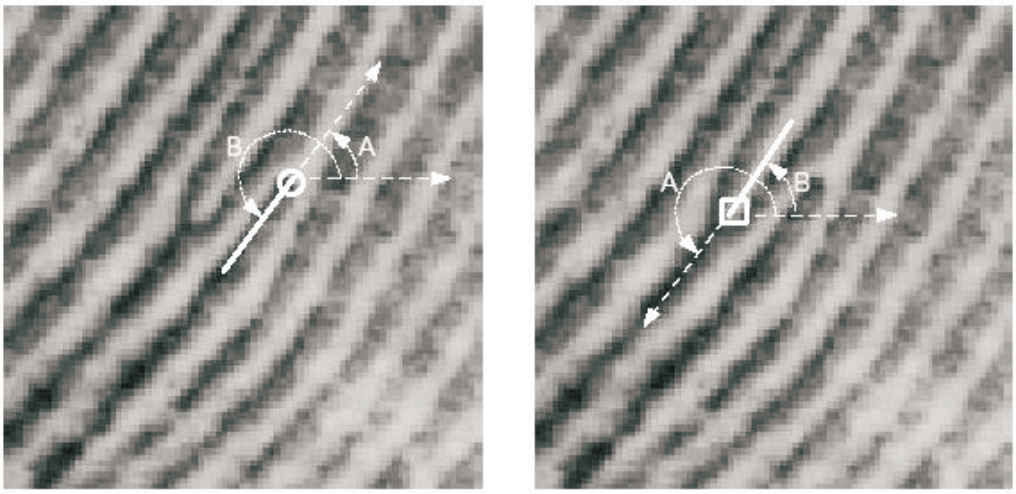


Figura 4.4: Orientação de minúcias conforme os padrões ANSI/NIST e EFTS. Os dois tipos de minúcias são apresentados acima, final de estria e bifurcação, onde o ângulo **A** representa a orientação conforme o padrão ANSI/NIST e o ângulo **B** representa a orientação segundo o padrão EFTS [GAR 00].

4.2.2 FBI/IAFIS EFTS 7.0

Enquanto o padrão ANSI/NIST visa permitir que todos os AFIS e sistemas afins possam comunicar-se, o *Electronic Fingerprint Transmission Specification* - EFTS detalha requisitos para que outras entidades possam estabelecer comunicação eletrônica com o AFIS do FBI: o *Integrated Automated Fingerprint Identification System* (IAFIS) [oI 99a]. Outro ponto distintivo entre essas duas especificações é de que a norma EFTS diz respeito somente à troca de informações relativas a impressões digitais, diferentemente daquela discutida na Subseção 4.2.1, que estabelece padrões para troca de outros tipos de informações.

Na Subseção 4.2.1, alguns aspectos relativos ao paradigma EFTS, a saber, resolução de imagem, códigos para a classificação de padrões, códigos representativos de minúcias e quanto a orientação de minúcias, já foram discutidos, estabelecendo-se inclusive comparação com a especificação ANSI/NIST. Dessa forma, no item 4.2.2.1, será destacado o ambiente para o qual foi concebida a especificação EFTS. No item 4.2.2.2, é apresentado o formato para compressão de imagens de impressão digital WSQ.

4.2.2.1 IAFIS

O projeto IAFIS teve origem nas décadas de 60 e 70, quando já se começava a investigar a possibilidade de automatizar o processo de identificação através da impressão digital. Nesse período, a divisão de identificação do FBI, juntamente com o então *National Bureau of Standards*, agora conhecido como NIST, desenvolvia algoritmos para busca e comparação de impressões digitais utilizando a computação [oI 02].

A partir daí, em vez de se coletar as impressões digitais em papel com o uso de tinta, as imagens começaram a ser digitalizadas através de *scanners* ou leitores de impressão digital. Dessa forma, as imagens de impressão digital passaram a ser comprimidas e formatadas de acordo com padrões aprovados e transmitidas eletronicamente, sendo processadas pelo IAFIS [oI 02].

O sistema compara imagens submetidas com uma grande base de dados de impressões digitais, respondendo em aproximadamente duas horas. Essa resposta inclui o histórico criminal completo da pessoa, se existir. Dessa forma, mesmo que a pessoa tenha fornecido identificação falsa, o sistema fará a identificação positiva pela comparação das impressões digitais. No passado, muitos fugitivos da justiça e criminosos perigosos eram postos em liberdade porque a informação criminal não estava disponível. Em adição à identificação criminal, o sistema processa imagens de impressões na área civil, isto é, aquelas verificações que o FBI realiza devido à requisição legal, tais como para professores, pessoas que cuidam de crianças, seguranças e outras ocupações que a sociedade necessite ter um alto grau de confiança nos que as exercem [oI 99b].

Nesse contexto, vários Estados e órgãos federais americanos submetem imagens de impressões digitais eletronicamente para que possam ser confrontadas com a base de dados existente. Uma das razões pelas quais isso funciona é a padronização para o intercâmbio dessas imagens, através da norma EFTS [oI 99b].

4.2.2.2 WSQ

Wavelet Scalar Quantization é uma especificação criada pelo FBI para compressão de imagens de impressões digitais. Junto com ela, é catalogado o algoritmo

de compressão *Joint Photographic Experts Group* - JPEG (ISO International Standard 10918-1), aplicável a imagens fotográficas. Ambos são algoritmos aprovados e catalogados pelo FBI.

Na Tabela 4.4, a codificação atribuída a cada tipo de compressão, bem como os tipos de imagens sobre os quais cada algoritmo incide, são mostrados. No caso da não utilização de compressão, o código utilizado é ”0”. O valor ”1” é utilizado para especificar o uso do algoritmo de compressão de imagens de impressões digitais WSQ, possibilitando uma taxa de compressão de 15:1. O valor ”2” é usado para especificar o uso do JPEG.

4.2.3 Interpol Implementation (INT-I)

A Interpol é uma organização internacional que tem por finalidade fomentar a integração entre organismos policiais espalhados pelo mundo na tarefa de combate ao crime. O Interpol Implementation (INT-I) é um documento escrito com a intenção de complementar a publicação ANSI/NIST-ITL 1a-1997, orientando as organizações policiais internacionais que fazem parte da Interpol [INT 02].

O padrão INT-I aborda, entre outras questões, a interoperabilidade entre sistemas diferentes e a troca de informações de impressões palmares e plantares, além das tradicionais impressões digitais. Além disso, o padrão contempla dados tipicamente da área policial. Prova disso é o campo *modus operandi*, que descreve como o infrator opera durante a prática delituosa - por exemplo, a ”mão armada”, no caso de assalto [INT 02].

A Interpol dispõe de um formulário modelo, ilustrado na Figura 4.5, onde as impressões digitais são coletadas. Esse procedimento é exigido toda vez que se enviam pedidos de consulta a ela.

O INT-I foi elaborado pelo *Interpol AFIS Experts Working Group*. O IAEG é composto por representantes de oito países membros, dentre eles o Brasil. A finalidade de grupo é prover diretrizes para países e organizações adquirirem, desenvolverem e integrarem sistemas AFIS.

Tabela 4.4: Codificação EFTS para tipos de compressão de dados.

Algoritmo de Compressão	Valor	Tipo de imagem
Não usado compressão	0	-
Wavelet Scalar Quantization (WSQ)	1	impressão digital
Joint Photographic Experts Group (JPEG)	2	fotográfica

Fonte: [oI 99a].

4.3 O Estado da Arte em Tecnologias

Existem na literatura muitas propostas de métodos para a identificação de pessoas, com graus variados de segurança e aceitação. Talvez, em decorrência das singularidades e potenciais problemas da implantação desses métodos, uma das mais importantes tecnologias de segurança resulte da mescla entre sistemas biométricos e infra-estrutura de chaves públicas. Nesse sentido, muitas organizações têm inovado no oferecimento de soluções relacionadas com a área.

Em junção com essas tecnologias, foi proposto o uso de *smart cards*, que são cartões que possuem um microprocessador e memória. Em [ASS 02], a empresa *Biometric Associates Inc.* apresenta o *BAI Authenticator*. Esse produto consiste num pequeno sensor baseado em *microchip* de silício, que captura a imagem da impressão digital através da técnica de capacitância, discutida na seção 2.6. Tal produto pode ser embutido em um *smart card* devido ao tamanho reduzido. Assim, o possuidor do cartão poderá autenticar-se diretamente no cartão. Considerando um esquema de infra-estrutura de chaves públicas, a idéia principal sobre o uso de tais cartões é armazenar uma representação ou *template* da imagem da impressão digital, a chave privada e certificado do usuário, incrementando a segurança no processo de autenticação. O custo desse cartão pode variar de U$ 600 a U$ 25 dependendo da quantidade do pedido. Na Tabela 4.5, algumas especificações sobre o sensor, ou seja, o *BAI Authenticator*, são mostradas.

Outro foco de pesquisa na área é o *Biometric Consortium* [CON 02].

Tabela 4.5: Especificações sobre o BAI Authenticator.

Especificação	**Valor**
Velocidade de reconhecimento	0.8 segundos
Taxa de Falsa Aceitação	$< 0.001\%$
Taxa de Falsa Rejeição	$< 0.08\%$

Fonte: [ASS 02].

Tal consórcio serve como ponto de referência do governo americano para pesquisa, desenvolvimento, teste e avaliação de tecnologias baseadas em identificação e verificação biométrica de pessoas. No sítio do consórcio, vários fornecedores de produtos biométricos são referenciados, bem como publicações científicas.

Muitas abordagens podem ser encontradas a respeito de tecnologias de autenticação, porém a idéia mais avançada gira em torno de modelos propostos que levam em consideração o uso de *smart cards* com sensores de impressões digitais embutidos, como apresentado em [ASS 02], estabelecendo, sobretudo, relação de tais cartões com esquemas de criptografia de chave pública. Essa tendência pode ser encontrada, por exemplo, no esquema de autenticação proposto em [Iso 01], no qual são combinados ICP, impressões digitais e *smart cards* a fim de garantir a segurança do *template*.

4.4 Conclusão

Os datilogramas tem sido amplamente usados para a identificação de pessoas. Os Estados Unidos despontam como um país bastante desenvolvido no assunto, de onde emanam padrões e pesquisas de ponta. No Brasil, nota-se que o avanço tecnológico nessa área é bastante modesto em relação a outras partes do mundo. Nas polícias, organizações tradicionalmente interessadas pela identificação datiloscópica, não se constata uma utilização mais acentuada do reconhecimento automatizado de impressões digitais no cotidiano.

Através deste capítulo, pôde-se perceber que a impressão digital é bastante utilizada em situações práticas onde se deseja identificar pessoas. Uma dessas situações é o uso de datilogramas para a realização de assinatura digital. O produto apresentado na Seção 4.3 explora tanto o uso de datilogramas como de cartões no processo de assinatura digital a fim de aumentar a confiabilidade no procedimento de assinatura. Essa possibilidade de usar impressões digitais e cartões em sistemas de assinatura digital é considerada no modelo que se propõe no capitulo 5.

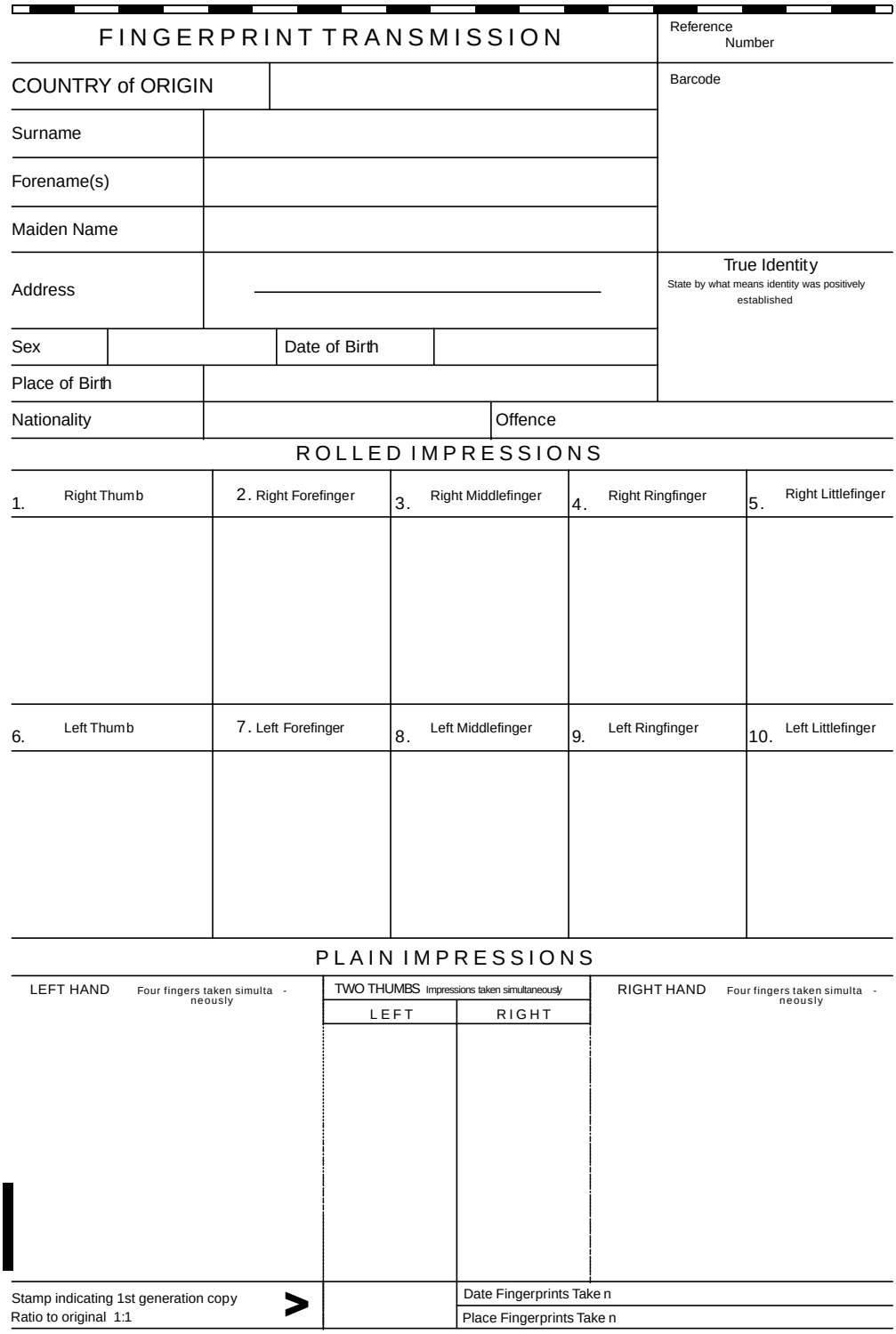


Figura 4.5: Formulário padrão para transmissão de impressões digitais à Interpol. Este formulário é utilizado quando do pedido de consultas à Interpol [INT 02]. Alguns dados como o país de origem do pedido, nome da pessoa, endereço, nacionalidade e data/local em que as impressões foram coletadas são exigidos. A coleta das impressões digitais dos cinco dedos (polegar, indicador, médio, anular e mínimo) de cada mão é realizada de maneira rolada e pousada. Essas duas formas de coleta foram discutidas no item 4.1.1.1, onde foi apresentada a identificação civil no Estado de Santa Catarina.

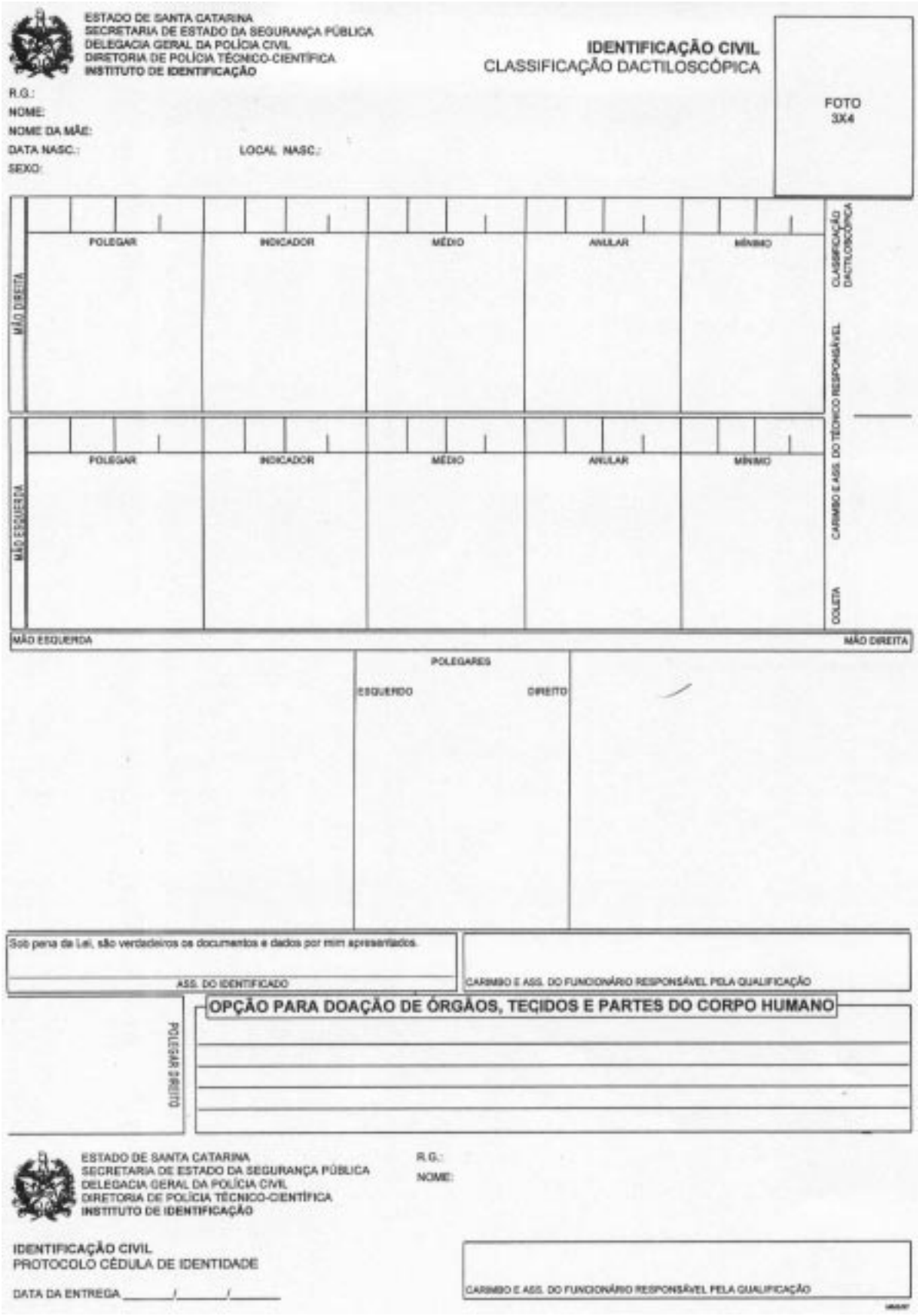


Figura 4.6: Ficha Classificação Datiloscópica.

ESTADO DE SANTA CATARINA

BOLETIM INDIVIDUAL

Nº

DELEGACIA POLICIAL

COMARCA | TERMO

I — DO CRIME OU DA CONTRAVENÇÃO

Distrito judiciário-administrativo onde ocorreu o delito | OCORREU NA ZONA ☐ URBANA ☐ RURAL

DATA CERTA OU PROVÁVEL | OCORREU DE ☐ DIA ☐ NOITE

Foi praticado em dia de trabalho, domingo, feriado ou dia santificado de festa?

LUGAR DA OCORRÊNCIA

MEIO EMPREGADO | MOTIVOS PRESUMÍVEIS

II — DO AUTOR

NOME | ALCUNHA

INICIADO COMO INCURSO NO

SEXO ☐ M ☐ F | IDADE | ANO DE NASCIMENTO | ESTADO CIVIL

NACIONALIDADE | NATURALIDADE

RESIDÊNCIA | PROFISSÃO

ESTAVA DESEMPREGADO ☐ SIM ☐ NÃO | INSTRUÇÃO | RELIGIÃO OU CULTO | COR

TEM FILHOS ☐ SIM ☐ NÃO | QUANTOS? | SÃO ☐ LEGÍTIMOS ☐ ILEGÍTIMOS ☐ LEGITIMADOS

Estava alcoolizado ou sob a ação de entorpecentes | INICIADO O PROCESSO EM

PRESO ☐ FLAGRANTE ☐ PREVENTIVAMENTE | DATA | TEM ANTECEDENTES CRIMINAIS ☐ SIM ☐ NÃO

FOI IDENTIFICADO EM | RECOLHIDO A | SOLTO EM VIRTUDE DE HABEAS-CORPUS

Solto em virtude de fiança, no valor de | EVADIU-SE?

FILIAÇÃO

☐ LEGÍTIMO ☐ ILEGÍTIMO ☐ LEGITIMADO

PAI | MÃE

III — DA VÍTIMA

NOME | ALCUNHA

NACIONALIDADE | NATURALIDADE | SEXO ☐ M ☐ F | IDADE

ESTADO CIVIL | COR | RESIDÊNCIA

PROFISSÃO | INSTRUÇÃO

TEM FILHOS ☐ SIM ☐ NÃO | QUANTOS? | DÁ-SE AO VÍCIO DA EMBRIAGUEZ ☐ SIM ☐ NÃO

IV — OUTROS ELEMENTOS

Valor dos danos (nos crimes contra a propriedade) | ARMAS APREENDIDAS

Os autos foram remetidos ao Juiz Criminal em

Polegar direito do indiciado

LOCAL E DATA

O ESCRIVÃO

(Esta parte será remetida à repartição incumbida do levantamento da estatística policial-criminal).

Figura 4.7: Boletim Individual.

Capítulo 5

Assinatura Digital Usando a Impressão Digital

Uma das principais críticas realizadas à assinatura digital diz respeito à fraca ligação entre o assinante e sua chave de assinatura, que é a denominação atribuída à chave privada, quando utilizada na cifragem de uma mensagem. O processo todo de assinatura digital não fornece nenhuma garantia de que o proprietário da chave, e somente ele, a utilizou para efetuar a assinatura. Essa vulnerabilidade é freqüentemente relatada no mundo científico [HER 95, ELL 99, FRE 00].

Por outro lado, os ataques a ambientes de assinatura digital têm levado estudiosos na área a empreender uma busca por mecanismos de proteção à chave privada. Muitos desses ataques tem por objetivo a sua descoberta, embora existam outras formas de ataques registradas na literatura [FRE 00].

Neste capítulo, propõe-se um modelo para assinatura digital combinado com o uso de impressões digitais. A intenção é aumentar a segurança e a ligação entre proprietário e chave através de uma característica pessoal do usuário. Procura-se mostrar os aspectos ocasionados pela junção dessas tecnologias. Na literatura relacionada são encontradas referências a essa associação, juntamente com *smart cards*, para o estabelecimento de sistemas de autenticação de alto nível [Iso 01, HOJ 00].

Na Seção 5.1, discute-se as formas de gerenciamento de chave privada.

Na Seção 5.2, é descrito o modelo proposto de assinatura digital usando a impressão digital. Na Seção 5.3, é detalhado o protocolo de autenticação da identidade de usuário para a realização de assinatura digital, que usa impressões digitais, *smart cards* e senhas para verificar a identidade da pessoa. Na Seção 5.4, discute-se os requisitos de segurança do documento eletrônico, entre outros aspectos. Na Seção 5.5, apresenta-se um protótipo de um sistema computacional desenvolvido visando mostrar a viabilidade de se usar a impressão digital para autenticar o usuário durante o processo de assinatura digital. Na Seção 5.6, concluí-se este capítulo.

5.1 O Gerenciamento de Chave

Conforme foi discutido no Capítulo 3, a criptografia de chave pública é marcada pela presença de duas chaves criptográficas. A chave pública deve estar disponível a todos, não havendo necessidade de segredo sobre o seu conhecimento, devendo possuir autenticidade. Por outro lado, o segredo deve ser uma característica intrínseca da chave privada.

Dessa forma, a segurança de um ambiente de autenticação baseado em criptografia por chave pública está diretamente relacionado ao nível de proteção provido à chave privada, bem como à autenticidade da chave pública [oC 94]. A autenticidade desta última pode ser provida por meio de certificados digitais. Já a proteção àquela deve ser cuidadosamente estudada e planejada.

O objeto desta seção é o gerenciamento da chave privada, representada neste trabalho por K_R. É importante perceber que ela pode ser usada por qualquer pessoa que tenha seu controle, inclusive impostores e levianos que atuam no meio digital. Imagine essas pessoas assinando documentos e gerando obrigações em seu nome! Isso é, no mínimo, desagradável! A seguir, são relacionadas três estratégias para sua gestão:

- **ARMAZENAMENTO EM DISCO RÍGIDO** - Uma das maneiras mais simples de proteger a chave de assinatura é cifrá-la usando uma senha. Uma desvantagem é que se alguém tiver acesso ao computador e descobrir a senha, poderá acessar a chave

privada. Outra desvantagem é que para ser usada, a chave privada deve ser decifrada e carregada para a memória do computador o que a torna vulnerável a ataques dentro da memória. Além disso, essa estratégia não permite boa mobilidade. Em [FRE 00], é discutida a insegurança decorrente do armazenamento de K_R em um computador devido aos vários tipos de ataques aos quais poderá estar sujeita.

- **ARMAZENAMENTO EM MEIO REMOVÍVEL** - O armazenamento em disquetes ou CD-ROM é um opção. Basicamente, traz as mesmas vulnerabilidades apresentadas no item anterior, possuindo, porém, melhor mobilidade.

- **ARMAZENAMENTO EM SMART CARDS** - Os ”cartões inteligentes” possuem processador e memória. Neles, é possível o armazenamento da chave privada e do certificado digital do usuário. As operações de assinatura são executadas dentro do cartão, sendo que a chave privada nunca sai de dentro do mesmo, o que proporciona maior segurança. O desenvolvimento desses cartões tem apontado para a possibilidade de manipulação de informações biométricas nos mesmos, como apresentado na Seção 4.3. Sob esse aspecto, assim como acontece com a chave privada, a informação biométrica não precisa ser copiada para a memória do computador ou mesmo ser transmitida através de uma rede, diminuindo riscos de segurança [oC 94]. Outro aspecto relacionado ao uso de cartões é que permitem uma ampla mobilidade - um cartão pode ser levado no bolso.

Desde que somente um determinado usuário possua uma dada chave privada, a assinatura gerada por essa chave faz prova irrefutável da sua identidade [oC 94]. Na verdade, mais do que possuí-la, o usuário deveria ser a única pessoa capaz de acessá-la e, em conseqüência disso, usá-la. Com essa finalidade, propõe-se o uso de *smart cards* com a inserção de impressões digitais no processo de assinatura. Elas têm sido aceitas como prova de identidade há tempos, devido ao seu caráter único e permanente em cada pessoa.

5.2 Modelo Proposto

O contexto no qual está inserido o modelo proposto para assinatura digital usando a impressão digital é o da Infra-estrutura de Chaves Públicas - ICP. No esquema exposto a seguir, pode-se notar a presença de algumas entidades componentes de tal infra-estrutura, tal como a Autoridade Certificadora e a Autoridade de Registro, explicadas na Seção 3.3 [Hun 01].

Na criação do modelo, considerou-se as seguintes técnicas e mecanismos de segurança:

- A criptografia assimétrica e simétrica são abordadas. Esta última é usada para tornar incompreensível ou cifrar a chave privada do usuário, a fim de protegê-la contra intrusos. A primeira serve à confecção da assinatura digital.

- As funções resumo de mensagem são utilizadas principalmente no processo de confecção da assinatura digital, a fim de garantir a integridade dos dados.

- Para autenticar a identidade do usuário e habilitá-lo a realizar a assinatura digital propõe-se o uso de Impressão Digital, *Smart Card* e Senha.

A seguir, explica-se de que maneira esses mecanismos e técnicas descritas acima, uma vez combinados com ICP, poderão servir à autenticação de usuários e posterior assinatura de documentos eletrônicos. No decorrer desta seção, é descrito e explicado detalhadamente o modelo proposto para assinatura de documentos eletrônicos exposto na Figura 5.1.

Parte-se do princípio de que o usuário detém um cartão com sua chave de assinatura e uma representação de sua impressão digital, podendo portá-lo a qualquer lugar. Para que seja possível o uso da referida chave, o reconhecimento da sua impressão digital é imprescindível no momento do uso para assinatura. A idéia é que no próprio cartão exista um leitor de impressão digital possibilitando sua leitura. A partir daí, um sistema para reconhecimento de impressões digitais passa a atuar na análise das impressões. Tais sistemas foram amplamente discutidos na Seção 2.6.

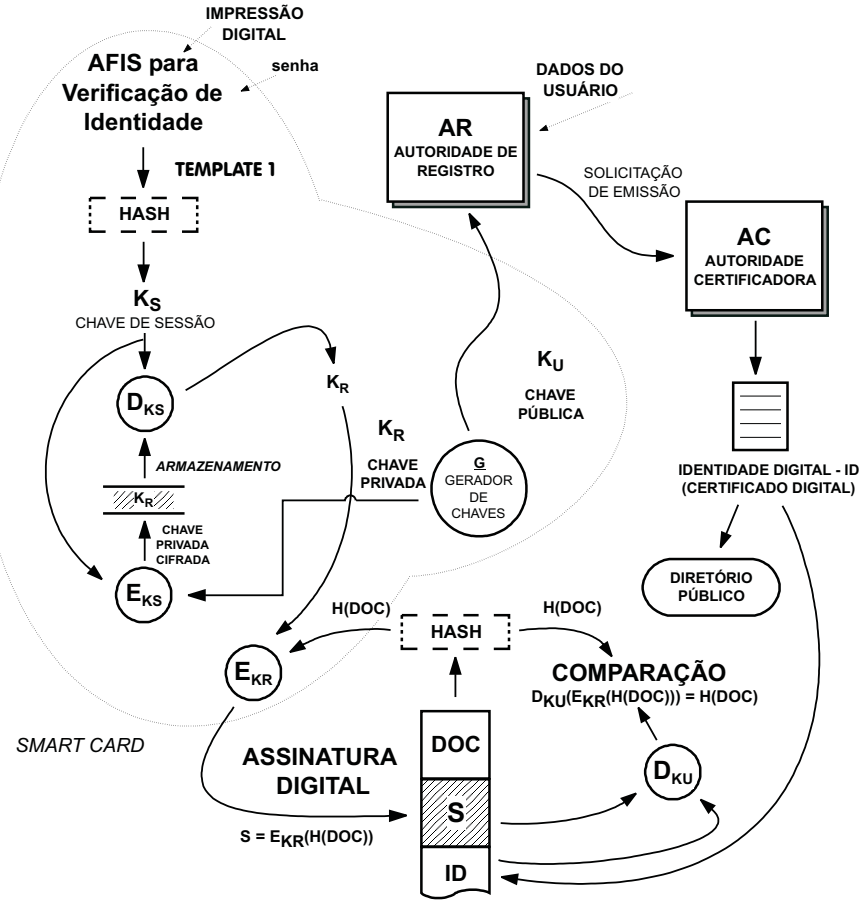


Figura 5.1: Estrutura geral do sistema de assinatura digital proposto. A área pontilhada da figura diz respeito aos dados armazenados e funções executadas no interior do *smart card*. Um aspecto importante diz respeito à geração do par de chaves criptográficas dentro do cartão. Assim, tanto na sua criação quanto no uso para assinatura de documentos, a chave privada nunca sairá de dentro do cartão.

Na etapa de autenticação de usuário, um AFIS para verificação, explicada na Subseção 2.2.4, é usado para habilitar, ou não, o usuário ao uso de K_R. Dessa forma, um confronto entre dois *templates* de impressão digital é procedido, um já armazenado no cartão e outro produzido no momento da autenticação, de forma que o próprio *template* que estava armazenado servirá para o deciframento de K_R, em caso de confronto positivo. Outro aspecto diz respeito à proteção do *template* que, assim como a chave privada, é uma informação pessoal. Assim, ele é decifrado com uma senha digitada pelo usuário no momento da autenticação. Na Seção 5.3, é apresentado o protocolo de autenticação de usuário e a criação do código de assinatura digital do documento

eletrônico.

No caso de confronto positivo, o resumo do *template* armazenado servirá de chave de sessão K_S para cifrar a chave privada do usuário: $E_{Ks}(K_R)$. Posteriormente, quando da necessidade de usar K_R para a assinatura, o mesmo processo descrito anteriormente é procedido, porém, desta vez, o resumo do *template* é utilizado para decifração da chave privada: $D_{Ks}(E_{Ks}(K_R)) = K_R$. Deve-se notar que, K_S é obtida através do resumo do *template* armazenado no cartão tanto para o decifrамento quanto para o ciframento da chave privada, ou seja, é a mesma nas duas situações. Nesse sentido, usa-se a criptografia simétrica a fim de proteger a chave particular do usuário, uma vez que a mesma chave usada para cifrar também decifra a informação. Outro aspecto é a geração do par de chaves assimétricas dentro do cartão. Assim, a chave pública é enviada inicialmente à AR e depois à AC para a criação do certificado digital do usuário, aqui chamado de Identidade Digital ou ID, enquanto a chave privada fica desde o momento de sua geração armazenada no *smart card*, conforme visto na Figura 5.2.

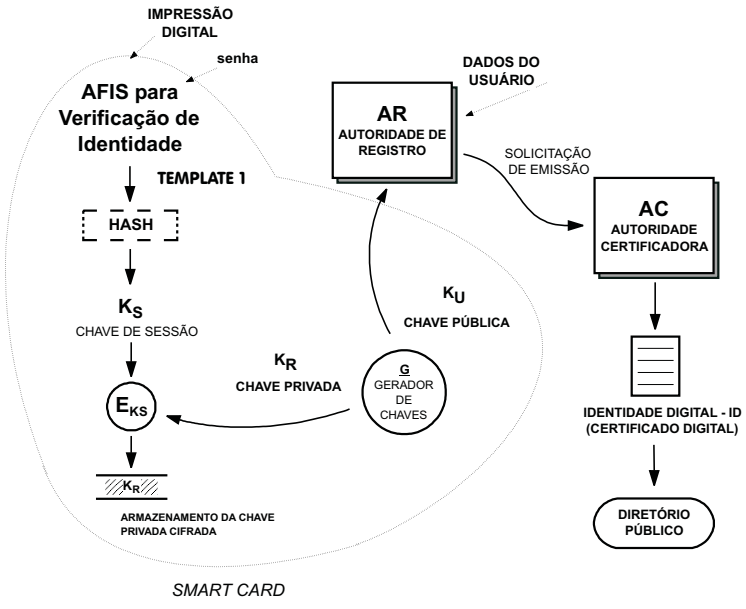


Figura 5.2: Processo de inicialização do *smart card* para assinatura digital com impressão digital.

As considerações traçadas até aqui destinam-se à restrição do acesso à chave privada, que, uma vez sendo liberada, poderá ser utilizada na assinatura de docu-

mentos eletrônicos. Na Figura 3.1, um esquema para assinatura digital é ilustrado. Nessa figura, a abordagem assimétrica é utilizada para a confecção de assinatura digital, sem sigilo da mensagem enviada. Conforme esse paradigma, um resumo do documento é gerado e cifrado com a chave privada K_R do usuário. Esse ”resumo cifrado” é anexado ao documento, juntamente, neste caso específico, com o certificado digital do signatário. Desse modo, dentro do próprio documento digitalmente assinado haverá dados suficientes para posterior verificação de assinatura. A função de assinatura de um documento é dada por $S = E_{KR}(H(DOC))$. A realização da assinatura é ilustrada na Figura 5.3.

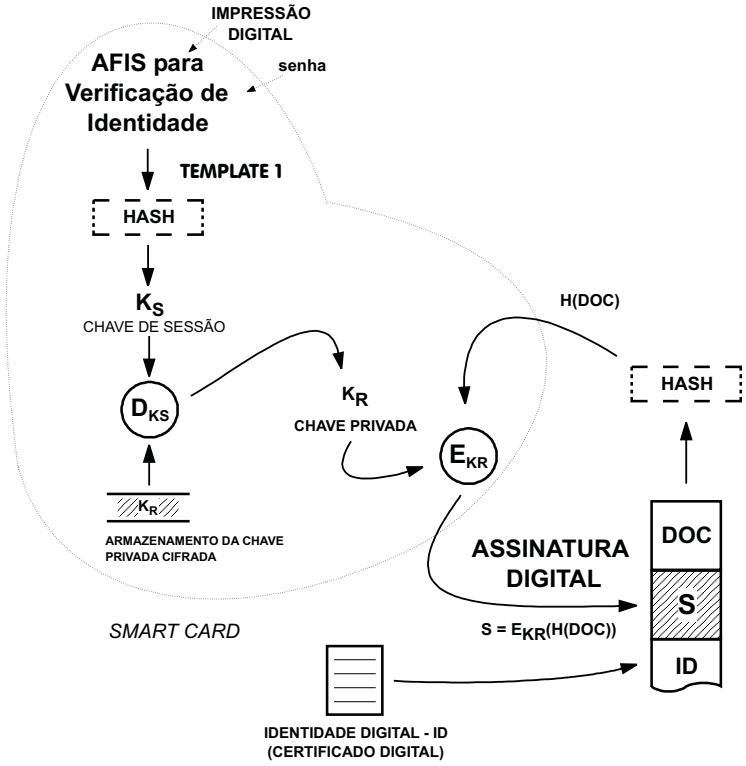


Figura 5.3: Processo de geração de assinatura digital de documentos eletrônicos com o *smart card*.

Quando da verificação da assinatura, o usuário verificador procede como segue. É decifrado o resumo do documento recebido com uso da chave pública do seu assinante e calculado um novo resumo a partir do mesmo documento. A chave pública K_U poderá ser obtida através do certificado digital do assinante. Tal certificado, conforme proposta, será anexado ao documento assinado, estando disponível também em diretório

público. Logo em seguida, é realizada a comparação entre os dois resumos. A função de verificação de assinatura é dada por $V = D_{KU}(S)$. Dessa forma, se ao final do processo os dois resumos forem iguais, então tem-se a confirmação não só da origem como da integridade da mensagem, certificando que o documento não foi corrompido desde a data da sua assinatura. Dessa maneira, a correção dos dados constantes no documento é garantida. Na Figura 5.4, é mostrado o processo de verificação de assinatura digital.

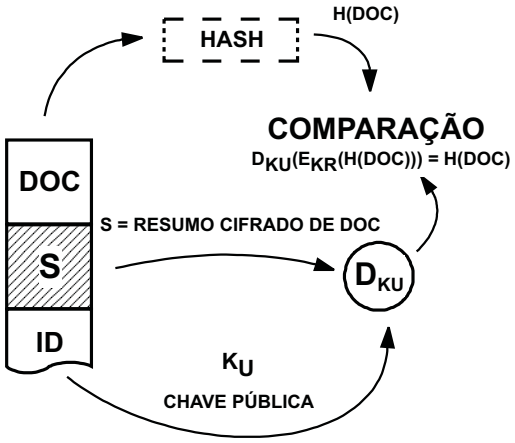


Figura 5.4: A verificação da assinatura é a usual, conforme ilustrado na Figura 3.1.

5.3 Protocolo de Autenticação

O processo de autenticação de usuário acontece dentro de um *smart card*. Tais dispositivos são similares aos conhecidos cartões de crédito e magnéticos, porém mais versáteis, possibilitando o processamento e armazenamento de dados. Associados à criptografia, proporcionam alto nível de segurança às informações registradas, dificultando sua leitura. Basicamente, tais dispositivos contribuem para os sistemas computacionais em dois aspectos. O primeiro diz respeito à portabilidade, porque o titular do cartão pode levá-lo consigo para o lugar onde desejar. O segundo está ligado à segurança dos dados. Eles são manipulados no interior do cartão, sem a necessidade de cópia para o computador ou transmissão via rede, diminuindo as possibilidades de ataque.

No entanto, para garantir que quem está usando o cartão é o seu titu-

lar, é preciso oferecer algo mais do que simplesmente o *smart card*. Um cartão pode ser emprestado, perdido, furtado, extraviado, entre outras tantas situações que podem propiciar o seu uso indevido por terceiros. Considerando isso, foram estabelecidas três formas de autenticação, relacionadas na Tabela 5.1, para o modelo proposto neste trabalho de pesquisa: senha, *smart card* e impressão digital.

Tabela 5.1: Formas de autenticação usadas no sistema de assinatura digital proposto [RAT 01b].

FORMA	**MÉTODO**
Senha	Baseado no que o usuário sabe
Smart card	Baseado no que o usuário tem
Impressão digital	Baseado no que o usuário é

Procura-se, por meio da junção de senhas, *smart cards* e impressões digitais, compor um esquema de autenticação forte, visando reduzir ao máximo a tentativa de fraudes no processo. Na Figura 5.5, é ilustrado o protocolo de autenticação de usuário baseado nessas três formas de autenticação. Nesse contexto, ficam permanentemente gravados no cartão os seguintes dados, introduzidos antes do seu primeiro uso:

- Certificado digital do usuário
- Chave privada do usuário cifrada, "K_R"
- *Template* do usuário cifrado, "template1"
- Resumo da senha para acesso ao *template*, "H(senha1)"

Esses dados são necessários para que se possa proceder a autenticação do usuário, bem como produzir a assinatura digital. Eles são de cunho pessoal, uma vez que estão relacionados ao titular do cartão.

A assinatura digital se dá mediante a prévia autenticação do usuário. O processo é iniciado com a entrada da impressão digital do usuário e uma senha. Após

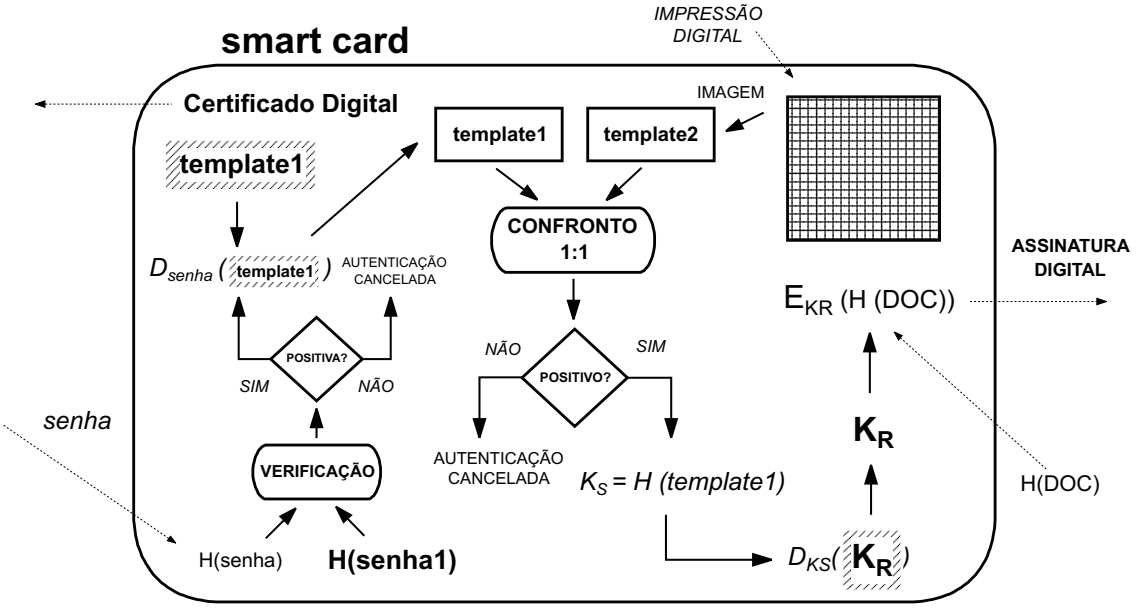


Figura 5.5: Protocolo de autenticação de usuário e assinatura.

verificada a identidade do usuário, um resumo do documento a ser assinado é cifrado com a chave privada que está no cartão. As saídas do cartão são: a assinatura digital de um documento e o certificado digital do usuário. De forma complementar, na Figura 5.6, é descrito um algoritmo que contempla os passos para execução da tarefa de autenticação e assinatura digital, ocorridas no interior do cartão.

A aquisição da imagem da impressão digital é realizada por um sensor baseado em *microchip* silício embutido no cartão. Dentre as tecnologias de sensores apresentadas na Seção 2.6, essa técnica permite a construção de sensores em tamanho compatível com as dimensões de um cartão a fim de que possam ser embutidos nos mesmos.

É importante considerar que o uso dessas tecnologias sobrecarrega o *smart card* em função, sobretudo, dos algoritmos criptográficos e de autenticação executados internamente, demandando memória e poder de processamento. Rotinas como sensitividade da impressão digital e confronto entre *modelos biométricos* estão, por exemplo, atreladas ao processo de autenticação. Para ampliar a capacidade de memória e o poder de processamento, algumas propostas têm sido apresentadas. Uma das alternativas é a

recebe senha;
gera resumo de senha;
se resumo de senha = resumo de senha1 então
decifra template1 usando como chave senha;
adquire imagem da impressão digital;
gera template2 a partir da imagem;
compara template1 com template2.
se template1 = template2 então
chave de sessão = resumo de template1;
decifra K_R usando chave de sessão;
recebe resumo do documento;
cifra resumo do documento com K_R;
envia assinatura digital;
envia certificado digital.

Figura 5.6: Procedimento executado no *smart card*.

utilização de dois processadores, sendo um deles um processador criptográfico dedicado que acelera os cálculos relativos à criptografia [NOO 00, LIU 01a].

5.4 Tecnologia de Documento Eletrônico

Em geral, quando da conceituação da palavra documento, os autores dividem-se em duas linhas de pensamento. Enquanto uns entendem que ele deva ser algo material, outros ressaltam o seu conteúdo independente do tipo de suporte utilizado para a informação. Considere as seguintes definições de ”documento”:

- *”Qualquer base de conhecimento, fixada materialmente e disposta de maneira que se possa utilizar para consulta, estudo, prova, etc. Escritura destinada a comprovar um fato; declaração escrita, revestida de forma padronizada, sobre fato(s) ou acontecimento(s) de natureza jurídica.*” [dHF 99]
- *”A característica de um documento é a possibilidade de ser futuramente observado; o documento narra, para o futuro, um fato ou pensamento presente.*

> *Daí ser também definido como prova histórica. Diversamente, representações cênicas ou narrativas orais, feitas ao vivo, representam um fato no momento em que são realizadas, mas não se perpetuam, não registram o fato para o futuro. Se esta é a característica marcante do documento, é lícito dizer que, na medida em que a técnica evolui permitindo registro permanente dos fatos sem fixá-lo de modo inseparável em alguma coisa corpórea, tal registro também pode ser considerado documento. A tradicional definição de documento enquanto coisa é justificada pela impossibilidade, até então, de registrar fatos de outro modo, que não apegado de modo inseparável a algo tangível.*" [MAR 98]

No primeiro conceito, tem-se uma visão mais tradicional onde o autor claramente condiciona a existência do documento a um suporte físico. No entanto, a segunda citação abre novas perpectivas para o significado da palavra documento, pois valoriza o seu teor e não o suporte onde está disposta a informação. Ressalta, sobretudo, o "registro permanente" dos fatos como característica marcante do documento, seja através do papel ou outra forma que cumpra essa condição.

Essa flexibilização de conceito é muito importante, pois a tecnologia tem mostrado a possibilidade de trabalho com uma nova forma de documentação: a eletrônica ou digital. Essa forma de documento pode ser vantajosa, quando comparada à física. Duas vantagens são o grau de conservação e a rapidez de transmissão do documento digital. Por outro lado, discute-se amplamente a possibilidade de fraude nos documentos digitais, procurando esclarecer se tais documentos são tecnicamente confiáveis ou não, garantindo autenticidade, não-repúdio, integridade, não-reuso, entre outros aspectos.

De acordo com [GAN 01], os requisitos que devem ser considerados em uma análise da segurança dos documentos, tanto físicos quanto eletrônicos, são: *tempestividade*, *autenticidade* e *integridade* do documento. Além disso, o mesmo autor atrela a validade jurídica do documento eletrônico ao suprimento desses três requisitos já citados.

A tempestividade, ou seja, a data e hora em que o documento foi assinado pode ser provida através da técnica de *time stamping*. Nesse caso, existem propostas que visam conferir maior sincronização ao processo de datação do documento digital, como a criação de um servidor de *time stamping* [PAS 01]. Embora não contemplada

na Figura 5.1, a questão da datação do documento eletrônico é pré-requisito para que o mesmo possa ter validade jurídica, segundo [GAN 01]. Os sistemas de assinatura digital que não levam em consideração a data e a hora em que o documento eletrônico foi assinado são ditos *atemporais*. A questão da datação digital é complexa, devendo considerar, entre outros elementos, o papel da Autoridade de Datação em sistemas de infra-estrutura para assinatura de documentos eletrônicos [PAS 01].

Já a autenticidade e integridade dos documentos eletrônicos são requisitos supridos pelo uso da técnica de assinatura digital mostrada na Figura 3.1. Porém, para aprimorar a autenticação quando da assinatura de documentos eletrônicos, foi adicionado um esquema biométrico junto ao processo de assinatura digital, no caso impressão digital. Com ele, procurou-se aumentar a segurança no momento da assinatura de um documento digital, conferindo maior confiança à etapa de autenticação de usuário.

Com efeito, os três requisitos discutidos devem ser satisfeitos para que se tenha uma assinatura digital coesa. No entanto, existem outros aspectos que devem ser considerados para que a assinatura digital de documentos eletrônicos seja realizável. Na Subseção 5.4.1, são discutidos alguns subsistemas importantes na montagem do documento digital. Na Subseção 5.4.2, pondera-se sobre o nível de confiança fornecido pelo sistema de assinatura digital apresentado nesta dissertação.

5.4.1 Subsistemas de Assinatura

Para que a assinatura digital de documentos eletrônicos seja possível, é necessário que existam alguns subsistemas compostos de *hardware* e *software* localizados no computador do usuário. Em suma, eles dizem respeito à etapa de autenticação de usuários e de montagem do documento eletrônico. Na Figura 5.7, é apresentado o contexto em que um documento eletrônico é assinado e montado.

O subsistema1 está localizado entre o homem e o cartão e visa autenticar o usuário legítimo do cartão e autor do documento eletrônico sendo por ele assinado. Esse subsistema tem sido amplamente discutido ao longo deste trabalho, já que é proposto o uso de esquema biométrico no processo de assinatura de documentos digitais.

Assim, faz-se necessário que exista um *scanner* de impressão digital para coletar esse dado biométrico do usuário. Essa identificação é submetida ao cartão, onde é feita a autenticação de usuário e gerado o código de assinatura. Quanto à localização do *hardware* que proporcionará a leitura da impressão digital, existem duas possibilidades: ele poderá estar embutido no cartão ou fora dele. Nesse caso, a identificação biométrica seria copiada para a memória RAM do microcomputador e submetida ao cartão. Um problema é que nessa memória a identificação biométrica poderia ser alvo de ataques ou mesmo cópias de seu conteúdo. Por isso, a primeira possibilidade, embutido no cartão, poderá proporcionar maior segurança na autenticação de usuário, uma vez que a sua identificação irá diretamente para a memória interna do cartão e lá será manipulada. Dessa forma, a autenticação de identidade do usuário deveria fazer parte do *smart card*. A idéia principal é de que no próprio cartão aconteça a autenticação e a geração do código de assinatura.

Além disso, deve-se considerar a existência de outros dois subsistemas que interagem diretamente com o *smart card* na montagem do documento eletrônico. Eles ficam localizados fora do cartão, servindo de suporte na operação de assinatura digital. Tais subsistemas são *softwares* que deveriam ser instalados no microcomputador do usuário. O subsistema2 é responsável pelo cálculo do resumo de um documento e a posterior submissão desse resumo ao cartão. O subsistema3 é responsável por anexar o código de assinatura ao documento. Ante o exposto, percebe-se que esses dois *softwares* realizam tarefas indispensáveis no processo de assinatura digital.

É importante salientar o nível de confiança que deve ser depositado nas tarefas desempenhadas pelos subsistemas 2 e 3. Não é fornecida garantia alguma acerca do funcionamento fidedigno desses programas. Ou seja, não há garantia alguma de que o resumo enviado ao cartão é aquele resumo relativo ao documento que está sendo visualizado na tela do computador. Outro problema é que o *smart card* é burro, ou seja, ele não sabe o que está assinando - ele simplesmente assina o resumo de um documento que lhe é enviado. Por isso, essas características tornam o sistema mais vulnerável a fraudes. Além disso, *software* de visualização também deve ser levado em consideração quando se fala da confiança na montagem final do documento eletrônico.

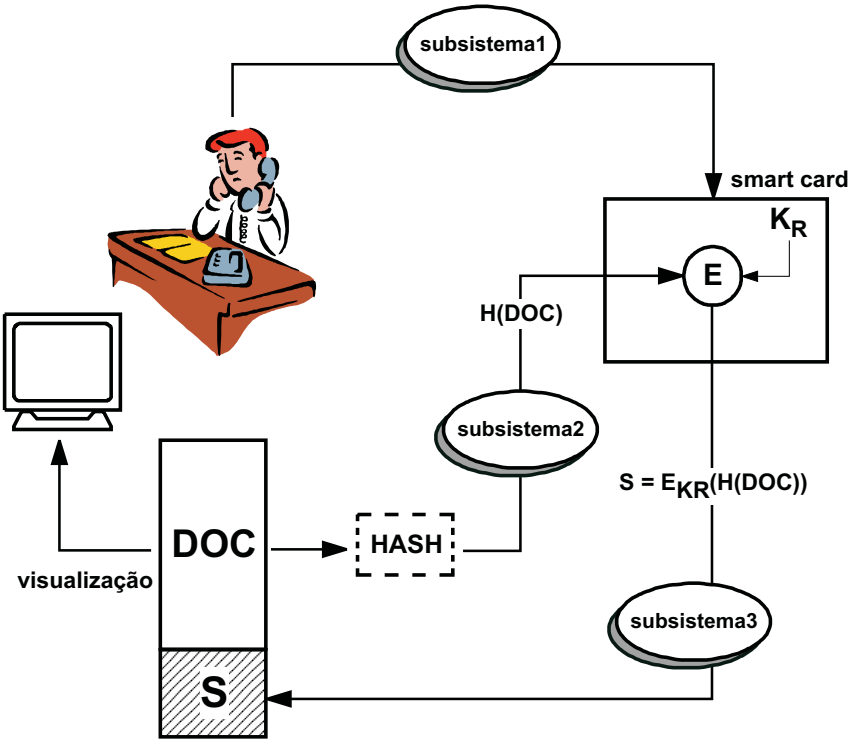


Figura 5.7: Subsistemas para assinatura digital de documentos eletrônicos.

5.4.2 Segurança do Documento Eletrônico

A crescente utilização do documento eletrônico ou digital tem suscitado várias discussões acerca da real segurança, ou seja, o nível de confiança oferecido pelos documentos digitais. Examina-se a possibilidade de equiparação dessa mídia aos documentos tradicionais ou físicos, para que também possuam validade jurídica. Para tanto, ambas formas de documentação devem atender aos mesmos requisitos de segurança, possuindo tempestividade, integridade e autenticidade. Esses parâmetros têm pautado os documentos físicos, os quais têm sido amplamente utilizados em nosso dia-a-dia. Todavia, para que os documentos eletrônicos possam também satisfazer tais requisitos, é importante analisar a assinatura dos documentos físicos. Embora esse paradigma seja superado pelo eletrônico, por fatores como conservação e rapidez de transmissão, deve-se considerar a existência de características de segurança do mundo físico ainda não alcançadas pelo documento eletrônico.

Particularmente, o sistema de assinatura apresentado ao longo deste tra-

balho fornece proteção à chave de assinatura e, além disso, cria uma ligação entre o usuário e essa chave através de uma informação pessoal, ou seja, a impressão digital. Entretanto, verificou-se no decorrer deste estudo que a identificação através desse esquema biométrico é questionável, especialmente, pelo fato de que cientistas conseguiram reproduzir dedos artificiais a partir de ”dedos vivos” e de impressões latentes, comprovando assim, que nem mesmo as impressões digitais estão imunes a fraudes. Os testes realizados revelaram que até mesmo o sensor por capacitância, tecnologia utilizada nos *smart cards*, obteve alto nível de aceitação de dedos falsos. No Apêndice A, é apresentada detalhadamente essa pesquisa a respeito dos dedos artificiais.

Por outro lado, a ligação estabelecida entre usuário e chave de assinatura contribui para dar maior praticidade e aceitabilidade do sistema, tornando transparente para o usuário o uso da sua chave privada. Porém, é importante perceber que o documento tradicional revela um tipo de ligação mais consistente do que essa. Ao observar os documentos físicos, é possível notar que a pessoa efetivamente deixa no papel algo de si através da assinatura manuscrita, ou seja, ficam agregados no documento elementos constitutivos da gênese gráfica do indivíduo, como a pressão e a direção do traço.

A gênese gráfica é a sucessão de movimentos determinados pelos impulsos cerebrais, que dão origem à forma. A gênese gráfica, portanto, é a materialização dos impulsos que emanam do centro nervoso da escrita. Por isso, é o elemento dinâmico e, por conseqüência, específico e inerente a cada indivíduo. Os movimentos possuem as seguintes características: início, projeção, intensidade ou pressão, aceleração, direção ou alinhamento gráfico, duração e cessação. A partir dessas características, é possível a realização de análises e perícias, ou seja, há a possibilidade de estimar, por exemplo, o estado emocional da pessoa através da assinatura manuscrita em um documento físico [TOC 95].

O mesmo não acontece com o documento eletrônico, pois é uma chave criptográfica que age diretamente sobre o texto, e não uma a firma biométrica. Essa firma simplesmente alavanca o procedimento de assinatura, não agregando informação biométrica ao documento eletrônico, ao contrário do ”mundo do papel”, onde a informação biométrica é agregada ao documento físico. Essa característica de segurança do docu-

mento físico é bastante relevante e não é detectada no documento digital.

Outro ponto merecedor de atenção quando da análise da segurança dos documentos digitais é a questão da visualização do documento durante a sua assinatura. No paradigma físico, a pessoa tem acesso direto ao papel, podendo vê-lo e tocá-lo, enquanto que no paradigma eletrônico é necessário a intervenção de um programa de computador para que se tenha acesso ao documento, visualizando-o. Na Subseção 5.4.1, considerou-se a possibilidade do funcionamento de forma maliciosa dos programas que atuam na montagem do documento digital e visualização do documento eletrônico. Esses *softwares* podem agir de maneira incorreta levando o usuário, inclusive, a assinar um documento que não estava predisposto a assinar.

É válido investigar a viabilidade de uso de outros tipos de identificação biométrica no processo de assinatura digital de documentos eletrônicos. Tanto assinatura manuscrita quanto a impressão digital não garantem que a pessoa tomou ciência do conteúdo do documento, seja ele eletrônico ou físico. Nesse sentido, a voz humana é uma alternativa bastante interessante. Por exemplo, o usuário poderia ler um trecho do documento. Isso poderia contribuir para uma associação o mais direta entre a pessoa e o documento eletrônico assinado, além de assegurar que o usuário tomou ciência, pelo menos em parte, do seu conteúdo.

5.5 Sistema Desenvolvido

Nesta seção, é apresentado o protótipo de um sistema computacional desenvolvido a fim de mostrar a viabilidade de realizar assinatura digital usando autenticação de usuário via impressão digital.

Na Subseção 5.5.1, são apresentados os aspectos gerais do sistema desenvolvido e os módulos que o compõe. Na Subseção 5.5.2, é explicada a interface do sistema. Na Subseção 5.5.3, discute-se o módulo biométrico. Na Subseção 5.5.4, é mostrado o módulo criptográfico. Na Subseção 5.5.5, apresenta-se os passos realizados pelo sistema para a geração da assinatura digital.

5.5.1 Aspectos Gerais

Devido à impossibilidade de acesso ao cartão inteligente com $scanner$ embutido que foi apresentado na Seção 4.3, fez-se necessária a emulação do mesmo. Assim, foi criado um *software* que assina um documento a partir da impressão digital do usuário. Para tanto, utilizaram-se a $CryptoAPI$[MIC 02b], biblioteca disponibilizada pela Microsoft junto ao Windows para o trato com criptografia e certificados digitais, e a $SecuAPI$, biblioteca utilizada com a finalidade de gerenciar padrões biométricos. Além disso, contou-se com um sensor óptico marca $SecuGen$.

A linguagem de programação escolhida para o desenvolvimento do sistema foi Visual C++, por mostrar-se compatível e amigável com as duas bibliotecas utilizadas, as quais oferecem interfaces para a referida linguagem de programação.

O sistema desenvolvido baseia-se em três módulos fundamentais:

- **Módulo Interface** - Responsável pela interação entre os módulos Biométrico e Criptográfico e pela emulação do cartão inteligente
- **Módulo Biométrico** - Parte responsável pela captação e a verificação do modelo biométrico ou *template*
- **Módulo Criptográfico** - Responsável pela assinatura digital

A seguir, discorre-se sobre cada um desses módulos.

5.5.2 Módulo Interface

O módulo interface é responsável pela união e interação entre o módulo criptográfico e o biométrico. Não obstante, também é sua função o relacionamento com o usuário e a emulação do cartão inteligente. A interface principal do *software* foi projetada de maneira a ser bastante intuitiva, facilitando o seu uso. Ela é mostrada na Figura 5.8, estando dividida nas três seções seguintes:

- *Informações Biométricas* - Área na qual é possível que o usuário configure o sistema biométrico, definindo, por exemplo, sua sensibilidade, além de ativar o leitor de

impressão digital para que possa ser usado.

- *Cadastro* - Nesta seção o usuário irá cadastrar a senha e suas impressões digitais, podendo cadastrar qualquer dedo da mão.
- *Cartão Inteligente* - Seção na qual o usuário irá identificar-se e selecionará um documento a ser assinado.

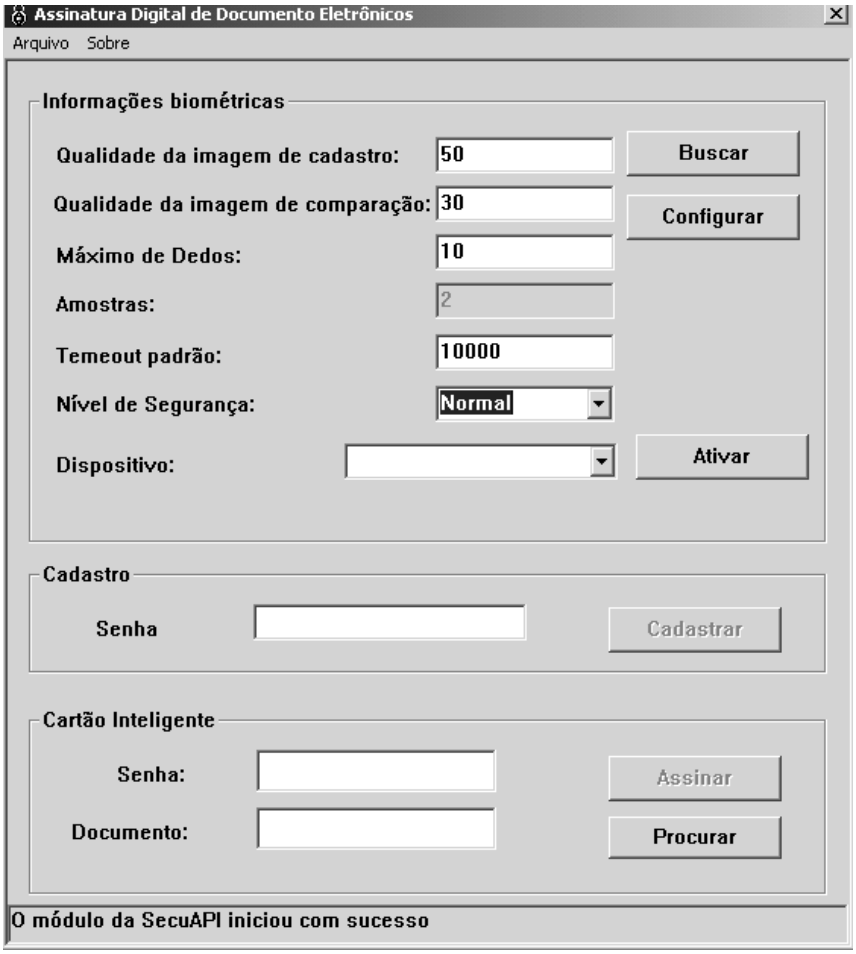


Figura 5.8: Tela principal do programa de assinatura de documentos eletrônicos através da impressão digital.

Dentre as informações biométricas que podem ser configuradas através da interface, estão as seguintes:

- Qualidade da imagem de cadastro, que pode variar de 0 a 100, e a de comparação, que pode variar de 0 a 100. A qualidade de cadastro é a qualidade da imagem

quando de seu registro. O valor inicial é 50. Conforme o valor aumentar, a qualidade de imagem melhorará. Assim, enquanto a imagem colhida pelo *scanner* não atingir o nível de qualidade preestabelecido, o dispositivo continuará a colher amostras até que os padrões mínimos de qualidade sejam atingidos.

- O número máximo de dedos que poderão ser cadastrados e conseqüentemente reconhecidos pelo sistema posteriormente.
- O número de amostras de impressão digital coletadas por dedo, que pode variar de 1 a 2.
- O tempo de espera ou *timeout* padrão, que é dado em milésimos de segundo para capturar a imagem da impressão digital através do dispositivo, sendo o valor inicial igual a 10000, que corresponde a 10 Segundos.
- O nível de segurança do sistema pode ser ajustado variando entre 1 e 9, tendo como valor inicial 5. Para cada valor numérico foi atribuído um termo. O nível 5 é o ”normal”, conforme aparece na Figura 5.8. Conforme o valor do nível aumentar, a taxa de falsa rejeição aumentará e a taxa de falsa aceitação diminuirá [SEC 00]. Essas taxas foram discutidas na Subseção 2.2.3.

Na tela principal do sistema, mostrada na Figura 5.8, pode-se notar a presença de alguns botões, os quais são explicados a seguir:

- O botão *Buscar* serve para buscar os valores padrões das informações biométricas.
- O botão *Configurar* aplica eventuais mudanças que o usuário faça em qualquer um dos valores das informações biométricas.
- O botão *Ativar* é usado para que o sistema verifique a existência do sensor biométrico e habilite o seu uso.
- O botão *Cadastrar* é utilizado no cadastro de um senha pelo usuário, além do cadastro de uma ou mais impressões digitais que serão usadas como modelo para posteriores autenticações da identidade do usuário.

- O botão *Assinar* é usado para gerar o código de assinatura a partir do documento que será selecionado através do botão *Procurar*. Antes de gerar a assinatura digital, o sistema requisita que o usuário entre com a senha e a impressão digital que será confrontada com o modelo previamente cadastrado.

- O botão *Procurar* serve para selecionar o documento eletrônico que será assinado.

Quando um usuário é cadastrado, ele deve fornecer uma senha e o seu padrão biométrico, ou seja, suas impressões digitais. A interface comunica-se com o módulo biométrico, como pode ser visto na Figura 5.11, utilizando funções específicas, e cria um registro desse usuário. Esse registro será usado para realizar a autenticação.

Caso fosse usado um *smart card*, esta etapa de cadastro de senha e padrão biométrico também deveria ser realizada durante a configuração do cartão para um determinado usuário. Assim, seria inserido no cartão inteligente o padrão biométrico formado por uma ou mais impressões digitais e senha do usuário.

Para o usuário assinar um determinado documento é preciso que um arquivo seja selecionado e que a autenticação, através da impressão digital e de uma senha, ocorra com sucesso. Se a autenticação for positiva, o *software* fará o resumo do documento e o cifrará com a chave privada padrão do usuário.

Realizando uma analogia com um sistema com *smart card* real, esta etapa corresponde à autenticação do usuário através da senha e do padrão biométrico. Se o resultado da autenticação for positivo, ou seja, a senha e o padrão biométrico coincidirem, o cartão inteligente receberá o resumo do documento a ser assinado e o devolverá cifrado com a chave privada, ou seja, assinado.

5.5.3 Módulo Biométrico

A principal função do módulo biométrico é fazer a ligação entre o *software* e a $SecuAPI$ de maneira mais amigável. O acesso a essa API é feito através de bibliotecas, como pode ser visto na Figura 5.9.

A $SecuAPI$ baseia-se em um provedor de serviços biométricos, ou seja, o BSP (*Biometric Service Provider*). Este provedor oferece funções para cap-

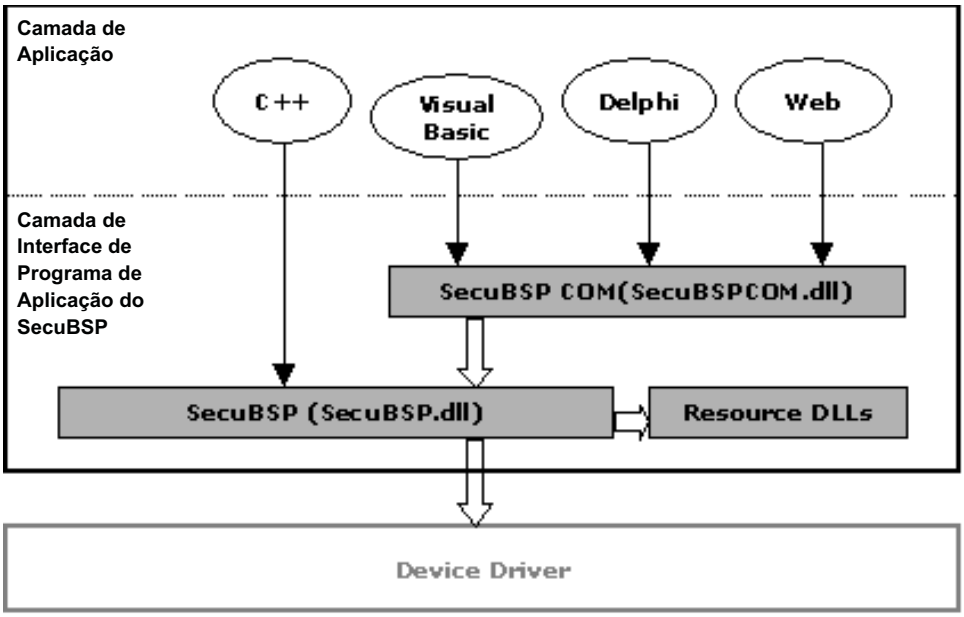


Figura 5.9: Modelo de desenvolvimento utilizando a SecuAPI.

turar, extrair, comparar e combinar imagens de impressão digital. Uma ilustração da comparação de impressões digitais pode ser vista na Figura 5.10.

As funções do BSP dividem-se nas três categorias seguintes:

- *Funções de Dispositivo* - Listam e acessam dispositivos existentes.
- *Funções de Captura* - Obtém uma impressão digital do sensor e extrai seus pontos característicos gerando o FIR (*Fingerprint Identification Record*), que é um registro de identificação da impressão digital, equivalente ao *template*, ainda chamado de ”modelo biométrico”.
- *Funções de Processamento* - Realizam a comparação entre os padrões biométricos.

As funções de dispositivo gerenciam os *scanners* de impressões digitais existentes no computador, sendo que, no máximo, podem existir 254 dispositivos. Essas funções realizam a ligação entre o dispositivo físico e sua parte lógica, facilitando o desenvolvimento de aplicações.

As funções responsáveis pela captura obtêm a imagem de uma impressão digital com definição de 500 dpi, em 256 tons de cinza. Essa imagem é trabalhada

e seus pontos característicos, ou minúcias, são extraídos. A partir desse ponto, o padrão biométrico dessa impressão digital já foi extraído, o que possibilita sua armazenagem em um banco de dados, seu envio pela Internet ou, até mesmo, que seja inserido em um cartão inteligente.

As funções de processamento são as mais importantes da $SecuAPI$, pois são responsáveis pela comparação entre dois padrões biométricos. Essas funções levam em conta o nível de segurança exigido pelo usuário, pois quanto maior for a segurança, maior será o número de pontos característicos exigidos pelo sistema para que uma comparação seja considerada positiva. Um exemplo da função de comparação pode ser visto na Figura 5.10, que ilustra a interface de comparação do *software*.

É importante salintar que a versão disponibilizada do $SecuAPI$ não possibilita o confronto 1:N [SEC 00].

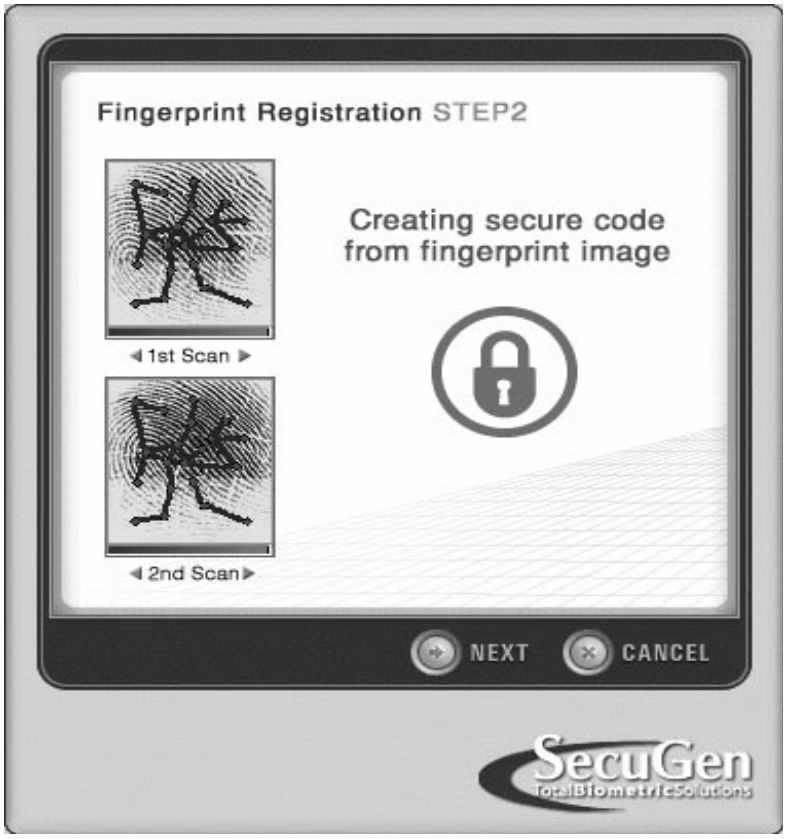


Figura 5.10: Interface de comparação de impressões digitais da SecuAPI.

5.5.4 Módulo Criptográfico

O módulo criptográfico é responsável por todas as funções relacionadas à criptografia do *software*. Ele serve como uma interface mais amigável à $CryptoAPI$, facilitando o acesso aos Provedores de Serviços Criptográficos ou CSPs (*Cryptographic Service Providers*) e utilizando funções para obter resumos e cifrar documentos.

Ao projetar este módulo, objetivou-se torná-lo o mais simples e independente possível, o que facilitaria sua utilização para trabalhos futuros. Objetivando manter um alto grau de compatibilidade, decidiu-se que o módulo criptográfico basear-se-ia em um CSP presente em todas as versões de Windows. O CSP escolhido denomina-se MY e é do tipo Servidor de Serviços Criptográficos Básicos. Por padrão da Microsoft, todo usuário possui este CSP. É importante lembrar que por medida de segurança, as chaves privadas são mantidas dentro dos CSPs, em depósitos de chaves. A única maneira de utilizá-las é através das funções do CSP.

De acordo com a interface deste módulo, para que a assinatura de um documento seja criada é necessário que ele receba um seqüência de bits, que representam o documento. A partir dessa seqüência de bits, cria-se o resumo do documento utilizando o algoritmo MD5. Após a criação do resumo, utiliza-se a chave privada armazenada na área de armazenamento de certificado do usuário corrente, MY, para assiná-lo e devolvê-lo. É importante lembrar que o MY/CSP só utiliza chaves do tipo RSA.

5.5.5 Procedimento Para Assinatura Digital

Descreve-se nesta seção os passos seguidos pelo *software*, desde o cadastramento até a assinatura de um documento eletrônico. Veja os passos descritos abaixo, ilustrados pela numeração na Figura 5.11:

1. Em um primeiro momento, o sistema biométrico deve ser configurado. Informações como a sensibilidade do sensor e qual o dispositivo a ser utilizado devem ser fornecidas. Em seguida, o usuário deve cadastrar suas impressões digitais e uma senha.

2. Após o usuário fornecer suas impressões digitais, o *software* utilizará o módulo

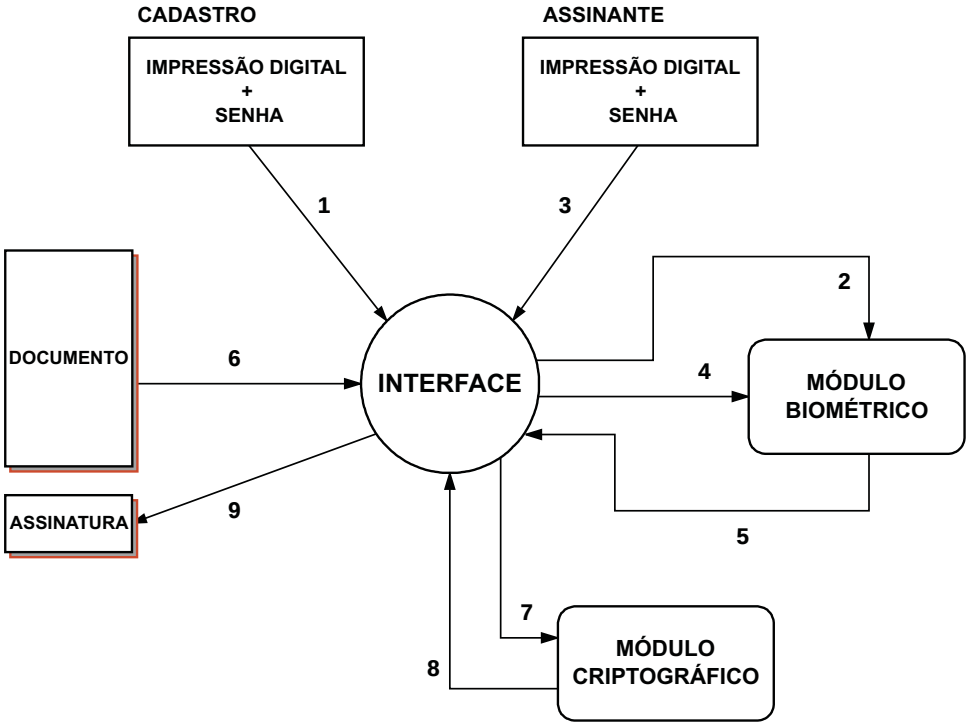


Figura 5.11: Passos realizados pelo *software* desde o cadastramento até a criação da assinatura digital.

biométrico, gerando o padrão biométrico do usuário que será utilizado em futuras comparações.

3. Neste passo o usuário deseja assinar um documento. Para isso, é necessário que ele escolha um documento e que forneça uma impressão digital e uma senha cadastrada.

4. Se a senha for a correta, o sistema enviará a impressão digital ao módulo biométrico e efetuará a comparação com o padrão biométrico já cadastrado.

5. O Módulo Biométrico retorna o resultado da comparação.

6. Se a impressão digital pertencer à pessoa cadastrada, o *software* lê o documento selecionado pelo usuário.

7. No módulo criptográfico, é feito o resumo deste documento. Este resumo é cifrado com a chave privada do usuário contida no MY/CSP.

8. A assinatura digital do documento é enviada à interface.

9. A interface cria um arquivo com extensão **”.sig”**. Este arquivo terá o mesmo nome do arquivo lido.

5.6 Conclusão

Neste capítulo, discutiu-se um modelo para assinatura digital de documentos envolvendo criptografia assimétrica, *smart cards* e a impressão digital do usuário, entre outros mecanismos. É importante observar que esse modelo foi projetado para interagir dentro de um ambiente de Infra-estrutura de Chaves Públicas. A segurança desses ambientes está diretamente relacionada à segurança das chaves privadas. Garantir que as mesmas sejam usadas somente pelos seus proprietários é um desafio que se propõe neste capítulo. De outra forma, permitir que a pessoa assine um documento eletrônico usando ”algo de seu” ajuda a diminuir a impessoalidade e a distância entre ser humano e computador, especialmente no caso da assinatura digital de documentos eletrônicos.

Existem alguns aspectos importantes sobre a montagem do documento eletrônico que devem ser considerados em um sistema de assinatura digital. Embora o código de assinatura seja gerado no interior do *smart card*, faz-se necessário subsistemas de suporte à assinatura do documento digital. Igualmente, refletiu-se sobre a confiança depositada nesses subsistemas, alertando para a possibilidade de fraude no momento da montagem do documento eletrônico.

Por fim, foi apresentado neste capítulo um sistema desenvolvido para a assinatura digital de documentos eletrônicos onde se realizou a autenticação de usuário via impressão digital. As tecnologias utilizadas para a construção do sistema foram a $CryptoAPI$e a $SecuAPI$. Com isso, demonstrou-se a viabilidade técnica do trabalho.

Capítulo 6

Boletim de Ocorrência Policial

Neste capítulo é apresentado um sistema proposto com a finalidade de mostrar uma aplicação prática da assinatura digital de documentos eletrônicos através da impressão digital. Para tanto, foi escolhido o Boletim de Ocorrência (BO) pelo importante papel que ocupa no dia-a-dia de uma Delegacia de Polícia. As informações contidas no BO são muito úteis para que a autoridade policial tome providências para esclarecer os fatos. Daí a importância de oferecer um forma segura e fácil de registro de ocorrências que leve o cidadão a efetiva comunicação de crimes a Polícia.

Na Seção 6.1, discutem-se os três sistemas de registro de BO existentes na Polícia Civil catarinense. Logo após, na Seção 6.2, é apresentado o Boletim de Ocorrência proposto que visa à universalização do registro de ocorrências policiais, como forma do cidadão ter acesso ao registro de ocorrências de modo fácil e seguro, quando comparado aos sistemas de registro atuais. Na Seção 6.3, concluí-se este capítulo.

6.1 Sistemas de Boletins de Ocorrência

O Boletim de Ocorrência é uma das formas pelas quais a Polícia Civil pode tomar ciência de um fato que a lei declara como punível. Com efeito, a notícia de crime pode chegar até ela através de requisições judiciais, representações, requisições de promotores de justiça, comunicação escrita pelo ofendido e requerimento [THO 97]. No

entanto, conforme se constata no cotidiano, nenhum desses tipos é mais freqüente que o registro de Boletim de Ocorrência, o qual tem se consolidado como a forma mais comum de informar à Polícia fatos delituosos.

Atualmente, existem três sistemas para registro de ocorrências policiais disponibilizados pela SSP/SC:

- BO Tradicional, apresentado na Subseção 6.1.1.
- BO Eletrônico via Intranet da SSP, tratado na Subseção 6.1.2.
- BO Eletrônico via Internet, abordado na Subseção 6.1.3.

6.1.1 Boletim de Ocorrência Tradicional

A Polícia Civil catarinense tem utilizado formulários para realizar o registro de ocorrências no Estado. Assim, de acordo com o tipo da ocorrência, existe um formulário apropriado para o seu registro. O tipo de formulário mais utilizado é o Boletim de Ocorrência Diversa, mostrado na Figura 6.3 e utilizado para o registro da maioria dos delitos existentes: homicídio, furto, roubo, ameaça etc. Além desse tipo, existem o Boletim de Perda de Documentos e Objetos, Boletim de Acidente de Trânsito, Boletim de Furto/Roubo de Veículo e o Boletim de Recuperação e Devolução de Veículo. Apesar desses formulários seguirem uma estrutura parecida, cada um guarda suas peculiaridades. Por exemplo, o BO de Acidente de Trânsito tem o campo ”Carteira Nacional de Habilitação”, o qual não aparece nos outros tipos de ocorrências.

No BO são arroladas todas as pessoas envolvidas, as circunstâncias, entre outras informações relevantes sobre o fato ocorrido. As informações prestadas durante o registro servirão de base para o início da investigação policial. A Figura 6.1 ilustra os possíveis participantes de um BO. Considerando o Boletim de Ocorrência apresentado na Figura 6.3, podemos especificar as seguintes pessoas relacionadas com o registro do fato noticiado: policiais, testemunhas, comunicante, acusado e vítima. É importante destacar que para o preenchimento do BO não é necessário que todas essas pessoas sejam arroladas. Muitas vezes, a identidade das pessoas envolvidas no fato delituoso fica a cargo da

própria investigação que será desenvolvida a partir do registro, como é o caso do acusado que geralmente não é conhecido quando da comunicação do fato. O BO é devidamente assinado pelo comunicante do fato e policiais, ou seja, o policial responsável pelo registro da ocorrência e o Delegado de Polícia.

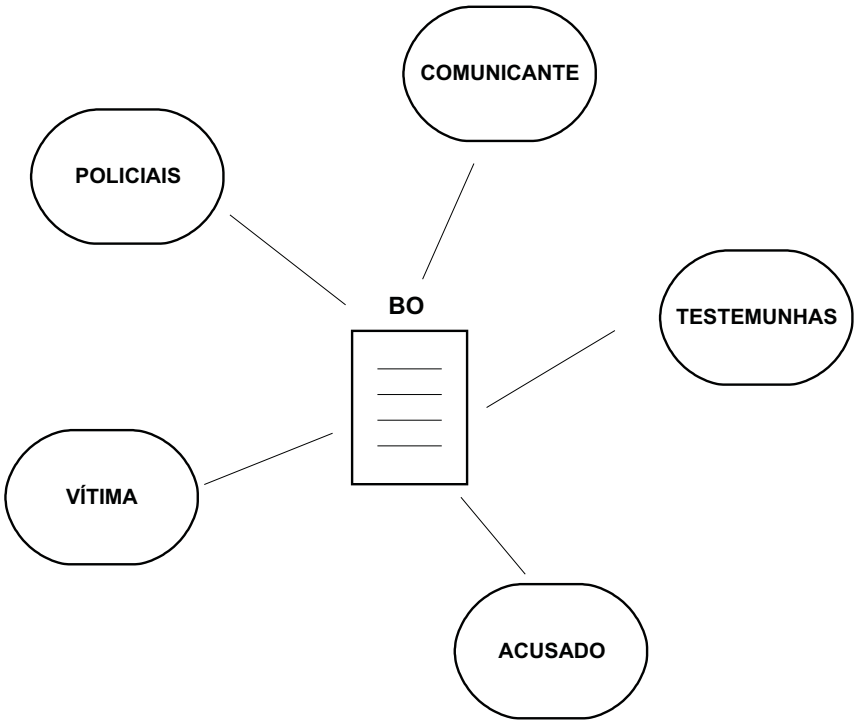


Figura 6.1: Possíveis participantes de um Boletim de Ocorrência.

O preenchimento do Boletim de Ocorrência deve responder à *"seis perguntas elementares da investigação policial"*, a saber [THO 97]:

- O quê?
- Quando?
- Como?
- Onde?
- Por quê?
- Quem Viu?

A autoridade policial contará com o Boletim de Ocorrência para tomar as primeiras providências no sentido da investigação dos fatos. Portanto, a elaboração do BO deve ser conduzida de maneira a responder de maneira clara e concisa esses seis questionamentos, evitando-se redundância de informações e salientando os detalhes do fato que podem levar a Polícia à elucidação do crime.

É importante perceber que as perguntas elementares ”Como?” e ”Por quê?”, de acordo com o formulário da Figura 6.3, devem ser descritas no campo **Histórico**. Um problema relacionado ao preenchimento desse campo é a sua subjetividade, podendo ser preenchido de maneira a não esclarecer o ”Como?” e o ”Por quê?” dos fatos.

6.1.2 Boletim de Ocorrência Eletrônico Via Intranet

Essa modalidade de registro de ocorrências tem sido apresentada em substituição ao BO tradicional que foi apresentado na Subseção 6.1.1.

A Secretaria da Segurança Pública de Santa Catarina - SSP/SC está implantando um sistema para registro de ocorrências no âmbito da rede interna da Polícia - *Intra@SSP*. Na verdade, mais do que automatizar o processo de confecção do BO, a SSP/SC deseja controlar por computador a maioria dos procedimentos realizados em uma Delegacia de Polícia, como os Inquéritos Policiais, Termos Circunstanciados, Perícias, Exames etc. [CIA 02]. Este tipo de BO só pode ser registrado por policial, assim como o BO tradicional. Desse modo, o comunicante de um fato terá que dirigir-se até uma Delegacia de Polícia, onde poderá ser feita a notícia de crime.

A segurança de uma rede Intranet fica restrita, a princípio, ao uso de *firewalls*, a saber, filtro entre uma rede local e a Internet por meio do qual só passa tráfego autorizado. No entanto, não é tratada com maior profundidade a questão da autenticação, integridade, confidencialidade e não-repúdio das informações [STA 99].

6.1.3 Boletim de Ocorrência Eletrônico Via Internet

É o único que pode ser usado pelo cidadão, sendo efetivamente preenchido pela pessoa. Na Tabela 6.1, são mostradas as pessoas que preenchem os BOs

conforme o sistema de registro utilizado.

No sítio da SSP/SC [dSC 02], é disponibilizado o serviço "*Boletim de Ocorrência Cidadão*", que possibilita o registro de ocorrências policiais pela Internet. Porém, o tipo de ocorrência que o cidadão pode registrar limita-se à Perda de Documentos, Perda de Objetos e denúncias.

Tabela 6.1: Pessoas responsáveis pelo registro de ocorrência de acordo com o sistema de Boletim de Ocorrência utilizado.

Sistema de Boletim de Ocorrência	**Quem Preenche o Formulário**
1. BO Tradicional	Policial Civil
2. BO Eletrônico na Intranet	Policial Civil
3. BO Eletrônico na Internet	O Próprio Cidadão

Fonte: SSP/SC.

Ao fim do registro, o comunicante é alertado de que um policial entrará em contato com ele através do telefone fornecido durante o registro da ocorrência. Desta forma, é feita a validação das informações prestadas durante o registro.

É importante destacar que o sistema de registro em questão não oferece outros mecanismos que permitam validá-lo de forma a verificar a autenticidade e integridade das informações digitadas pelo usuário.

6.2 Boletim de Ocorrência Eletrônico Seguro

O Boletim de Ocorrência Eletrônico Seguro - $BOES$ é a proposta de um sistema voltado para o registro de ocorrências policiais através da Internet. Existem três aspectos fundamentais em relação a ele:

- **Universalização do registro de BOs** - Pretende-se tornar acessível os vários tipos de registro de ocorrências policiais ao cidadão através da Internet.

- **Segurança da informação** - O BO seguro leva em consideração assuntos consagrados no campo da segurança em computação, como as assinaturas digitais e sistemas biométricos, para estabelecer a identidade de pessoas, computadores etc., proporcionando maior credibilidade ao processo de registro de ocorrências remoto.

- **Popularização do uso do BO** - Popularizar o uso do Boletim de Ocorrência como mecanismo de comunicação de delitos em geral.

6.2.1 Protocolo Para Registro de Ocorrência

Considerando a arquitetura Cliente/Servidor, os passos a serem seguidos para o registro de ocorrências dentro do modelo proposto são os seguintes:

1. O CLIENTE ACESSA O SERVIDOR SEGURO - O usuário acessa o sítio do servidor seguro através do seu navegador de Internet. Nesse momento, é criado um ”canal de comunicação seguro” entre o computador do cliente e do servidor, onde o sigilo das comunicações e a autenticação do servidor ficam garantidas.

2. SERVIDOR REQUER AUTENTICAÇÃO DE CLIENTE - O servidor requer a identidade digital do usuário, o seu certificado digital. Algumas políticas poderiam ser adotadas no caso do usuário não possuir uma identidade digital, a saber:

   - A primeira alternativa seria a Polícia emitir um certificado digital com um pequeno período de validade para a pessoa.
   - Outra hipótese é do usuário ser tratado como anônimo. Logo após o registro da ocorrência, um policial pode ligar para o telefone fornecido no preenchimento do formulário a fim de verificar os dados prestados pela pessoa. Esse procedimento já é adotado por algumas secretarias estaduais de segurança, que oferecem ao cidadão o serviço de registro de ocorências pela Internet, como é o caso da SSP/SC [dSC 02] e da SSP/SP [MIC 02a].

3. PREENCHIMENTO DE FORMULÁRIOS WEB NO CLIENTE, ASSINATURA DOS DADOS E ENVIO AO SERVIDOR DE APLICAÇÃO - O usuário assina os dados prestados

nos formulários de ocorrência. O processo de assinatura ocorre na máquina cliente. Na verdade, para que o sistema se torne exeqüível, deve-se estabelecer as seguintes formas de acesso ao sistema e à identificação de usuário em cada caso:

- *Direto:*
  - Acesso através de Quiosques - Locais de acesso público onde a pessoa pode efetuar o registro de ocorrências policias através de computadores específicos que permitam identificação através de impressão digital e foto do usuário. O registro realizado em quiosques deve também possibilitar a operação com certificados digitais.
  - Acesso através de Computador Particular - Nesse caso, o usuário poderá identificar-se através de certificados digitais, assinando digitalmente os dados. A autenticação via impressão digital deve ser possível, caso o usuário possua um leitor de impressão digital.
- *Indireto:*
  - Acesso por Telefone - O comunicante liga para uma central de atendimento telefônico e efetua o registro da ocorrência. Durante a ligação, os padrões da voz do comunicante são gravados junto com os demais dados do registro. Além disso, a possibilidade de assinatura do Boletim de Ocorrência através do reconhecimento da voz humana deve ser estudada.

4. DADOS ASSINADOS SÃO RECEBIDOS PELO SERVIDOR - Nesta etapa, o servidor verifica a assinatura do usuário, conferindo a autenticidade e integridade dos dados que foram assinados digitalmente.

5. O SERVIDOR DE APLICAÇÃO ARMAZENA OS DADOS DO BO E ASSINATURA EM UMA BASE DE DADOS - As informações prestadas no registro e a assinatura são armazenadas em uma base de dados da Polícia.

6. SERVIDOR DE APLICAÇÃO GERA UM RECIBO ASSINADO E O ENVIA AO USUÁRIO - O recibo contém informações como o Número de Protocolo, Nome do Comunicante, Data/Hora, além de informações dizendo que o BO foi efetivamente recebido

pela Polícia. O número de protocolo poderá ser usado para que a pessoa acesse seu Boletim de Ocorrência através da Internet, imprimindo-o se desejar. Tal recibo, que é assinado digitalmente pelo servidor de aplicação e datado por uma autoridade de datação [PAS 01], serve como prova de que a pessoa efetuou o registro da ocorrência junto à Polícia. Na Figura 6.2, é ilustrada a estrutura do recibo, considerando sua autenticidade, integridade e tempestividade. Nesse sentido, uma aplicação sendo executada do lado do servidor assina o recibo que é também devidamente datado por uma Protocoladora Digital de Documentos Eletrônicos - PDDE[1] [PAS 01]. A fim de que o recibo seja auto-verificável, o certificado digital do servidor de aplicação é juntado à estrutura do recibo. Por fim, este último é enviado ao comunicante do fato à Polícia.

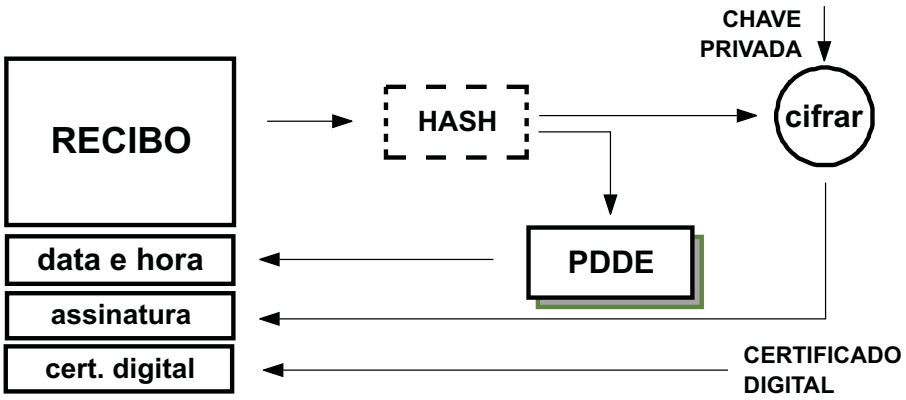


Figura 6.2: Estrutura do recibo com validade jurídica.

7. CONTROLE E AUDITORIA DE BOLETINS DE OCORRÊNCIA - Um policial recebe as ocorrências e faz análise das mesmas. Na verdade, ele irá analisar a coerência e veracidade das informações prestadas durante o seu registro. Pretende-se classificar os BOs em válidos, isto é, aceitos pela Polícia, e inválidos, ou seja, desconsiderados em função de mau preenchimento, como os que se configuram em trotes. Esse último tipo de Boletim de Ocorrência receberá tratamento especial, para que a Polícia procure identificar e punir as pessoas responsáveis pela falsa comunicação

[1]A empresa BRy Tecnologia S.A., *http://www.bry.com.br*, desenvolveu a PDDE em parceria com a UFSC em Santa Catarina.

de crime. Já os BOs válidos receberão atenção da Polícia, sendo adicionados em uma base de dados confiável para a realização de estatísticas de crimes, além de poderem dar início às investigações dos crimes relatados.

6.2.2 Benefícios do *BOES*

O Boletim de Ocorrência Eletrônico Seguro contribui para a melhoria no processo de registro de ocorrências policiais de acordo com os seguintes itens:

- **Agilidade** - A possibilidade do auto-atendimento através da Internet torna mais rápido o registro de ocorrências para o cidadão, reduzindo, por exemplo, as filas em delegacias. Nos registros efetuados de casa, o comunicante o faz imediatamente. Já naqueles registros efetuados nos quiosques, o esperado é que as filas sejam, no mínimo, menores do que em uma Delegacia de Polícia. Isso dependerá do número de quiosques existentes em uma cidade e da quantidade de terminais disponibilizados nos mesmos.

- **Custo Reduzido e Ênfase à Investigação** - Por um lado, tem-se o custo reduzido para a população, que poderá efetuar o registro de casa ou de um quiosque[2], não precisando deslocar-se até uma Delegacia de Polícia, que fica, muitas vezes, distante, para efetuar o registro. Por outro lado, uma ampla aceitação do sistema por parte da população propiciaria uma diminuição no fluxo de pessoas nas Delegacias. Esse aspecto é importante, pois o tempo dedicado pelo policial ao atendimento da comunidade poderia ser ocupado na investigação e elucidação dos crimes.

- **Formas de Acesso e Segurança** - O sistema prevê três maneiras para o usuário registrar a ocorrência, conforme apresentado na Subseção 6.2.1: por telefone, quiosque e computador particular. Na primeira possibilidade o registro é efetivamente digitado por uma policial, conforme relato do comunicante do fato. Nas demais alternativas é o próprio comunicante o responsável pelo preenchimento do BO. Em

[2]Pretende-se que existam vários quiosques para registro de ocorrências policiais localizados estrategicamente dentro das cidades.

qualquer uma das modalidades de acesso, o comunicante é identificado, seja através de uma informação biométrica sua, por assinatura digital ou ambas. Esse procedimento visa assegurar a autenticidade e integridade dos dados. Como o sistema em questão visa popularizar o uso do BO, as três formas de acesso já elencadas são essenciais, uma vez que se deve viabilizar a qualquer pessoa, independente de possuir computador pessoal ou não, a efetivação o registro.

- **Aumento da Notificação de Crimes** - É importante perceber que muitos crimes não são comunicados à Polícia. Vários fatores contribuem para isso. Um deles é o sentimento de ”perda de tempo” demonstrado por muitas pessoas em relação ao serviço policial, no sentido de que não será descoberta a autoria do crime, nem mesmo serão recuperados objetos outrora subtraídos da vítima. Outro fator diz respeito ao ambiente da Delegacia de Polícia, que pode ser considerado hostil por várias pessoas. Outro ainda, é o medo de represálias de criminosos. Enfim, essa fatia de crimes que, por um motivo ou outro, não são noticiados à Polícia corresponde às *cifras negras da criminalidade*. Para Andrade, a *cifra negra* corresponde *”a defasagem que medeia entre a criminalidade real, isto é, as condutas criminalizáveis efetivamente praticadas, e a criminalidade estatística oficialmente registrada”* [dA 97]. Desse modo, as estatísticas sobre a criminalidade, realizadas puramente a partir dos delitos comunicados ao órgão policial, acabam não refletindo os verdadeiros números acerca dos delitos ocorridos na sociedade. Com isso, pode-se notar que o problema da mensuração da criminalidade é mais profundo do que parece. Não obstante, à medida que a notificação de crimes aumenta, as *cifras negras da criminalidade* diminuem. Assim, a notificação de crimes deve ser impulsionada, seja pelo oferecimento de uma serviço policial de qualidade e de resultados, seja pelo oferecimento de serviços alternativos como o $BOES$. Esse sistema oferece uma forma fácil, segura e cômoda para que o cidadão efetue de registro de ocorrências.

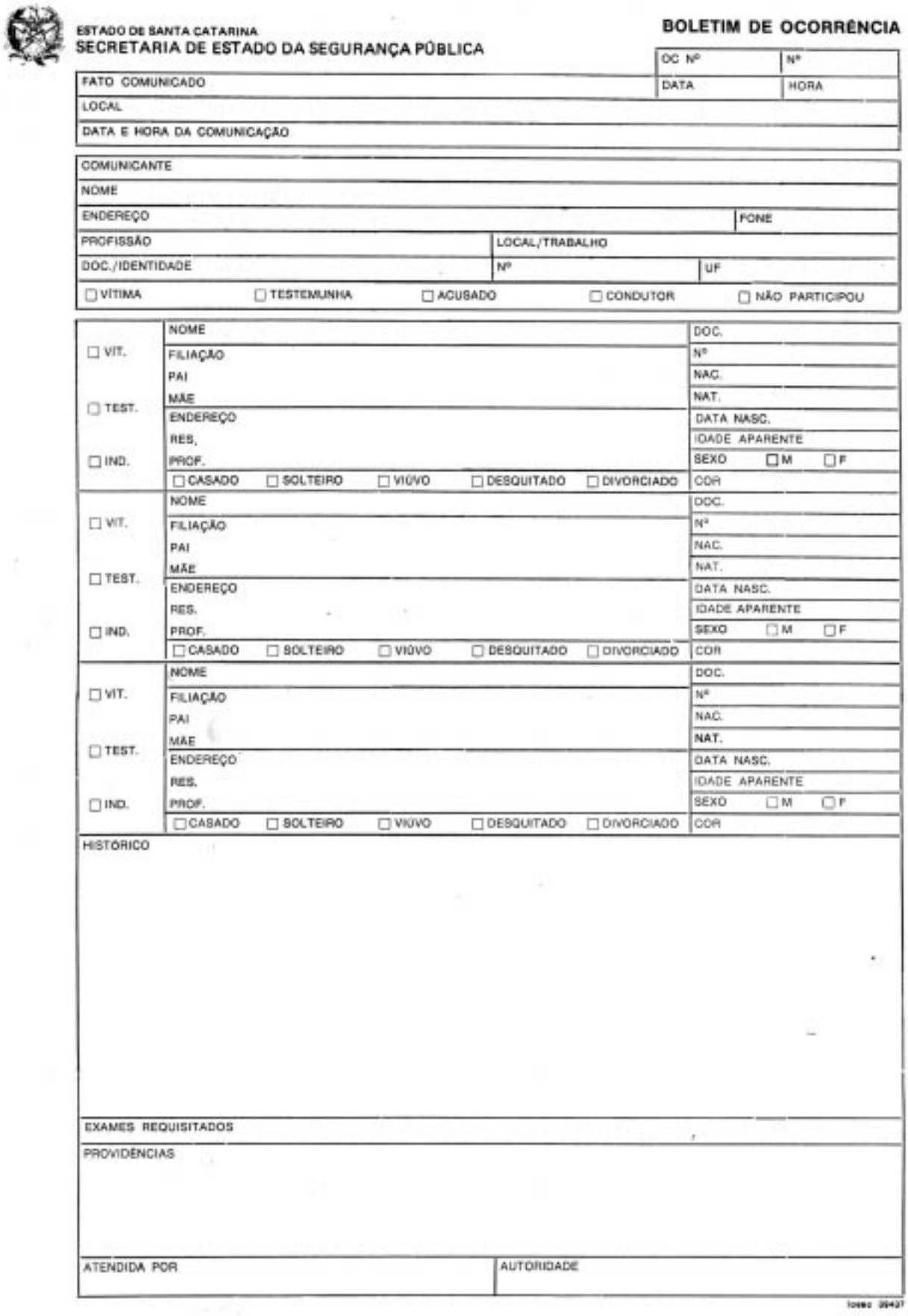
- **Rastreabilidade de Ocorrência de Delitos** - Maior facilidade na realização de estatísticas e consultas à base de dados do sistema e, em decorrência disso, possibilidade de melhor planejamento das ações policiais, otimizando a distribuição de

recursos para a prestação do serviço à comunidade. Como um exemplo dessas estatísticas, pode-se citar o seguinte: um grande mapa da cidade ou região poderia ser integrado ao $BOES$, alertando para o índice de crimes de forma dinâmica em cada localidade.

6.3 Conclusão

Neste capítulo, foram revisados os sistemas de registro de ocorrências usados pela Polícia Civil do Estado de Santa Catarina.

Por conseguinte, apresentou-se o Boletim de Ocorrência Eletrônico Seguro, onde o próprio cidadão poderá registrar uma ocorrência policial de sua casa ou através de locais de acesso público. Junto a isso, foi colocado sob enfoque os benefícios proporcionados pelo sistema: Agilidade, Custo Reduzido e Ênfase à investigação, Formas de Acesso e Segurança, Aumento da Notificação de Crimes e Rastreabilidade da Ocorrência de Delitos.



ESTADO DE SANTA CATARINA
SECRETARIA DE ESTADO DA SEGURANÇA PÚBLICA

BOLETIM DE OCORRÊNCIA

OC Nº	Nº	
FATO COMUNICADO	DATA	HORA
LOCAL		
DATA E HORA DA COMUNICAÇÃO		

COMUNICANTE				
NOME				
ENDEREÇO				FONE
PROFISSÃO		LOCAL/TRABALHO		
DOC./IDENTIDADE		Nº		UF

☐ VÍTIMA ☐ TESTEMUNHA ☐ ACUSADO ☐ CONDUTOR ☐ NÃO PARTICIPOU

☐ VIT.	NOME	DOC.
	FILIAÇÃO	Nº
	PAI	NAC.
☐ TEST.	MÃE	NAT.
	ENDEREÇO	DATA NASC.
	RES.	IDADE APARENTE
☐ IND.	PROF.	SEXO ☐ M ☐ F
	☐ CASADO ☐ SOLTEIRO ☐ VIÚVO ☐ DESQUITADO ☐ DIVORCIADO	COR

☐ VIT.	NOME	DOC.
	FILIAÇÃO	Nº
	PAI	NAC.
☐ TEST.	MÃE	NAT.
	ENDEREÇO	DATA NASC.
	RES.	IDADE APARENTE
☐ IND.	PROF.	SEXO ☐ M ☐ F
	☐ CASADO ☐ SOLTEIRO ☐ VIÚVO ☐ DESQUITADO ☐ DIVORCIADO	COR

☐ VIT.	NOME	DOC.
	FILIAÇÃO	Nº
	PAI	NAC.
☐ TEST.	MÃE	NAT.
	ENDEREÇO	DATA NASC.
	RES.	IDADE APARENTE
☐ IND.	PROF.	SEXO ☐ M ☐ F
	☐ CASADO ☐ SOLTEIRO ☐ VIÚVO ☐ DESQUITADO ☐ DIVORCIADO	COR

HISTÓRICO

EXAMES REQUISITADOS

PROVIDÊNCIAS

ATENDIDA POR	AUTORIDADE

Figura 6.3: Cópia de Boletim de Ocorrência da SSP/SC.

Capítulo 7

Considerações Finais

Neste capítulo, são feitas as considerações finais acerca deste trabalho de pesquisa. Na Seção 7.1, discute-se as conclusões obtidas a partir desta pesquisa. Na Seção 7.2, são apresentadas as contribuições deste trabalho. Na Seção 7.3, propõe-se algumas sugestões para trabalhos futuros.

7.1 Conclusões

A área de segurança em computação é vasta e há muito o que estudar a seu respeito. A cada dia surgem novas fraudes e formas de corromper os sistemas de informação. Pode-se constatar isso através dos vírus de computador, onde um novo tipo de vírus surge a todo instante, deflagrando uma verdadeira guerra entre os *softwares* anti-vírus e os vírus.

O objetivo principal desta dissertação traduziu-se em utilizar a impressão digital para autenticar a identidade do usuário no processo de realização da assinatura digital de documentos eletrônicos. Nesse sentido, foi proposto um modelo para assinatura de documentos eletrônicos que usa Infra-estrutura de chaves públicas, *smart cards* e impressão digital. Sistemas baseados nesses três elementos tem sido estudados e desenvolvidos por organizações e cientistas.

No modelo proposto neste trabalho, procurou-se aumentar a confiança

no processo de geração da assinatura digital dos documentos eletrônicos. Impressão digital, *smart card* e senhas, são formas de autenticar a identidade do usuário utilizadas a fim de garantir que a chave privada criptográfica possa ser usada somente por seu proprietário. Dentre essas formas de autenticação, a biometria merece destaque, por usar aspectos pessoais do indivíduo para identificá-lo. Com isso, mais do que proteger a chave de privada, a impressão digital fortalece a ligação entre a chave privada e seu proprietário. Ou seja, o uso da chave de assinatura torna-se transparente para o usuário, bastando, simplesmente, usar a sua polpa digital para assinar um documento digital. O uso dessa característica única e pessoal reúne simplicidade, conveniência e segurança, além de aperfeiçoar o processo de autenticação de pessoas em ambientes de assinatura digital.

Aspectos importantes revelados através da análise do modelo proposto e do protótipo desenvolvido podem ser notados a seguir:

- *Disponibilidade dos dados* - Os dados necessários para a realização da assinatura de um documento eletrônico permanecem dentro do *smart card*, podendo ser utilizados na assinatura de documentos a qualquer momento.

- *Armazenamento distribuído* - Cada usuário carrega consigo os seus dados particulares em um *smart card*, evitando a existência de grandes bases de dados com informações sobre usuários, como, por exemplo, *templates* de impressão digital. Além disso, elimina-se a necessidade de transmissão de dados via rede, onde eles poderão ser corrompidos ou alterados.

- *Alta proteção a ataques* - O código de assinatura é gerado no interior do cartão, utilizando dados particulares do usuário como chave privada e *template* de impressão digital, os quais ficam armazenados dentro do cartão. A autenticação da identidade do usuário ocorre dentro do cartão, incluindo o confronto entre *templates*. O usuário poderá assinar um documento eletrônico se souber uma senha, possuir o cartão e apresentar uma característica pessoal e única, no caso, a impressão digital.

Por outro lado, os possíveis ataques ao sistema proposto foram estudados. Um deles, tratado com detalhe no Apêndice A, revela a possibilidade de fraudes na

autenticação da identidade de usuários envolvendo o uso de dedos artificiais. Atualmente, existem tecnologias de sensores de impressão digital que previnem o ataque realizado com dedos artificiais.

Embora tenha sido possível criar um vínculo entre o usuário e sua chave privada através do modelo proposto, não foi possível estabelecer uma ligação direta do usuário com o documento eletrônico. Quando da comparação com o documento físico, esse tipo de ligação é possível, uma vez que são deixadas diretamente no papel características pessoais através da assinatura manuscrita da pessoa, como, por exemplo, a pressão exercida sobre o papel.

Uma situação de obtenção de assinatura digital mais segura, seria aquela em que o usuário pudesse deixar ”algo de si” no próprio documento. Na verdade, a implementação disso em documentos eletrônicos necessitaria de estudo mais profundo.

7.2 Contribuições do Trabalho

Organizações e cientistas tem buscado o aprimoramento dos sistemas de assinatura digital, conferindo especial atenção ao nível de confiança e credibilidade que tais sistemas podem oferecer. Em [Iso 01], nota-se a preocupação com a elaboração de sistemas seguros de autenticação de usuário, envolvendo Infra-estrutura de chaves públicas, *smart cards* e impressões digitais.

Nesse sentido também, um grupo de empresas nórdicas projetou e construiu um sistema para assinatura digital de documentos eletrônicos baseado em ICP, *smart cards* e impressões digitais. No sistema elaborado, existe um único dispositivo leitor, servindo tanto para a leitura do *smart card*, como para a leitura da impressão digital do usuário [HOJ 00].

Além do uso combinado com sistemas de assinatura digital, as impressões digitais tem sido usadas na autenticação de usuários de uma forma geral. Um exemplo disso é a disponibilização do serviço de *webmail* com autenticação de usuário via impressão digital, como aquele desenvolvido pela empresa Compuletra Ltda [COM 01]. Perceba-se que, neste caso específico, não houve uso da tecnologia de assinatura digital,

mas sim o simples uso de autenticação biométrica para acesso a conta de *e-mail*.

O modelo proposto nesta dissertação utiliza Infra-estrutura de chave pública, *smart card* e impressão digital para a criação de um ambiente onde se possa assinar documentos eletrônicos. Uma das maiores contribuições deste estudo emana do uso de um sensor de impressão digital embutido no próprio *smart card*, permitindo que todo o processo de autenticação da identidade do usuário e geração do código de assinatura ocorram no interior do cartão, inclusive a aquisição da imagem da impressão digital. Isso proporciona maior segurança e confiança no processo de assinatura de documentos, pois os dados particulares do usuário como impressão digital e chave privada serão manipulados somente no interior do cartão. O *smart card* com o sensor de impressão digital embutido foi apresentado na Seção 4.3.

Na prática, procurou-se aplicar o modelo proposto a uma situação do cotidiano social, ou seja, o registro de ocorrências policiais da Polícia Civil catarinense. Dessa forma, um sistema para assinatura de documentos eletrônicos poderia ser usado para tornar mais ágil e seguro o registro de ocorrências policiais através da Internet.

7.3 Sugestões para Trabalhos Futuros

O assunto desenvolvido nesta dissertação dá margem a outras pesquisas relacionadas à área, tanto nesta universidade quanto em outras instituições de ensino. A seguir, são relacionadas algumas sugestões julgadas pertinentes:

- Propor um esquema atrelado à padronização de *templates* de impressão digital para que os mesmos possam ser intercambiados entre sistemas de fabricantes diferentes.
- Estudar e pesquisar técnicas que não permitam a leitura de dedos artificiais na aquisição da imagem da impressão digital.
- Propor o uso desta forma de assinatura digital para a ICP-Brasil.
- Estudar sobre a possibilidade de usar os poros da pele para reconhecimento de impressões digitais.

- Investigar acerca do uso da voz humana como fonte biométrica para a assinatura de documentos digitais, por exemplo, para uso do sistema de Boletim de Ocorrência Eletrônico Seguro, descrito no Capítulo 6.

Referências Bibliográficas

[ALC 01] ALCÂNTARA, D. M. R. Identificação civil e criminal. **Impressões**, [S.l.], , n.10, p.49–55, Abril/Maio/Junho, 2001.

[ANT 02] ANTHEUS, S. C. T. **A Tecnologia ARID**. Disponível em <http://www.antheus.com.br/>. Acesso em: Janeiro, 2002.

[ASS 02] ASSOCIATES, B. **Fingerprint ID Module Technology for Smartcards**. Disponível em <http://www.biometricassociates.com/products.html>. Acesso em: Fevereiro, 2002.

[BAD 01] BADARÓ, G. H. R. I. **A Nova Regulamentação Da Identificação Criminal**. Disponível em <http://www.ibccrim.com.br/>. Acesso em: Setembro, 2001.

[BAL 01] BALIEIRO, S. A íris é a senha. **INFO Exame**, [S.l.], , n.189, p.110–111, Dezembro, 2001.

[BBC 02] BBCI. **Doubt Cast on Fingerprint Security**. Disponível em <http://news.bbc.co.uk/hi/english/sci/tech>. Acesso em: May, 2002.

[BIC 99] BICZ, W. et al. **Ultrasonic Setup For Fingerprint Patterns Detection and Evaluation**. Disponível em <http://www.optel.com.pl/>. Acesso em: April, 1999.

[BOR 02] BORTOLI, D. L. **O Documento Eletrônico No Ofício de Registro Civil de Pessoas Naturais**. Universidade Federal de Santa Catarina, Julho, 2002. Dissertação de Mestrado.

[BRA 94] BRASIL. **Constituição Da República Federativa Do Brasil : Promulgada Em 5 de Outubro de 1988**. 9. ed. São Paulo: Saraiva, 1994.

[BRA 02] BRASIL. **Medida Provisória N. 2.200-2, de 24.08.2001**. Disponível em <http://www.mct.gov.br>. Acesso em: Julho, 2002.

[Car 83] **Lei N7.116 de 29 de Agosto de 1983**.

[Car 00] Detran elimina fraudes com carteira 'digital'. **A tribuna do povo - Umuarama/PR**, [S.l.], 11, Junho, 2000.

[CHA 00] CHAPARRO, P. R. Digitalização eletrônica de documentos de identificação civil e criminal com preparação para o AFIS. Dezembro, 2000.

[CHA 01] CHAVES, A. L. F. AFIS - análise comparativa entre alguns sistemas. **Impressões**, [S.l.], , n.10, p.46–48, Abril/Maio/Junho, 2001.

[CIA 02] CIASC. **Atendimento Policial - Tutorial Para Ocorrência Diversa**. Centro de Informática e Automação Do Estado de Santa Catarina - CIASC, 2002.

[COM 01] COMPULETRA. **BioWeb**. Disponível em <http://www.bioweb.com.br>. Acesso em: Junho, 2001.

[CON 02] CONSORTIUM, B. **The Biometric Consortium**. Disponível em <http://www.biometrics.org/>. Acesso em: Janeiro, 2002.

[COR 99] CORCORAN, D.; SIMS, D.; HILLHOUSE, B. Smart cards and biometrics: The cool way to make secure transactions. **Linux Journal**, [S.l.], v.1999, n.59es, p.7, March, 1999.

[dA 97] DE ANDRADE, V. R. P. **A Ilusão de Segurança Jurídica - Do Controle Da Violência À Violência Do Controle Penal**. Porto Alegre: Livraria do Advogado, 1997.

[DAN 01] DANTAS, L. A. **ECN: Protocolo Criptográfico Para Emissão de Certidões de Nascimento Na Internet**. Universidade Federal de Santa Catarina, Dezembro, 2001. Dissertação de Mestrado.

[Dec 83] **Decreto N 89.250, de 27 de Dezembro de 1983.**

[Det 00] Detran lança sistema digital para habilitação de motoristas. **A tribuna do povo - Umuarama/PR**, [S.l.], 03, Fevereiro, 2000.

[dF 01] DE FRANÇA, R. M. V. Brasileiro: Você é a sua senha. **Impressões**, [S.l.], , n.9, p.14–16, Janeiro/Fevereiro/Março, 2001.

[dHF 99] DE HOLANDA FERREIRA, A. B. **Dicionário Aurélio Eletrônico Século XXI**. Versão 3.0. ed. Novembro, 1999.

[DIF 76] DIFFIE, W.; HELLMAN, M. New directions in cryptography. **IEEE Transactions on Information Theory**, [S.l.], v.IT-22, n.6, p.644–654, 1976.

[dO 01] DE OLIVEIRA, E. R. **Reconhecimento Automático de Impressão Digital Pela Polícia Federal**. Mensagem de correio eletrônico recebida de ”SEOP - Setor de Orientação e Planejamento”seop.ini@dpf.gov.br.

[DOM 97] DOMENICONI, C. **Direct Gray Scale Ridge Reconstruction in Fingerprint Images**. International Institute Advanced Scientific Studies, Salerno-Italy, November, 1997. Dissertação de Mestrado.

[dSC 02] DE SANTA CATARINA, S. D. S. P. D. E. **Secretaria Da Segurança Pública**. Disponível em <http://www.ssp.sc.gov.br/>. Acesso em: Fevereiro, 2002.

[ELL 99] ELLISON, C. M. The nature of a useable PKI. **Computer Networks**, [S.l.], v.31, p.823–830, 1999.

[eS 01] E SILVA, J. R. L. **Levantamento de Locais de Crime - Datiloscopia Criminal**. Polícia Civil do Distrito Federal, 09-20/07/2001. Curso de Perícias Criminais - Curitiba/PR.

[FAR 99] FARINA, A.; KOVÁCS-VAJNA, Z. M.; LEONE, A. Fingerprint minutiae extraction from skeletonized binary images. **Pattern Recognition**, [S.l.], v.32, p.877–889, 1999.

[FED 82] FEDERAIS, P. P. **Identificação Papiloscópica**. Instituto Nacional de Identificação - Departamento de Polícia Federal, 1982.

[fIS 00] FOR INFORMATION SYSTEMS, A. N. S.; OF STANDARDS TECHNOLOGY, N. I. Data format for the interchange of fingerprint, facial, scar mark and tattoo SMT information. ANSI / NIST-ITL, 2000. Relatório Técnico1.

[FRE 00] FREUNDENTHAL, M.; HEIBERG, S.; WILLEMSON, J. Personal security environment on palm PDA. In: COMPUTER SECURITY APPLICATIONS, 2000. ACSAC '00 16th Annual Conference, 2000. p.366 –372.

[GAN 01] GANDINI, J. A. D.; SALOMÃO, D. P. D. S.; JACOB, C. **A Segurança Dos Documentos Digitais**. Disponível em <http://www.jus.com.br>. Acesso em: Agosto, 2001.

[GAR 00] GARRIS, M. D.; MCCABE, R. M. **NIST Special Database 27 : Fingerprint Minutiae from Latent and Matching Tenprint Images**. Disponível em <http://www.itl.nist.gov/iaui/894.03/databases>. Acesso em: June, 2000.

[HER 95] HERDA, S. Non-repudiation: Constituting evidence and proof in digital cooperation. **Computer Standards and Interfaces**, [S.l.], v.17, p.69–79, 1995.

[HOJ 00] HOJERBACK, P. Digital signatures made easy with card-based fingerprints. **Ctt**, [S.l.], p.2–3, June, 2000.

[Hun 01] **PKI and Digital Certification Infrastructure**. Ninth IEEE International Conference on Networks, 2001.

[IDE 01] IDENTIX. **Biologon White Paper**. Indentix Incorporated, May, 2001.

[INT 02] INTERPOL. **Welcome to the Official Interpol Site**. Disponível em <http://www.interpol.int>. Acesso em: Março, 2002.

[Iso 01] **Development Of Personal Authentication System Using Fingerprint with Digital Signature Technologies**. Proceedings of the 34th hawaii international conference on system sciences, 2001.

[JAI 97] JAIN, A. K. et al. An identity-authentication system using fingerprints. **Proceedings of the IEEE**, [S.l.], v.85, n.9, p.1365–1388, September, 1997.

[JAI 00] JAIN, A.; PANKANTI, S. **Fingerprint Classification and Matching**, Handbook for image and video procesing. ed., April, 2000.

[JÚN 91] JÚNIOR, G. D. S. T. **A Papiloscopia Nos Locais de Crime: Dactiloscopia, Quiroscopia, Podoscopia**. São Paulo: Editora Ícone, 1991.

[JUS 02] JUSTIÇA, M. D. **Programa de Integração Nacional de Informações de Justiça e Segurança Pública**. Disponível em <http://www.mj.gov.br/>. Acesso em: Fevereiro, 2002.

[lei 00] **Lei N 10.054, de 7 de Dezembro de 2000**. Publicada no Diário Oficial da União de 08/12/2000.

[LEU 91] LEUNG, W. F. et al. Fingerprint recognition using neural network. **Proceedings of the 1991 IEEE Neural Networks for Signal Processing**, [S.l.], p.226–235, September, 1991.

[LIU 01a] LIU, J. K. et al. Multi-application smart card with elliptic curve cryptosystem certificate. In: EUROCON'2001 INTERNATIONAL CONFERENCE ON TRENDS IN COMMUNICATIONS., 2001. [s.n.], 2001. v.2, p.381–384.

[LIU 01b] LIU, S.; SILVERMAN, M. A practical guide to biometric security technology. **IT Pro**, [S.l.], p.27–32, January/February, 2001.

[LUM 97] LUMINI, A.; MALTONI, D. M. D. Continuous versus exclusive classification for fingerprint retrieval. **Pattern Recognition Letters**, [S.l.], v.18, p.1027–1034, September, 1997.

[MAC 02] MACCABE, R. M. **Interoperability of Biometric Information**. Disponível em <http://www.ncits.org/>. Acesso em: January, 2002.

[MAI 97] MAIO, D.; MALTONI, D. Direct gray-scale minutae detection in fingerprints. **IEEE Transactions on Pattern Analysis and Machine Intelligent**, [S.l.], v.19, n.1, p.27–39, January, 1997.

[MAI 99] MAINGUET, J.-F.; PÉGULU, M.; HARRIS, J. B. Fingerprint recognition based on silicon chips. **Future Generation Computer Systems**, [S.l.], v.16, p.403–415, March, 1999.

[MAR 98] MARCACINI, A. T. R. **O Documento Eletrônico Como Meio de Prova**. Disponível em <http://www.advogado.com/internet/zip/tavares.htm>. Acesso em: Outubro, 1998.

[MAT 02] MATSUMOTO, T. Importance of open discussion on adversarial analyses for mobile security technologies - a case study for user identification. In: ITU-T WORKSHOP ON SECURITY, SEOUL, 2002. [s.n.], 2002.

[MIC 02a] MICROSOFT. **Casos de Sucesso - Secretaria de Segurança Do Estado Traz Serviços on-Line**. Disponível em <http://www.microsoft.com/brasil/missaocritica/>. Acesso em: Novembro, 2002.

[MIC 02b] MICROSOFT. **MSDN**. Disponível em <http://msdn.microsoft.com>. Acesso em: Julho, 2002.

[NAV 01] NAVARRO, P. L. K. G. **AFIS - Automated Fingerprint Identification System**. Disponível em <http://www.pr.gov.br/celepar/celepar/batebyte/edicoes/2001/bb111/afis.htm>. Acesso em: Novembro, 2001.

[NIS 01] NIST. **NIST Image Group's Fingerprint Research**. Disponível em <http://www.itl.nist.gov/iad/894.03/fing/>. Acesso em: April, 2001.

[NOO 00] NOORE, A. Highly robust biometric smart card design. **IEEE Transactions on consumer electronics**, [S.l.], v.46, n.4, p.1059–1063, november, 2000.

[oC 94] OF COMMERCE, U. S. D.; OF STANDARDS, N. I.; TECHNOLOGY. Guideline for the use of advanced authentication technology alternatives FIPS PUB 190. 28, September, 1994. Relatório técnico.

[oI 99a] OF INVESTIGATION, F. B. Electronic fingerprint transmission specification. Department of Justice - Criminal Justice Information Services (CJIS), 1999. Relatório TécnicoV7.

[oI 99b] OF INVESTIGATION, F. B. **Inauguration of the Integrated Automated Fingerprint Identification System**. Disponível em <http://www.fbi.gov/pressrel/pressrel99/iafis.htm>. Acesso em: August, 1999.

[oI 02] OF INVESTIGATION, F. B. **IAFIS - Integrated Automated Fingerprint Identification System**. Disponível em <http://www.fbi.gov/hq/cjisd/iafis.htm>. Acesso em: Março, 2002.

[PAS 01] PASQUAL, E. S. **IDDE - Uma Infra-Estrutura Para a Datação de Documentos Eletrônicos**. Universidade Federal de Santa Catarina, Abril, 2001. Dissertação de Mestrado.

[PHI 00] PHILLIPS, P. J. et al. An introduction to evaluating biometric systems. **Computer**, [S.l.], p.56–63, February, 2000.

[PRI 01] PRINTRAK. **Printrak - A Motorola Company**. Disponível em <http://www.printrakinternational.com/>. Acesso em: Abril, 2001.

[RAB 96] RABELLO, E. **Curso de Criminalística**. Rua João Alfredo , 448 - Cidade Baixa - Porto Alegre/RS: Sagra- DC Luzzatto, 1996.

[RAT 00] RATHA, N. et al. **Robust Fingerprint Authentication Using Local Structural Similarity**. Fifth IEEE Workshop on Applications of Computer Vision.

[RAT 01a] RATHA, N. K.; CONNELL, J. H.; BOLLE, R. An analysis of minutiae matching strength. **Audio and Video-based Personal Indentification (AVBPA-2001)**, [S.l.], 2001.

[RAT 01b] RATHA, N. K.; SENIOR, A.; BOLLE, R. Automated biometrics. **Proceedings of ICAPR**, Rio de Janeiro, Brasil, 2001.

[RIV 77] RIVEST, R.; SHAMIR, A.; ADELMAN, L. A method for obtainig digital signatures and public-key cryptosystems. 1977. 15 p. Relatório TécnicoMIT/LCS/TM-82.

[ROD 97] RODDY, A. R.; STOSZ, J. D. Fingerprint features - statistical analysis and system performance estimates. **Proceedings of the IEEE**, [S.l.], v.85, n.9, p.1390–1421, September, 1997.

[SAN 01] SANTOS, G. C. D. Qual é o documento oficial de identidade apto a satisfazer à garantia constitucional? **Impressões**, [S.l.], , n.10, p.72, Abril/Maio/Junho, 2001.

[SEC 00] SECUGEN. **SecuAPI Especificação API**. SecuGen Corporation, 1. ed., 2000.

[STA 99] STALLINGS, W. **Cryptography and Network Security: Principles and Pratice**. 2. ed. New Jersey: Prentice Hall, 1999. 569 p.

[THO 97] THOMÉ, R. L. **Contribuição À Prática de Polícia Judiciária**. 2. ed. 1997.

[TOC 95] TOCHETTO, D. et al. **Tratado de Perícias Criminalísticas**. Rua João Alfredo, 448 - Cidade Baixa - Porto Alegre/RS: Sagra-DC Luzzatto, 1995.

[TOC 99] TOCHETTO, D. et al. **Identificação Humana**. 1. ed. Proto Alegre/RS: Editora Sagra Luzzatto, 1999.

Apêndice A

Dedos Artificiais

A.1 Introdução

A biometria tem sido apresentada como ferramenta de autenticação que oferece alta segurança e conveniência. Em [LIU 01b], por exemplo, a impossibilidade das características biométricas serem roubadas e a dificuldade de serem forjadas, são mencionadas. Entretanto, esses sistemas também estão sujeitos a ataques. Em [RAT 01a] são especificadas algumas formas de ataques a ambientes de identificação e autenticação biométrica. Eles vão desde a aquisição de uma imagem até o resultado do cotejo, considerando inclusive a possibilidade de se forjar uma característica biométrica, seja através de um dedo artificial, assinatura manuscrita ou por meio de uma máscara facial.

Notícias recentes questionam a segurança das impressões digitais na identificação de pessoas. Cientistas japoneses produziram um dedo artificial a base de gelatina. De acordo com os experimentos, tais dedos foram submetidos a sistemas de reconhecimento biométrico e obtiveram alto índice de aceitação, ”tapeando” os sistemas na maioria dos testes realizados [BBC 02].

O trabalho foi conduzido pelo professor Matsumoto[1] e um grupo de cientistas da Universidade Nacional de Yokohama, no Japão. Basicamente, foram criados dedos artificiais a partir de ”dedos reais” e de impressões digitais latentes.

[1]Tsutomu Matsumoto é Ph.D. em engenharia elétrica pela Universidade de Tóquio no Japão.

O estudo foi apreciado pelo especialista em segurança, Schneier[2], o qual disse que o fato de sistemas serem tapeados através do uso de ingredientes facilmente disponíveis deveria ser suficiente para pôr fim ao uso de sistemas de segurança baseados em impressões digitais [BBC 02].

A.2 Os Experimentos

O primeiro experimento envolvendo dedos falsos foi realizado quando gelatina foi despejada em uma moldura criada através do pressionamento de um ”dedo real” em um material plástico maleável. Ao final do processo, a moldura foi colocada no refrigerador para resfriar.

O segundo experimento envolveu a criação de dedos falsos a partir de impressões digitais latentes, novamente usando a gelatina para produção do dedo artificial. Dessa vez, a moldura foi criada da seguinte forma:

- Aplica-se cola sobre a impressão latente a fim de fixar a marca deixada pelas estrias da impressão digital.
- A imagem da latente é capturada através de fotografia.
- Realiza-se um processamento de imagem através do *software* Adobe Photoshop, visando ressaltar a diferença entre estrias e vales.
- A imagem é impressa em uma folha foto-sensível transparente, criando uma máscara.
- Esta máscara é juntada a uma placa de circuito impresso sendo ambas expostas a luz ultra-violeta.
- Logo após, a moldura é criada através da gravação da imagem em metal (cobre).

[2]Bruce Schneier é um pesquisador renomeado internacionalmente na área de segurança em computação, sendo fundador/diretor da empresa *Counterpane Internet Security, Inc.* (www.counterpane.com). Autor de vários livros, Schneier criou os algoritmos de criptografia *Blowfish* e *Twofish*.

Em ambos os casos, foram utilizados dois tipos de sensores, óptico e por capacitância, sendo que tais leitores aceitaram esse tipo de fraude em 80 por cento dos casos [MAT 02, BBC 02]. A Tabela A.1 resume esses achados.

Tabela A.1: Aceitação de dedos artificiais por sensores ópticos e de capacitância.

MATERIAL UTILIZADO	SENSOR ÓPTICO	SENSOR POR CAPACITÂNCIA
DEDO DE SILICONE	alta aceitação	baixa aceitação
DEDO DE GELATINA	alta aceitação	alta aceitação

Fonte: Publicação científica [MAT 02].

A.3 Perspectivas

Vários tipos de ataques são descritos no mundo científico [RAT 01a]. A biometria também é passível dessas investidas. Particularmente, o tipo de ataque apresentado é direcionado à etapa de aquisição de imagem, onde vulnerabilidades dos sensores de impressão digital são exploradas. No entanto, essas deficiências conduziram pesquisadores e indústria à proposição de técnicas para a construção de sensores mais eficientes no combate a esse tipo de fraude.

Além do problema dos dedos artificiais, deve-se contar com a hipótese macabra dos ”dedos mortos”. Nesse sentido, uma técnica interessante é a medida da quantidade de hemoglobina oxigenada no sangue através da espectroscopia. Essa quantidade é muito diferente entre dedos vivos e mortos. Por outro lado, esse método previne a fraude por intermédio dos dedos artificiais já que a análise é feita com base no sangue [COR 99].

De maneira especial, a pesquisa apresentada neste apêndice revela a necessidade de conduzir a avaliação da segurança em sistemas biométricos sob dois aspectos. O primeiro é o da precisão no processo de autenticação, comumente levado em consideração. O segundo é o aspecto segurança contra fraude, que não pode ser negligenciada e nem posta em segundo plano.

Apêndice B

NFIS

B.1 Introdução

O *Nist Fingerprint Image Software* é um sistema desenvolvido pelo NIST e distribuído gratuitamente através do seu sítio na Internet [NIS 01]. Nesse projeto, o FBI constituiu-se em um importante parceiro, exercendo papel fundamental no desenvolvimento e fornecimento de tecnologia.

Em contato mantido via *e-mail* com o Sr. Michael D. Garris[1], foi recebido um CD-ROM. Nele, existem alguns utilitários destinados a manipulação e análise de impressões digitais. Na Seção B.2, esses aplicativos são relacionados.

B.2 Conteúdo do CD-ROM

Trata-se de um software de domínio público com os códigos-fonte escritos na linguagem de programação ”C”. É possível a compilação dos programas nas plataformas UNIX, LINUX e WIN32. Basicamente, os aplicativos existentes estão distribuídos em quatro categorias:

[1]Michael D. Garris é cientista da computação do NIST atuando junto ao grupo de pesquisas relacionadas a imagens. Tal grupo de trabalho faz parte do Laboratório de Tecnologia da Informação (Divisão de acesso à informação).

1. PCASYS. Um sistema destinado à classificação das imagens de impressões digitais levando em conta os seguintes padrões: arco, presilha externa e interna, cicatriz, arco tendido e verticilo.

2. MINDTCT. Um detector de minúcias que localiza automaticamente os finais de linhas e as bifurcações.

3. Formato ANSI/NIST-ITL 1-200. O conjunto de utilitários foi projetado para ler, gravar, editar e manipular as imagens de impressões digitais baseado nesse formato de intercâmbio de imagens. No item 4.2.1, o padrão ANSI/NIST-ITL 1-200 foi apresentado.

4. Utilitários de imagem. Conjunto de aplicativos relacionados ao processamento de imagens, suportando a manipulação dos formatos de imagem JPEG e WSQ. Eles foram apresentados na Tabela 4.4.