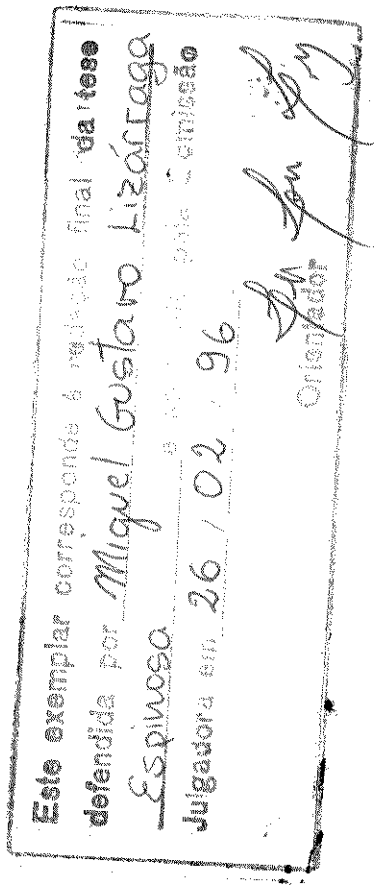
Universidade Estadual de Campinas
Faculdade de Engenharia Elétrica
Departamento de Comunicações

Um Sistema Automático de Consulta e Verificação de Assinaturas Estáticas



Autor

Miguel Gustavo Lizárraga Espinosa

Orientador

Lee Luan Ling

Tese apresentada à Faculdade de Engenharia Elétrica, Departamento de Comunicações, como parte dos requisitos para a obtenção do título de Mestre em Engenharia Elétrica

Campinas, 26 de Fevereiro 1996

FICHA CATALOGRÁFICA ELABORADA PELA
BIBLIOTECA DA ÁREA DE ENGENHARIA - BAE - UNICAMP

L768s

Lizárraga Espinosa, Miguel Gustavo
Um sistema automático de consulta e verificação de assinaturas estáticas / Miguel Gustavo Lizárraga Espinosa.--Campinas, SP: [s.n.], 1996.

Orientador: Luan Ling Lee
Dissertação (mestrado) - Universidade Estadual de Campinas, Faculdade de Engenharia Elétrica.

1. Reconhecimento de padrões. 2. Assinaturas. 3. Sistemas de reconhecimento de padrões. I. Lee, Luan Ling II. Universidade Estadual de Campinas. Faculdade de Engenharia Elétrica. III. Título.

Para meus queridos pais,

Gustavo e Carmen,

pelo seu amor, sua dedição e

inúmeros ensinamentos

que vêm me oferecendo

ao longo de toda minha vida.

Agradecimentos:

Ao meu orientador, Prof. Lee Luan Ling, pela sua ajuda e apoio na realização deste trabalho.

A Célia Piglione, minha futura esposa, pelo seu carinho e afeto que tem me brindado desde o momento que nos conhecemos.

Ao meu compadre David Aguilar, pela sua amizade sincera.

Aos meus colegas do Laboratório de Reconhecimento de Padrões e Redes de Computadores, em especial a Natanael Gomes, Emiliano Alves, Flavia Schneider Gean Breda, Antonio de Moraes e Gladys Maquera.

Aos meus colegas, amigos e conterrâneos que me ajudaram ao longo da minha vida acadêmica, em especial ao meu amigo Ricardo Ramirez.

Ao Centro de Pesquisa e Desenvolvimento da Telebrás pela colaboração neste trabalho.

Sumário

Capítulo 4

Capítulo 5

Capítulo 6

Capítulo 7

Capítulo 8

Lista de Tabelas

Lista de Figuras

Resumo

A presente tese apresenta um sistema automático de consulta e verificação de assinaturas estáticas. Tal sistema permite mostrar imagens de assinaturas na tela do computador, comprimir e descomprimir imagens de assinaturas, enviar e receber dados via rede de computadores e verificar automáticamente a autenticidade ou não de assinaturas.

Como parte do sistema, foi implementado um novo método de compressão de arquivos de assinaturas, que consegue uma taxa de compressão de até 96,05%. Além disso, o presente trabalho, introduz uma nova técnica de extração de características de assinaturas que utiliza operações da morfologia matemática.

Nos testes de verificação de assinaturas estáticas, foi utilizado o total de 950 assinaturas. Esse conjunto de assinaturas é dividido em três partes: 550 assinaturas verdadeiras, 100 falsificações aleátorias e 300 assinaturas habilitadas. Como desempenho do nosso sistema de verificação, obtivemos as médias de taxas de erros iguais de 14,6 % frente a falsificações habilitadas e de 3,0 % frente a falsificações aleatórias.

Capítulo 1

Introdução

A assinatura humana tem um papel importante na nossa sociedade, sendo considerada um símbolo de reconhecimento, de autorização, de responsabilidade e de autentificação. Por este motivo, a assinatura é atualmente aceita como um dos métodos mais comuns para se autenticar a identidade de um indivíduo. Além disso, é também utilizada como complemento na validação dos meios tradicionais de identificação, tais como carteira de identidade, selos, carimbos, cartões magnéticos etc.

Hoje, no Brasil, o uso de cheques e cartões de crédito pela população é tão comum quanto o papel moeda, mas raramente os funcionários de lojas, de bancos e de cartórios estão habilitados a verificar a autenticidade das assinaturas apresentadas. Para aliviar esse problema, se faz necessário o estudo e a implementação de sistemas de identificação pessoal que permitam, entre outras funções, a verificação automática das assinaturas em documentos, com o objetivo de agilizar o processo de verificação e diminuir o número de falsificações.

Na década passada, o problema de verificação automática de assinaturas foi solucionado através de sistemas de verificação de assinaturas dinâmicas [Plamondon], também chamados de sistemas *on-line*. Estes sistemas se caracterizam pelo uso de informações dinâmicas do processo de escrita, tais como velocidade e aceleração. A taxa de acerto dos sistemas *on-line* é bastante elevada, mesmo quando as falsificações são feitas por especialistas [Lee92]. O bom desempenho desses sistemas é obtido por que os falsificadores procuram imitar somente a forma da assinatura original e não

conseguem reproduzir os traços da assinatura, nos mesmos intervalos de tempo que o indivíduo genuíno. Desta forma, esses sistemas se valem da falta de consistência dos dados temporais em assinaturas falsificadas, para obter uma melhor discriminação entre a classe de assinaturas verdadeiras e a classe de assinaturas falsas.

O principal limitante desse tipo de sistema é que a assinatura sempre deve ser escrita sobre um equipamento que permite a aquisição das informações dinâmicas. No entanto, escrever sobre este tipo de equipamento muitas vezes não deixa que o escritor assine de maneira natural, implicando em mudanças do estilo de sua assinatura.

Por outro lado, os sistemas de verificação de assinaturas estáticas, também chamados de sistemas *off-line*, se caracterizam por utilizar apenas a imagem da assinatura para extrair as informações que alimentam o sistema. As taxas de acerto dos sistemas *off-line* são geralmente inferiores que as taxas de acerto dos sistemas *on-line*. Isto se deve ao fato de que as imagens de assinaturas poderem ser facilmente copiadas, e a informação dinâmica que poderia ser extraída dessas imagens torna-se altamente degradada na amostra estática [Boccignone]. Desta forma, um bom falsificador poderia criar uma copia suficientemente fiel da assinatura original, levando o sistema a classificar erroneamente a assinatura falsificada como sendo verdadeira.

A principal vantagem dos sistemas *off-line* é preservar ao máximo a naturalidade do processo de escrita, pois no ato de assinar não existe nenhum tipo de dispositivo que venha interferir diretamente na escrita da assinatura [Gomes].

Nesta tese é proposto um sistema *off-line* que consegue distinguir, com uma alta taxa de acerto, as falsificações feitas sem o conhecimento da assinatura original. Todavia, o sistema proposto é capaz de apresentar um bom desempenho na detecção de falsificações feitas conhecendo-se previamente a assinatura original.

1.1 Objetivo do trabalho

O objetivo desse trabalho é apresentar o sistema automático de verificação de assinaturas estáticas, que desenvolvemos no Laboratório de Reconhecimento de Padrões e Redes de Comunicações (LRPRC) da Faculdade de Engenharia Elétrica da UNICAMP.

Nosso trabalho especifica e implementa os processos de consulta e verificação de assinaturas estáticas dentro de um sistema que permite codificar, compactar, descompactar, apresentar e verificar automaticamente imagens de assinaturas. No decorrer da tese apresentaremos os vários componentes que formam o protótipo do nosso sistema completo de verificação de assinaturas estáticas.

1.2 Estrutura do trabalho

Divido em 8 capítulos, nosso trabalho traz no capítulo 2 uma introdução sobre o processo de escrita das assinaturas e discute suas características e tipos de falsificações. No capítulo 3 apresentamos o ambiente gráfico desenvolvido para o protótipo do sistema automático de verificação. No capítulo 4 mostramos algumas técnicas clássicas de compressão de dados e também nosso método de compressão de imagens desenvolvido para o sistema. As principais diferenças entre sistemas *on-line* e *off-line* estão detalhadas no capítulo 5, que apresenta ainda uma exposição sobre os parâmetros de desempenho para esses sistemas e várias técnicas de verificação utilizadas por outros autores. No capítulo 6 é apresentada uma breve introdução à morfologia matemática, que é a técnica utilizada na extração de características das assinaturas. O método de verificação utilizado é discutido no capítulo 7, no qual detalhamos os diferentes estágios

por onde a assinatura passa, até que se obtenha a resposta do pedido de verificação. Finalmente, no capítulo 8 apresentamos as conclusões, as discussões e os comentários a respeito do trabalho aqui desenvolvido.

Capítulo 2

Assinaturas Manuscritas

Por ser considerada tradicionalmente a forma mais confiável e légítima de reconhecimento da identidade de um índivíduo, a assinatura manuscrita é exigida em transações financeiras, de forma que o indivíduo também ateste o conhecimento, o conteúdo e sua concordância com os termos do documento.

O motivo que permite utilizar a assinatura como um dos meios mais confiáveis de identificação é que ela contém características únicas da escrita do assinante. Essas características são o reflexo de um conjunto de fatores físicos e psicológicos desse indivíduo durante a escrita. Com base nessas características, especialistas em assinaturas procuram quantificá-la com o intuito de definir, de maneira consistente, se uma certa assinatura foi feita pelo indivíduo genuíno ou por uma outra pessoa qualquer [Mantas].

Neste capítulo apresentaremos como as pessoas gradativamente criam suas assinaturas, os problemas que influenciam na sua escrita, as características que geralmente os especialistas em assinaturas utilizam para estabelecer sua legitimidade e, finalmente, os tipos de falsificações que ocorrem na prática.

2.1 A assinatura humana

A seguinte definição para a palavra *assinatura* é encontrada no Dicionário Aurélio Básico da Língua Portuguesa: "É o ato ou efeito de subscrever o próprio sinal ou nome em documento". Especialistas em análise de documentos, e outros que se confrontam com um grande número de assinaturas, de fato constatam a frase

"subscrever o próprio sinal". Essa frase é verdadeira por que muitas vezes as assinaturas não correspondem à escrita legível do seu nome. O que ocorre, na verdade, é uma junção entre componentes da escrita manuscrita com uma série de traços estilísticos, que tem por objetivo individualizar a assinatura através de um sinal gráfico. Mesmo que a assinatura seja totalmente ilegível, ela é suficiente para ser reconhecida como pertencendo a um determinado indivíduo [Hilton].

A assinatura de uma pessoa evolui à medida em que vai sendo feita repetidamente, aparecendo pequenas diferenças na sua forma e em seu estilo cada vez que o escritor se dispõe a reproduzí-la. Por isso constata-se que duas assinaturas da uma mesma pessoa nunca são exatamente iguais. As pequenas diferenças ou variações que as assinaturas de um mesma pessoa apresentam são chamadas de variações intrapessoais [Plamondon].

Passamos a nos referir como assinatura verdadeira àquela que o escritor reproduz mantendo um mesmo padrão de letras e de traços, sem a necessidade de um esforço grande de concentração. Assim através de um grupo de assinaturas verdadeiras é possível se derivar hábitos e qualidades da escrita. Esses tipos de amostras são a base do estudo da assinatura humana e é com elas que se pode determinar se a assinatura de uma pessoa é autêntica ou não.

A assinatura de uma pessoa não apresenta uma forma única e bem definida, pois aparecem variações em seus traços a cada momento em que ela é reproduzida. Ainda mais, quando nos referimos ao ato de verificação de assinaturas, a assinatura de uma pessoa só é consistente se comparada com um conjunto de assinaturas que ela espontaneamente reproduziu.

Partindo da utilização de um conjunto de assinaturas verdadeiras, especialistas em assinaturas vêm se valendo das características de forma, de movimento e de possíveis influências externas do meio para estabelecer sua autenticidade. Esses especialistas definiram dois tipos de fatores que influenciam de maneira direta no processo de escrita de uma assinatura. O primeiro fator se refere às influências internas, que são qualidades inerentes da pessoa que assina, e o segundo fator diz respeito às influências externas ou do meio, que atuam no momento da escrita da assinatura [Hilton].

2.2 Análise de assinaturas

Na análise de assinaturas procura-se características de sua escrita que sejam específicas a ela. Podemos citar os toques inicias e finais da assinatura, a rapidez da execução, a forma da letra, os alinhamentos vertical e horizontal, a razão de distância entre as várias letras, o espaçamento entre palavras da mesma assinatura, a qualidade das linhas da escrita, o tamanho total da assinatura e os traços de estilo, entre outras características [Lindgren].

Num mesmo indivíduo, a maioria dessas qualidades variam levemente e se enquadram dentro de um limite máximo. É por causa disso que, quando se tenta determinar a legitimidade de uma assinatura, o examinador do documento tentará conduzir a verificação pela comparação da assinatura em questão, com um conjunto de assinaturas verdadeiras. Esse conjunto de assinaturas deve, de preferência, ter sido adquirido de forma semelhante e mais ou menos na mesma época da assinatura que se deseja examinar [Eden].

O objetivo do exame utilizando um conjunto de assinaturas verdadeiras é determinar o grau de variação, ou seja, quanto podem variar as assinaturas de uma mesma pessoa. De maneira geral, o grau de variação será diferentemente afetado por influências internas e externas que atuam no momento do assinar. Assim sendo, pode se esperar um alto grau de variação entre as assinaturas onde influências internas e externas se apresentaram, e uma variação pequena quando as influências externas e internas se mantiveram constantes.

Podemos citar como influências externas o tamanho do instrumento de escrita, seu peso e a maneira como a ponta do instrumento desliza sobre o papel. A posição do escritor em relação ao papel que irá assinar possui uma relevância importante no grau de variação. Ou seja, se o escritor se encontra em pé ou não, se está confortavelmente sentado ou de maneira incomoda, se está numa posição mais inclinada ou reta, se a mão, pulso, braço e cotovelo estão na posição normal de escrita ou não. O tipo de papel que se está utilizado pode também criar alguns problemas, como por exemplo, se a folha de papel em que se está escrevendo é muito áspera ou lisa. A inclinação do papel com relação à posição do escritor é também importante, principalmente se ele tem algum problema físico [Foley].

As influências internas são principalmente do tipo psicológico. O estado emocional, a pressa, a idade do assinante ou ainda uma simples dor de cabeça influem no resultado final da assinatura.

O conjunto destas influências resulta, de uma forma geral, em variações no traço da assinatura, dentre as quais podemos citar a proporção entre as palavras, a inclinação e arredondamento das letras, a ornamentação, a legibilidade etc. Ocorrem também

variações nas características ligadas à dinâmica dos movimentos da escrita, como a não-uniformidade da velocidade e interrupções durante a escrita das palavras [Chuang].

2.3 Assinaturas pessoais

Quando uma pessoa deseja criar sua assinatura, começa a fazer uma série de esboços. Depois de algum tempo de exercício constante, consegue reproduzir seus traços de forma automática.

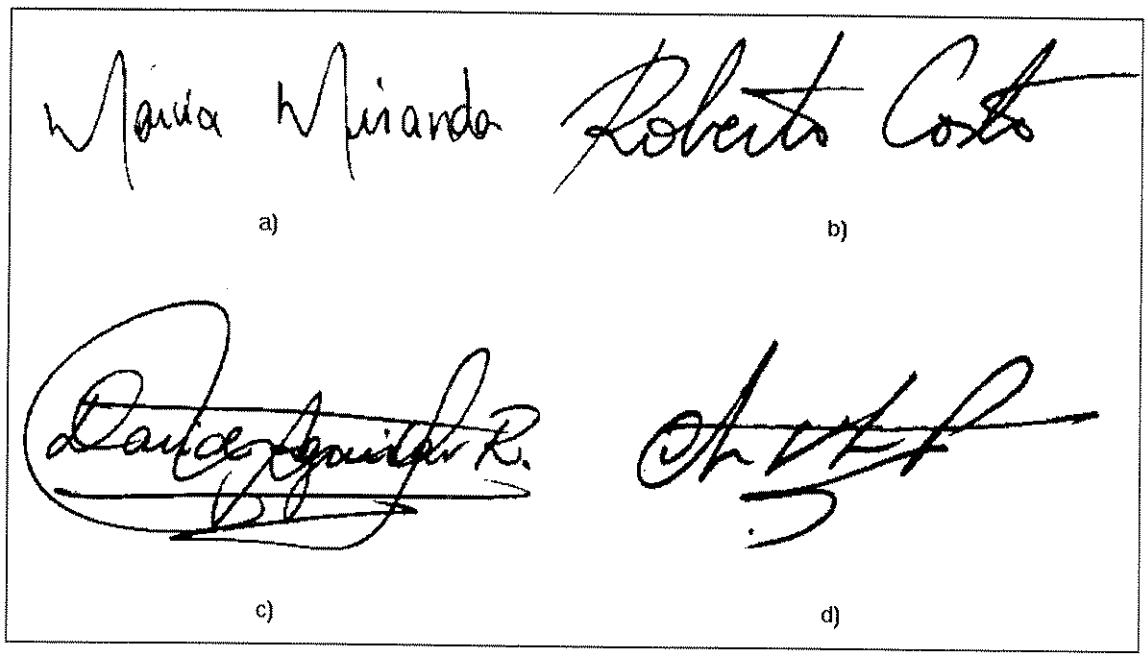


Figura 2.1: Estilos de assinaturas manuscritas.

Dependendo da aparência final que o indivíduo deseja dar para sua assinatura, ela pode ser classificada em dois grupos. O primeiro grupo é aquele no qual a aparência final reflete o próprio nome do escritor. Nesse caso, a pessoa assina se valendo quase que exclusivamente da semântica do seu nome e do seu estilo padrão de escrita, como nas assinatura a) e b) da figura 2.1. O segundo grupo é aquele em que a aparência final da assinatura toma a forma de um sinal gráfico. Nesse caso, a habilidade gráfica do

escritor é em geral mais aprimorada, visto a dificuldade em tentar sempre reproduzir um grafismo que se preocupa mais com a forma dos traços do que com a semântica do próprio nome, como nas assinaturas c) e d) da figura 2.1.

Em ambos os grupos, a assinatura da pessoa irá tornar-se personalizada à medida em que o tempo passa e ela for produzida regularmente.

2.4 Falsificações de assinaturas

Uma assinatura falsificada é aquela feita com o intuito de imitar uma assinatura verdadeira para se passar por legítima.

Tomando como referência a semelhança existente entre uma assinatura original e sua falsificação, encontramos três tipos de falsificações: as aleatórias, as simples e as habilitadas. Pelas informações obtidas através de um banco nacional, mais de 90% das assinaturas falsificadas encontradas em documentos bancários são constituídas de falsificações aleatórias e simples.

2.4.1 Falsificação aleatória

As falsificações aleatórias se caracterizam por ter sua forma gráfica e constituintes semânticos completamente diferentes da assinatura original. Nesse caso, o falsificador faz uma assinatura no documento sem se importar em imitar os traços básicos da assinatura original, inclusive chegando a escrever seu próprio nome ou qualquer outro grafismo para indicar que se trata da assinatura genuína.

2.4.2 Falsificação simples

Esse tipo de falsificação ocorre quando um falsificador escreve o nome da pessoa corretamente mas não consegue imitar sua forma gráfica. Desta maneira, a falsificação pode parecer ou não com a assinatura original.

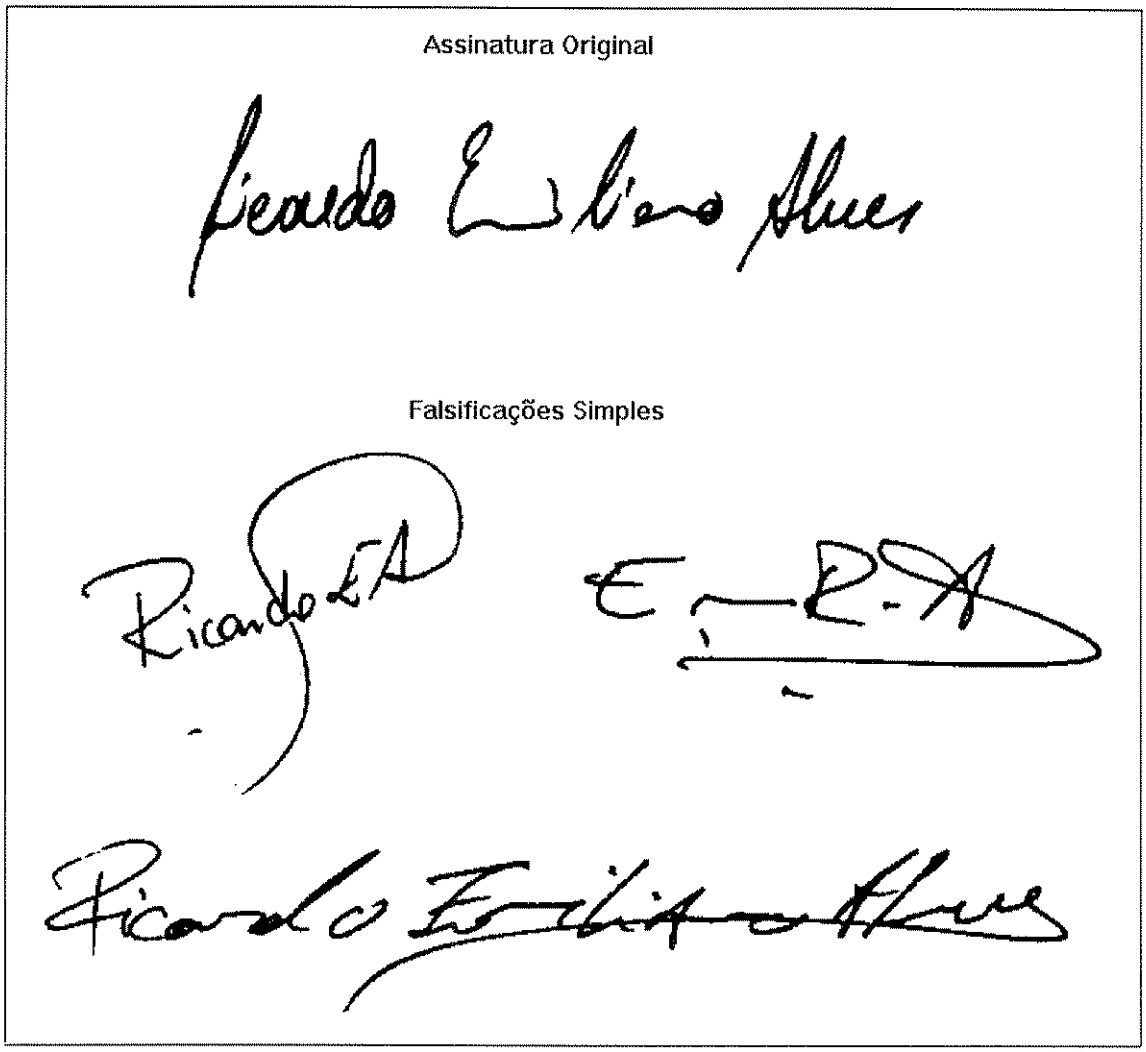


Figura 2.2: Exemplo de falsificações simples.

Esse tipo de falsificação geralmente ocorre quando o falsificador possui apenas o conhecimento do nome da pessoa, mas não tem nenhuma cópia impressa da assinatura verdadeira para se basear e assim poder desenhar uma falsificação mais aprimorada. A

figura 2.2 mostra um exemplo de falsificação simples, onde temos a assinatura genuína na parte superior e as falsificações na parte inferior.

2.4.3. Falsificação habilitada

Esse tipo de falsificação é produzida quando o falsificador tem acesso a uma amostra da assinatura original. O falsificador faz um esforço para obter a reprodução fiel dessa assinatura, trabalhando da maneira mais detalhada possível traço após traço, até conseguir uma falsificação de excelente qualidade. A figura 2.3 mostra o exemplo de duas falsificações habilitadas, que tiveram como modelo a assinatura que se encontra na parte superior dessa figura.

Figura 2.3: Exemplo de falsificações habilitadas.

Capítulo 3

Apresentação de Assinaturas Estáticas

O presente capítulo introduz o software que desenvolvemos para a apresentação, compressão e verificação de assinaturas.

Dentro desse contexto, o software possui as seguintes funções:

1. Aquisição de assinaturas.
2. Apresentação das imagens de assinaturas na tela do computador.
3. Compressão e descompressão das imagens de assinaturas.
4. Envio e recepção de dados via rede de computadores.
5. Extração do vetor de características de uma assinatura.
6. Verificação automática de uma assinatura.

Nas próximas seções apresentaremos o equipamento utilizado na implementação do nosso sistema, detalharemos a base de dados de assinaturas utilizada, mostraremos o ambiente gráfico do software de verificação de assinaturas e finalizaremos com a proposta de um sistema automático de consulta de assinaturas através de redes de computadores.

3.1 Equipamento

O formato geral do equipamento utilizado para a execução desse trabalho está ilustrado na figura 3.1. Os componentes principais foram um computador pessoal e um *scanner* de mesa.

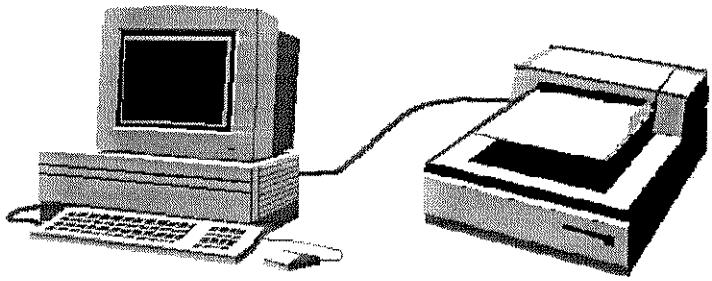


Figura 3.1: Equipamento utilizado no desenvolvimento do sistema automático de verificação de assinaturas estáticas.

O *scanner* de mesa utilizado é o HP Jetscan II. O software que gerencia o *scanner* é o "DeskScan" e permite gerar imagens digitais em formatos de arquivo tipo PCX, JPEG, GIF e BMP. A resolução utilizada para a digitalização das assinatura é de 300 dpi.

O microcomputador utilizado é o IBM-PC compatível 486DX2 / 66 Mhz, com 16 Mbytes de RAM e um monitor de vídeo com resolução de 1024 x 768 pixels.

3.2 Banco de dados

O total de 950 imagens constitui o banco de dados de assinaturas desse trabalho. As imagens das assinaturas estão divididas em três grupos: as verdadeiras, as falsificações habilitadas e as falsificações aleatórias.

O grupo de assinaturas verdadeiras totaliza 550 imagens. Essas assinaturas foram obtidas junto a cinco pessoas, sendo que cada uma delas contribuiu com 110 assinaturas. As assinaturas verdadeiras foram coletadas num período de seis meses.

Para cada um dos cinco tipos de assinaturas verdadeiras foram adquiridas 60 falsificações habilitadas. Essas 60 falsificações foram feitas por outras cinco pessoas

diferentes, tendo cada uma assinado 12 vezes. Dessa forma o grupo de falsificações habilitadas consta de 300 imitações.

O grupo das falsificações aleatórias é formado por 100 assinaturas de mais 50 pessoas diferentes. Assim, o número de assinaturas adquiridas para os testes do sistema é de 550 verdadeiras e de 400 falsas, totalizando 950 assinaturas.

Todas as assinaturas coletadas ficam restritas a uma área retangular de 10 centímetros de comprimento por cinco centímetros de altura, que por sua vez são os parâmetros que definimos para o *scanner* fazer a digitalização das mesmas. Esses parâmetros foram estipulados empiricamente, visto que a totalidade das assinaturas coletadas pôde ser enquadrada utilizando-se essa área sem nenhuma perda de informação. A utilização de 300 dpi para a digitalização de uma área de 10cm por 5cm gera imagens digitais de 1200 pixels por 600 pixels. A figura 3.2 mostra um exemplo de assinatura coletada.

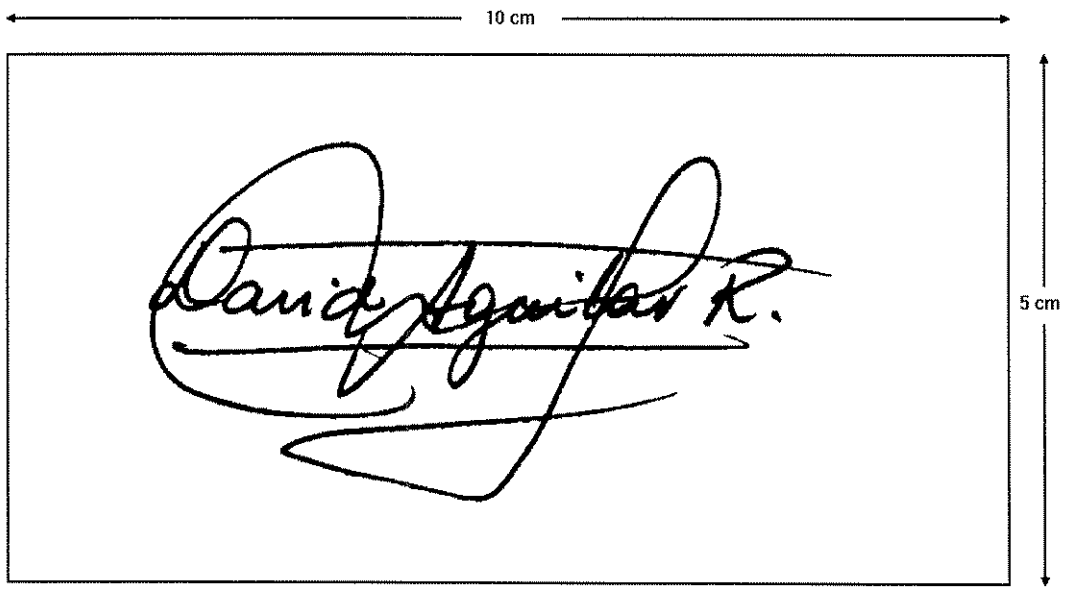


Figura 3.2 - Exemplo de uma assinatura.

Outro fato importante durante o processo de coleta das assinaturas foi a utilização de uma caneta com tinta de cor preta e diâmetro de ponta 0.5 mm. Esse detalhe se fez necessário para que na digitalização da imagem conseguíssemos maior contraste entre a folha branca de papel e a assinatura, obtendo assim melhor qualidade na imagem digitalizada.

3.3 Ambiente gráfico do software de verificação

O ambiente gráfico desenvolvido para a verificação e apresentação das assinaturas foi implementado através da linguagem C++ dentro do ambiente Windows. A finalidade é fornecer uma interface amigável ao operador no trabalho de consulta e verificação de assinaturas [Calvert].

A figura 3.3 mostra uma janela do ambiente gráfico desenvolvido apresentando uma assinatura. Na área superior da janela temos denominado o "Sistema Automático de Verificação de Assinaturas Estáticas" e, a seguir, existe uma barra contendo os comandos das diferentes operações que o sistema pode realizar.

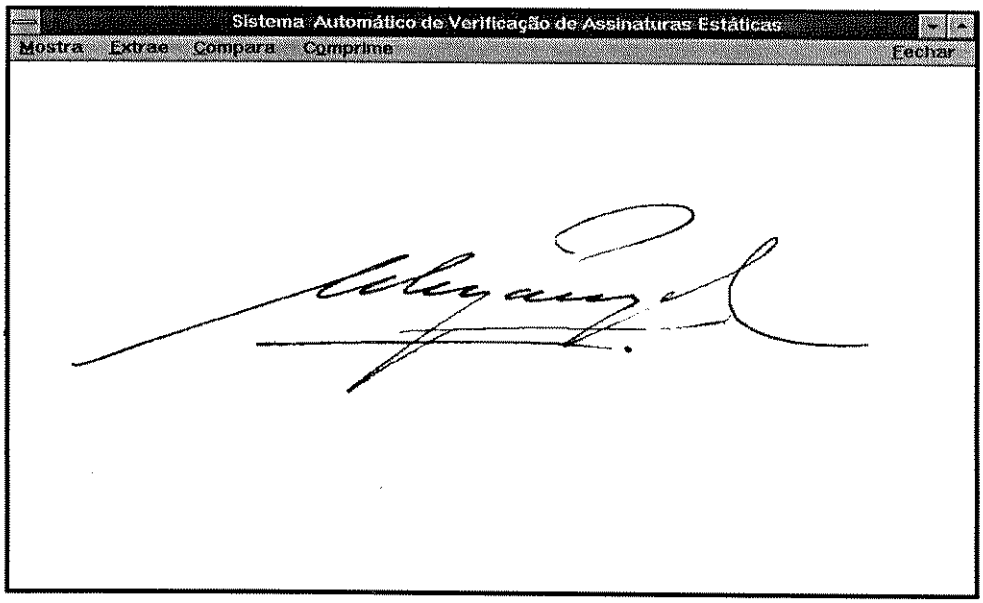


Figura 3.3: Exemplo do ambiente gráfico apresentador de assinaturas.

Em seguida detalhamos cada operação:

Mostra: Nessa operação o sistema acessa um arquivo contendo a imagem da assinatura que se quer analisar. Quando o arquivo é aberto, a imagem da assinatura é apresentada na tela do computador. Essa opção pode ser utilizada pelo operador que deseja fazer a verificação visual da assinatura através do seu conhecimento de técnicas grafológicas.

Extrae: Trata-se da execução de um algoritmo que extrai um vetor de características de uma assinatura previamente selecionada. Esse vetor é composto por 62 elementos. Os 32 primeiros elementos estão relacionados à inclinação dos traços da assinatura. Os 30 restantes estão relacionados com a inclinação dos contornos da imagem.

Compara: Nessa operação o sistema executa o processo de verificação automática da autenticidade de uma assinatura. Essa operação é composta do envio do pedido de verificação e da imagem da assinatura, avaliação da assinatura pelo banco de dados e retorno da resposta do pedido.

Comprime: É a operação que faz a compressão da imagem de uma assinatura.

Fechar: Desativa a janela do software de sistema de verificação de assinaturas.

Dentro do contexto da utilização do software de verificação de assinaturas numa rede de computadores, implementamos a opção de transmissão de dados via rede. Isso permite o acesso do banco de dados de assinaturas por terminais remotos que estejam ligados à rede. A implementação foi testada através de uma rede local tipo Ethernet de 10 Mbits/seg, utilizando protocolos IPX/SPX e TCP/IP com o sistema operacional WINDOWS NT.

A figura 3.4 apresenta o tipo de janela que é aberta pelo software de verificação de assinaturas quando acontece um pedido de transferência de dados entre um terminal local e o banco de dados, ou outro terminal que esteja ligado à rede.

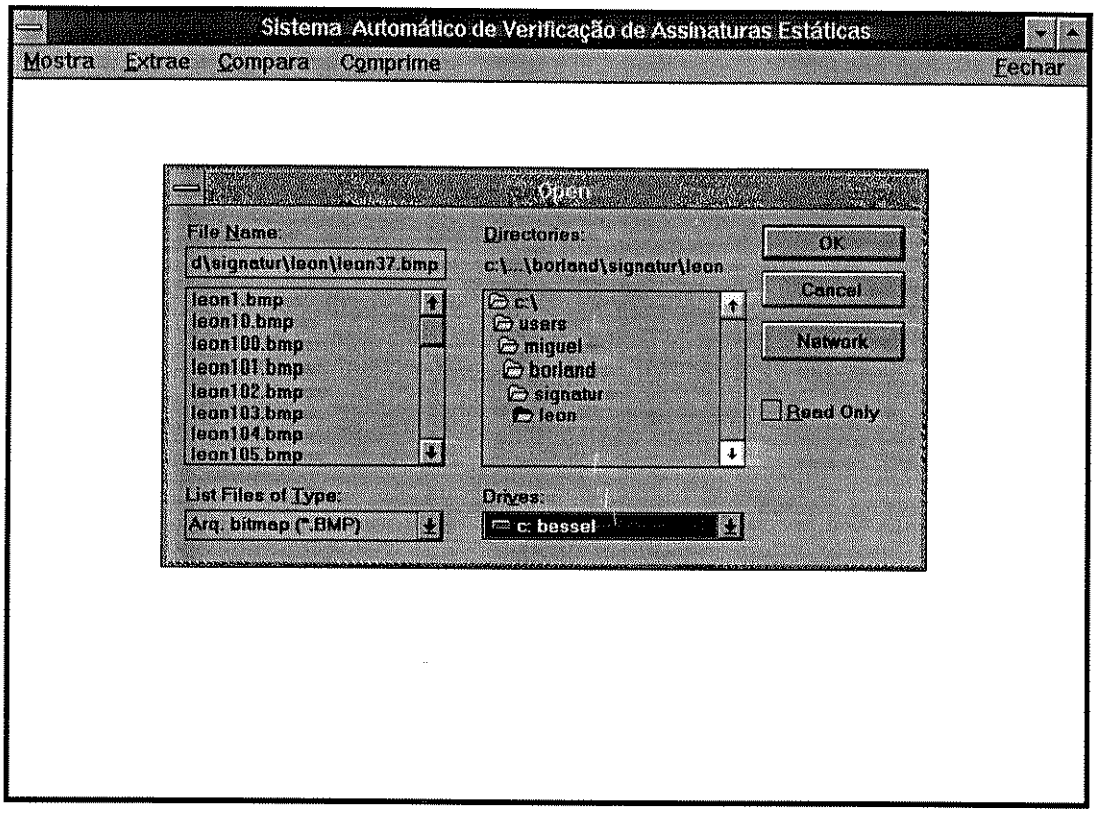


Figura 3.4: Transmissão de dados via rede.

3.4 Consulta de assinaturas via rede

No contexto de redes de computadores, a figura 3.5 apresenta um modelo de sistema automatizado de consulta e verificação de assinaturas estáticas, que utiliza uma rede em anel.

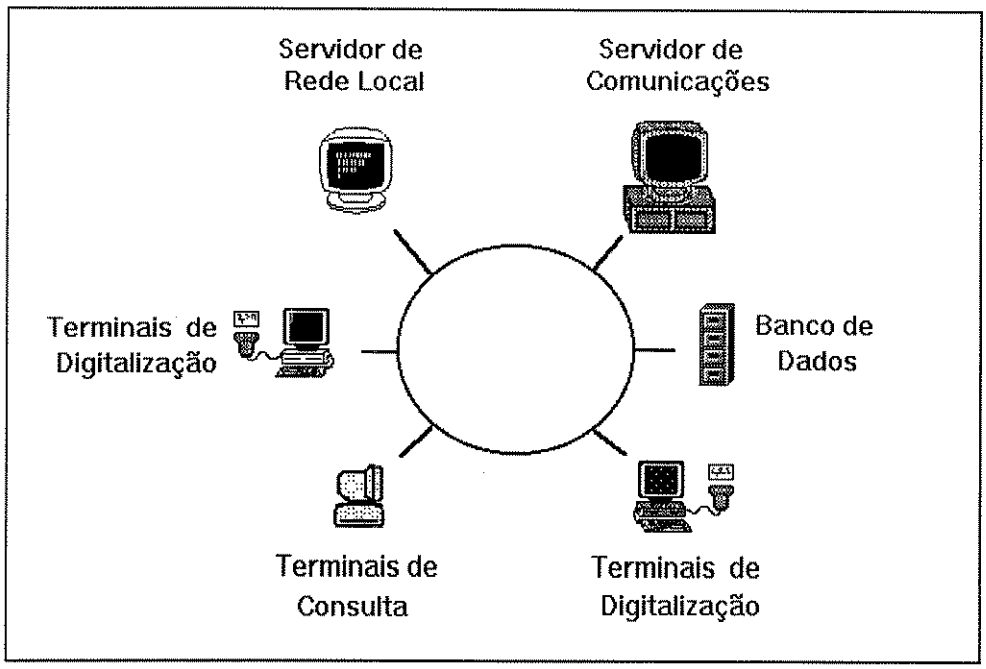


Figura 3.5: Sistema automatizado de aquisição, verificação e consulta de assinaturas.

Na rede local em anel temos os diversos dispositivos que estariam interligados para viabilizar o sistema de verificação:

- Terminais de consulta: através deles seria possível fazer o pedido de consulta ao banco de dados para verificação da assinatura.
- Terminais de digitalização: nesses terminais, além da consulta ao banco de dados, seria possível a digitalização de assinaturas estáticas para serem enviadas ao banco de dados para a verificação automática das mesmas.
- Servidor de rede local: computador encarregado de gerenciar os recursos entre os demais terminais pertencentes à rede local.
- Servidor de comunicações: através desse dispositivo todos os terminais ligados à rede local podem entrar em contato com outras redes em outros lugares, compartilhando e acessando informações distribuídas por aquelas redes.
- Banco de dados: responsável pelo armazenamento das informações necessárias para a verificação de assinatura e de outros dados importantes para o sistema.

A verificação da autenticidade de uma assinatura poderia ser feita basicamente de duas maneiras [Lee92]:

1.- **Manual**: a própria pessoa que pede a consulta ao banco de dados de assinaturas utiliza técnicas de grafologia para constatar a autenticidade, comparando a imagem apresentada no seu terminal de vídeo com o documento que deseja avaliar.

2.- **Automática**: nesse caso, é necessário que o consultante tenha acesso a um *scanner* para digitalizar o documento a ser verificado. A seguir, deve entrar com o pedido junto ao banco de dados para a verificação automática da assinatura que acabou de ser digitalizada. Uma vez recebido o pedido de verificação, serão utilizados os algoritmos pertinentes que realizarão a verificação automática, retornando para o consultante o resultado da operação.

Capítulo 4

Compressão de Imagens de Assinaturas Estáticas

A compressão de imagens de assinaturas estáticas se faz necessária uma vez que o tamanho do arquivo que armazena assinatura estática — que foi digitalizada se utilizando 300 dpi sobre uma área e 10cm por 5cm — pode chegar a 90.000 bytes. Isso implica num elevado espaço para armazenamento e na utilização ineficiente dos sistemas de transmissão de dados.

O método implementado para nosso sistema de verificação utiliza técnicas clássicas de compressão de imagens, levando em consideração as características das imagens de assinaturas. Entre essas característica podemos citar:

1. Serem imagens em preto e branco (binárias).
2. Existir um grande número de pixels brancos e pixels pretos em seqüência.
3. Serem imagens compostas por traços de espessura constante.

4.1 Compressão de imagens digitais

Uma imagem digital é definida como uma função bidimensional de intensidade luminosa $I(x,y)$, onde x e y representam coordenadas espaciais e o valor de $I(x,y)$ é proporcional ao briho (ou nível de cinza) no ponto (x,y). A compressão de

uma imagem visa à redução da quantidade de bits necessária para sua representação [Pentland].

A compressão de imagens apresenta três campos básicos de aplicação:

1. Armazenamento
2. Transmissão
3. Análise de imagens

Os métodos de compressão de imagens são aplicáveis a qualquer um dos campos acima citados, mas é importante observar que a escolha de um método específico está ligada principalmente à aplicação e ao tipo de imagem que se deseja comprimir.

São exemplos de aplicações de compressão de imagens:

- A otimização da utilização de recursos de memórias de bancos de imagens para uso científico, educacional, médico, artístico etc.
- A transmissão de imagens comprimidas de satélite, TV, radar, teleconferência, fac-símile e outros tipos de comunicação via sinais digitais.
- A redução da quantidade de dados processados por algoritmos de reconhecimento de padrões.

O processo de compressão de imagens pode ser modelado por uma seqüência de três operações - a quantização, a codificação e a otimização -, como ilustra a figura 4.1. Na quantização, cada dado amostrado no processo de digitalização fica definido por um conjunto de bits. Já na codificação, uma palavra é associada a cada saída quantizada. Finalmente, na otimização é gerado um novo código de menor tamanho do que aquele obtido simplesmente pela codificação [Lizárraga].

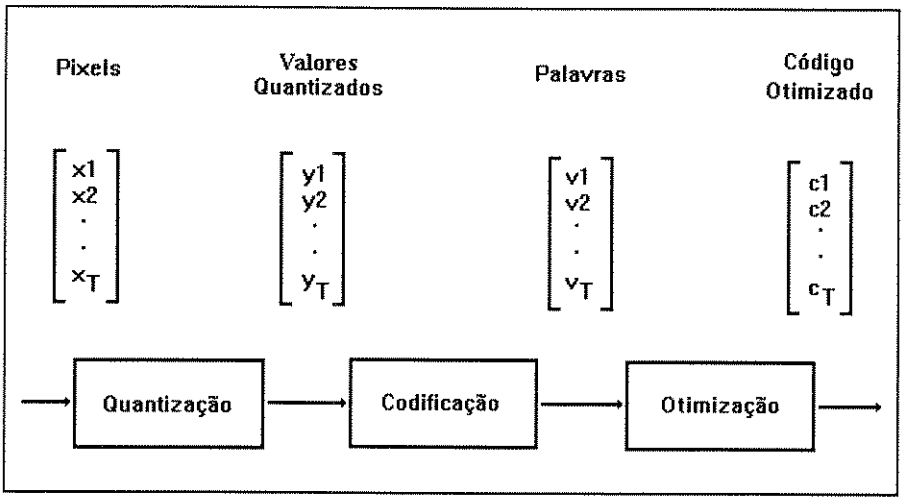


Figura 4.1: Modelo de compressão de imagens.

4.1.1 Quantização

O processo de quantização é o que define a quantidade de níveis de cinza que cada pixel pode tomar. Desta forma, a quantização dos pixels consiste em agrupar o conjunto dos possíveis valores de pixels em intervalos. Se um valor a ser quantizado se encontra dentro do k-ésimo intervalo, o seu valor quantizado corresponderá ao valor representativo daquele intervalo.

4.1.2 Codificação

Codificação é o processo que associa uma palavra-código a cada um dos valores quantizados.

Define-se a palavra-código como um conjunto de bits ao qual se atribui um significado. O termo código representa o conjunto de palavras-código que é associado a um conjunto de padrões.

Um conjunto de valores quantizados é representado pelos T elementos do vetor $y = [y_1, y_2, \ldots y_T]$ a figura 4.1. Supondo-se que cada elemento y_i possa assumir um

entre T padrões $\{w_1, w_2, \ldots, w_T\}$, a codificação define para cada y_i uma palavra-código v_i, que estabelece uma correspondência com o padrão assumido w_i.

Um código de tamanho fixo é constituido por palavras-código com um mesmo número de bits. Um código unicamente decodificável é aquele em que qualquer combinação de palavras só pode ser decodificada de uma maneira, sem ambigüidades. Assim, o código composto pelas palavras v_1 = "0", v_2 = "1", v_3 = "01", v_4 = "10" não é unicamente decodificável porque a seqüência de bits "0011" pode ser interpretada como a seqüência de palavras $v_1\ v_1\ v_2\ v_2$, ou $v_1\ v_3\ v_2$.

É desejável a utilização de um código com o menor comprimento médio possível. Uma vez que podem ser definidas S palavras de mesmo tamanho $b = \log_2 S$ bits, um código com b bits pode representar até 2^b valores de entrada. Esse código só é ótimo quando os padrões de entrada são equiprováveis, ou seja, têm sua probabilidade P:

$$P(w_1) = P(w_2) = \ldots = P(w_S) = 1/S$$

Para os casos em que as probabilidades diferem para cada w_i, utiliza-se palavras de tamanho variável, atribuindo as menores aos padrões mais prováveis, o que implicará na redução de bits gerados pela codificação. A técnica usada para construir códigos de menor comprimento médio é denominada codificação por entropia [Gonzales].

4.1.3 Otimização

O processo de otimização trata de utilizar técnicas de compressão de tamanho de código, para gerar um novo código mais eficiente e de menor tamanho para representar a informação original.

Sabe-se ainda que durante o processo de otimização de código pode existir a perda ou não de informação da imagem. Se durante a compressão dessa imagem ocorrer a perda de algum tipo de informação, dizemos que esse foi um processo de compressão com perdas. Por outro lado, se ao fazer a compressão da imagem todas as informações contidas em seus dados forem preservados, e conseqüentemente essa imagem pode ser recuperada sem nenhum tipo de distorção, dizemos que esse foi um processo de compressão sem perdas.

4.2 Técnicas de otimização para compressão de dados

As duas técnicas de compressão de dados apresentadas a seguir são consideradas clássicas, visto sua larga utilização na prática.

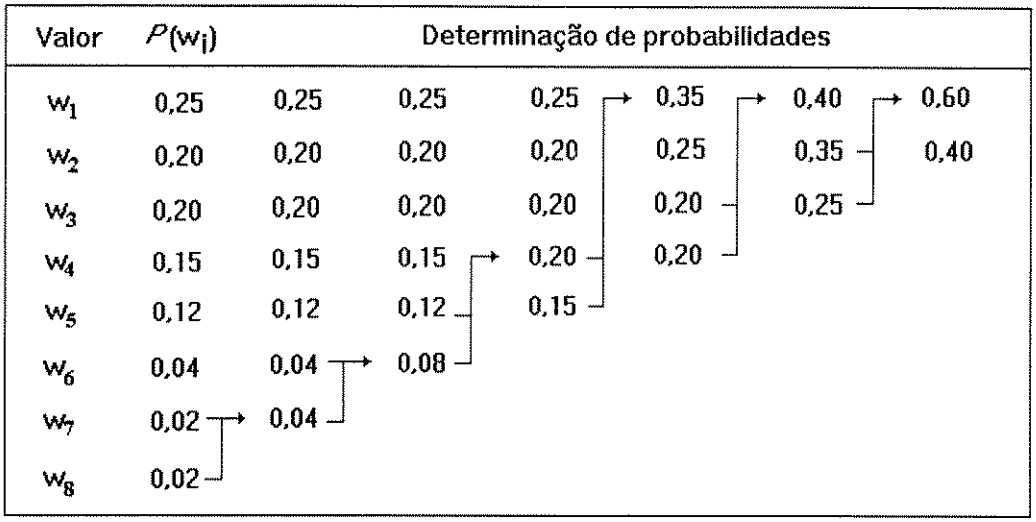
4.2.1 *Run Lenght Coding* - RLC

Esse é um dos mais antigos algoritmos de compressão de imagens. É muito aplicado para imagens binárias, embora também possa ser utilizado na otimização do código de imagens em níveis de cinza. Essa técnica não causa perda de informação.

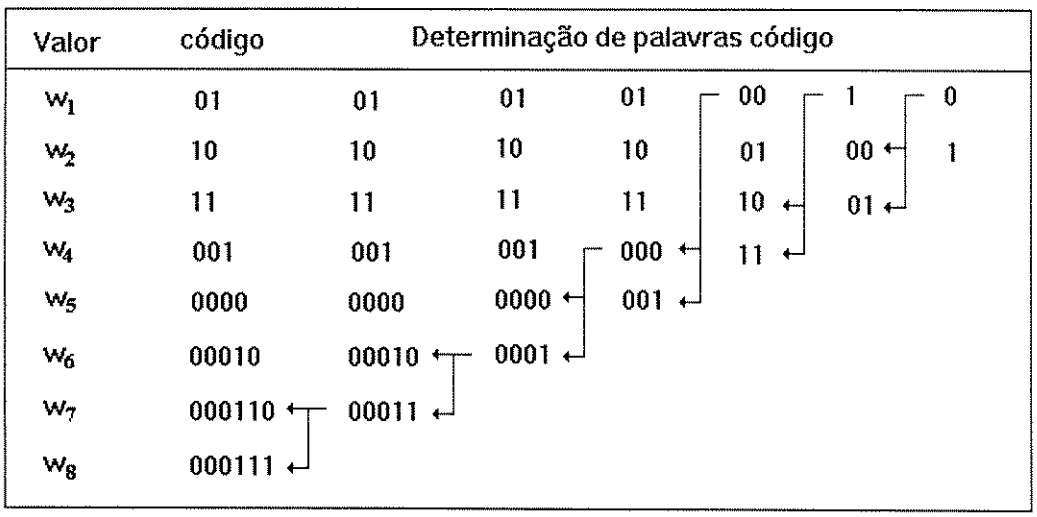
A RLC se baseia no fato de que imagens binárias são constituídas de seqüências alternadas de pixels brancos e pixels pretos. Assim, ao invés de se codificarem os pixels individualmente, codificam-se as quantidades de pixels brancos (ou pretos) de modo seqüencial. Ou seja, é uma técnica que tira proveito da repetição de pixels de um mesmo gênero, ao longo de uma porção da imagem. Na sua forma original, o código resultante da aplicação do *Run Lenght Coding* é constituído pelos pares de números, especificando duas informações: tipo de pixel e sua freqüência de repetição.

4.2.2 Codificação de Huffman

A codificação de Huffman é um método de codificação por entropia para geração de palavras-código unicamente decodificáveis, com uma taxa média mínima de bits para a representação da informação [Huffman].



a)



b)

Figura 4.2: Exemplo da determinação o código de Huffman.

O método para gerar o código de Huffman consiste na determinação das probabilidades $P(w_1)$, $P(w_2)$, . . . , $P(w_T)$, na seleção sucessiva do par de valores de menor magnitude, na aglutinação dos mesmos e na associação do novo valor gerado a um caminho dentro de uma árvore binária (figura 4.2.a). Ao final do processo, os caminhos definidos da raiz, até cada uma das folhas, determinarão as palavras-código para os padrões w_1, w_2,. . . ., w_T (figura 4.2.b). A figura 4.2 ilustra a geração das palavras-código para um universo de $S = 8$ padrões possíveis. O algoritmo descrito acima gera palavras de tamanho variável, associando os valores mais prováveis a palavras de menor tamanho.

Uma vez formado o código, sua decodificação é feita de forma única e sem perda de informação. Isso ocorre por que a seqüência de palavras-código pode ser apenas decodificada de uma única forma, através de um exame individual dessas palavras analisadas da esquerda para a direita. Para o código obtido da figura 4.2, a seqüência de bits 000111000100000011000111000110 mostra que a primeira palavra-código é 000111, a qual representa o padrão w_8. A próxima palavra-código válida é 00010, que corresponde ao padrão w_6. Prosseguindo o mesmo procedimento de mapeamento, obtemos a seguinte sequência de padrões: $w_8\, w_6\, w_5\, w_1\, w_2\, w_4\, w_3\, w_7$.

4.3 Descrição do método utilizado para compressão de imagens de assinaturas

O método destina-se a minimizar o tamanho dos arquivos gerados por imagens de assinaturas, reduzindo portanto a base de dados de nosso sistema, sem causar perda de informação.

Para atingir esse objetivo, propomos o seguinte procedimento: fazer o enquadramento da imagem, a codificação em blocos de 3 x 3 pixels, a eliminação de redundância de padrões utilizando a técnica RLC e, finalmente, utilizar o código de Huffman truncado em 32 palavras para chegar ao tamanho mínimo do arquivo da assinatura.

4.3.1 Aquisição e digitalização de assinaturas estáticas

Para o teste desse método foram utilizadas 250 assinaturas como amostras. Cada uma foi escrita numa área retangular de 10cm por 5cm, em folhas de papel de cor branca, utilizando-se caneta de tinta preta, como foi descrito na seção 3.2.

Uma vez que o objetivo da digitalização é capturar a imagem e transformá-la num registro que possa ser entendido pelo computador, o primeiro passo é digitalizar as assinaturas com base numa área fixa de 10cm por 5cm. Para tal processo foi utilizado um *scanner* de mesa de alta resolução, empregando-se 300 dpi.

4.3.2 Pré-processamento das imagens de assinaturas estáticas

O objetivo do pré-processamento das imagens de assinaturas é eliminar áreas que não trazem informação e assim conseguir uma redução do seu tamanho. A presente técnica consiste em enquadrar a assinatura com as coordenadas mais extremas que ainda contenham pelo menos um pixel preto [Searfoss].

As coordenadas que delimitam a área a ser enquadrada serão dadas por (X_{min}, Y_{min}) e (X_{max}, Y_{max}), obtidas da seguinte maneira:

$$X_{min} = \min \{ Lp \mid Lp \in I \}$$

$$Y_{min} = \min \{ Cp \mid Cp \in I \}$$

$$X_{max} = \max \{ Lp \mid Lp \in I \}$$

$$Y_{max} = \max \{ Cp \mid Cp \in I \}$$

onde:

Lp : Número da linha da imagem contendo pelo menos um pixel preto.

Cp : Número da coluna da imagem contendo pelo menos um pixel preto.

I : Área da imagem da assinatura estática original.

De posse desses dados, passamos a utilizar apenas a imagem que fica enquadrada por essas coordenadas, como pode ser visto nas figuras 4.3 e .4.4

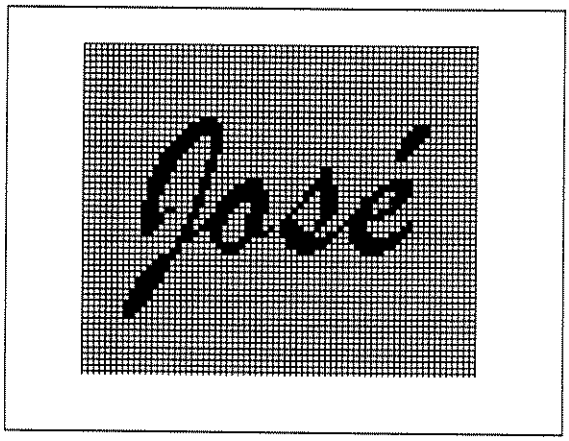


Figura 4.3: Imagem não enquadrada.

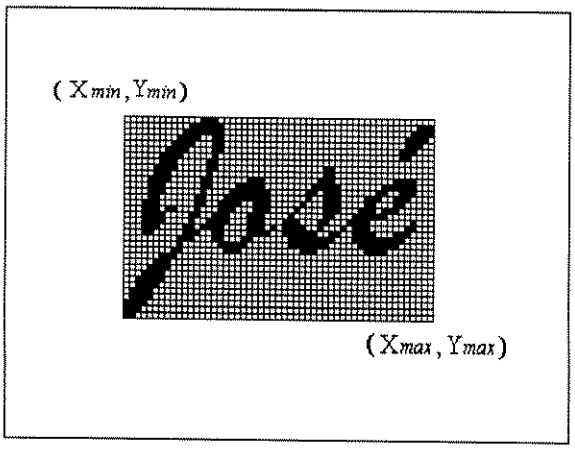


Figura 4.4: Imagem armazenada após enquadramento.

4.3.3 Codificação e representação dos padrões na imagem da assinatura estática

A codificação da imagem é feita dividindo-se a imagem em pequenos blocos de 3 por 3 pixels, como mostra a figura 4.5. A cada um desses blocos é associada uma palavra-código que representa um padrão. No caso do bloco a ser codificado não conter todos os 9 pixels, serão inseridos pixels brancos no lugar daqueles não existentes.

Na representação feita os pixels pretos são armazenados com o valor *0* e os pixels brancos com valor *1*. Por se tratar de blocos com 9 pixels - e cada pixel poder tomar o valor *0* ou *1* - obtemos um número máximo de 2^9 palavras, implicando em 512 tipos diferentes de padrões possíveis, começando em 0 e terminando em 511.

Na seqüência de bits gerados, o pixel mais significativo é o de número 1 e o menos significativo é o pixel número 9, conforme a figura 4.6.

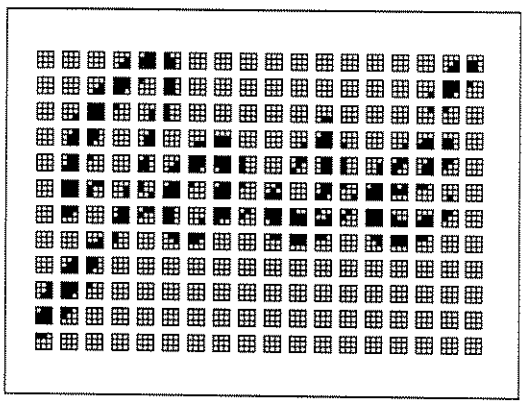


Figura 4.5: Imagem enquadrada e codificada em blocos 3 por 3 pixels.

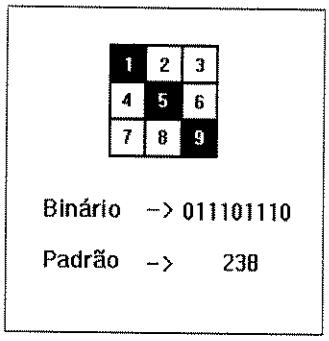


Figura 4.6: Representação utilizada para gerar as padrões compostos por 9 pixels

As vantagens de se fazer a codificação das imagens das assinaturas em blocos de 3 por 3 pixels são seguintes:

1. Na digitalização das assinaturas em 300 dpi, normalmente os traços feitos pela caneta ocupam blocos pretos de 3 por 3, ou 4 por 4 pixels. Após o processo de codificação,verifica-se a existência de grandes seqüências de blocos adjacentes, todos pretos ou todos brancos. Ou seja, se produz uma imagem codificada com alta redudância de dados.
2. Ao se empregar métodos de codificação por entropia, é desejável que os padrões a serem codificados sejam compostos de um grande número de bits (nossa representação utiliza 9 bits). Dessa forma, quando associarmos a esses padrões palavras-código de menor tamanho, a razão média de compressão entre o código original e o código otimizado se tornará maior.
3. Esse modelo de representação reduz a quantidade de informação processada e apresenta maior correlação entre os dados que são utilizados pelos algoritmos de reconhecimento de padrões.

Como resultado da codificação, o arquivo gerado nessa etapa do processo de compressão de imagens é composto de valores que variam entre 0 e 511.

4.3.4 Utilização do *Run Lenght Coding* para eliminação de redundância de blocos

De maneira geral as assinaturas possuem alguns traços representando o nome ou as iniciais do nome das pessoas, bem como outros traços estilizados para enfeitar e personalizar a assinatura. Assim, percebe-se que a imagem da assinatura que apresenta hastes ou laçadas, que se projetam para cima ou para baixo da sua linha de base, faz com que continuem aparecendo espaços em branco pela imagem, mesmo utilizando-se o enquadramento, como se vê na figura 4.7.

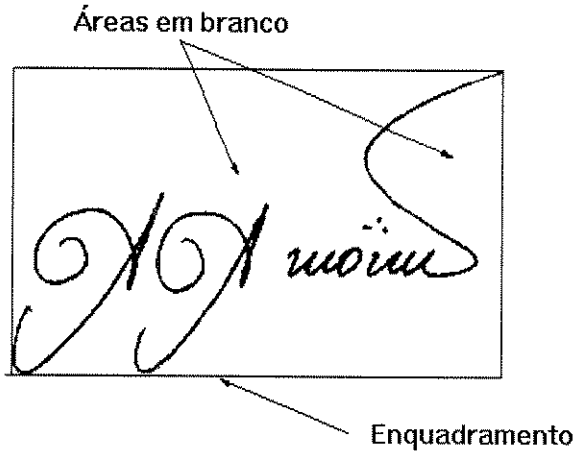


Figura 4.7: Grandes áreas em branco que podem aparecer após o enquadramento da imagem da assinatura.

Ao fazermos uma análise estatística sobre imagens codificadas pela técnica descrita na seção 4.3.3, verificamos que existem poucos padrões que aparecem com freqüência alta. Os restantes possuem freqüência muito baixa ou nula. Dos resultados obtidos, constamos que 81,42% das palavras-código referem-se ao padrão 511 (isto é, um bloco todo branco) e 6,51% das palavras-código se referem ao padrão 0 (um bloco todo preto). Os demais padrões apresentaram probabilidade abaixo de 0,01% ou zero.

Foi constatado ainda que tanto o padrão 511 como o padrão 0 não se apresentam de modo isolado. Ou seja, na maioria das vezes existe uma seqüência grande de padrões 511 um após o outro, e do mesmo jeito acontecendo com o padrão 0.

Ao identificarmos essas características nesse tipo de imagem, optamos por utilizar o *Run Lenght Coding* para eliminar a redundância de padrões. No entanto, para se conseguir o desempenho ótimo da presente técnica, resultando em maior número de padrões repetidos em seqüência, as palavras-código dos padrões da imagem são todas concatenadas uma após a outra no sentido horizontal.

Dessa maneira utilizamos um algoritmo que gera um código da seguinte forma: se o padrão que se está codificando for diferente de 511 ou 0, ele continua o mesmo. Por outro lado, se o padrão for igual a 511, o código resultante será o número de vezes que esse padrão se repete, seguido do próprio padrão. O mesmo acontece quando o padrão for igual a 0.

Por conseguinte, para uma seqüência de padrões 511, 511, 2, 5, 0, 0, 0, 0, 5, 5, 5, 511, obteremos como novo código 2, 511, 2, 5, 4, 0, 5, 5, 5, 1, 511. Como pode ser observado nesse exemplo, esse tipo de abordagem passa a ser vantajosa quando o número de vezes que o padrão se repete é maior ou igual a três. Caso contrário acontecerá um aumento no código da representação. Para o tipo de imagem com a qual estamos tratando esse fato acontece raramente, pois a seqüência de padrões 0 e 511 é muito freqüente e produz uma considerável redução de código.

Quanto ao número máximo de repetições possíveis para os padrões, utilizando-se nosso banco de dados foi verificado que, no caso extremo em que a assinatura chega a utilizar o espaço de 10cm por 5cm, existirão no máximo 394 padrões repetidos no sentido horizontal, ou seja, não se alcança um valor superior a 512. Portanto, as

palavras-código que irão representar o número de repetições do padrão também podem ser representadas por um código de 9 bits.

4.3.5 Redução final do tamanho do arquivo de imagem através do Código de Huffman truncado

Para essa fase do trabalho nosso método se serve do código de Huffman truncado em 32 palavras-código, as quais estão representadas na tabela 4.1, ao invés das 512 palavras-código que representariam o código completo [Gonzales]. A primeira palavra do código de Huffman gerado é definida como um prefixo. As 31 palavras-código restantes serão associadas aos 31 padrões de maior probabilidade, extraídos de uma nova análise estatística sobre o código das imagens conseguido pela técnica da seção 4.3.4. Os 31 padrões correspondem, em média, a mais de 85% do total de padrões existentes no arquivo. Os demais padrões são codificados anexando-se a palavra-código prefixo ao padrão do código original.

Pelo exemplo da seção 4.3.4 — onde temos uma seqüência de palavras-código que representam os padrões 2, 511, 2, 5, 5, 0, 5, 5, 5, 1, 511 —, sabemos que esses padrões ocupam um total de 99 bits. Podemos então encontrar o número de bits que a utilização do código de Huffman truncado viria a apresentar. Calculando a freqüência de cada um dos padrões, verificamos que existem cinco padrões 5, dois padrões 511, dois padrões 2, um padrão 1 e um único padrão 0. Empregando a tabela 4.1 e recodificando esses padrões através desse código, o novo tamanho seria de apenas 47 bits.

Palavra	Código
prefixo	100
1	111
2	0100
3	0101
4	0110
5	0111
6	1011
7	1100
8	00001
9	00010
10	00011
11	11010
12	11011
13	000001
14	001000
15	001010
16	001011
17	001100
18	001101
19	001110
20	001111
21	101000
22	101001
23	0000001
24	0010010
25	0010011
26	1010100
27	1010101
28	1010110
29	1010111
30	00000000
31	00000001

Tabela 4.1: Código de Huffman truncado em 32 palavras-código.

Na prática, as imagens de assinaturas possuem os 512 padrões para serem codificados. Portanto, para os 481 padrões restantes que representam aproximadamente 15% do total de padrões da imagem, a codificação é feita adicionando-se a palavra-código prefixo. Ou seja, para representar um desses padrões estamos utilizando 12 bits em vez de apenas 9. Isso parece uma contradição quando o que queremos é minimizar o tamanho da representação. O que nos levou a utilizar essa abordagem foram dois fatores:

1. Se fizéssemos a implementação do código de Huffman completo as próprias palavras-código que representariam estes padrões seriam do mesmo tamanho ou inclusive maiores que 12 bits.
2. O fato de utilizarmos o código truncado em 32 palavras implicaria apenas num aumento de 5% sobre o tamanho final do código, o que consideramos pouco diante da taxa de compressão obtida por esta técnica e sua facilidade de implementação.

4.4 Formato do arquivo gerado

O arquivo comprimido que é gerado por este método tem seus 62 primeiros bytes contendo os 31 padrões de maior probabilidade daquela imagem. Os dados a seguir são da imagem em si, sendo os dois primeiros o comprimento e altura da imagem, como apresentado na figura 4.8.

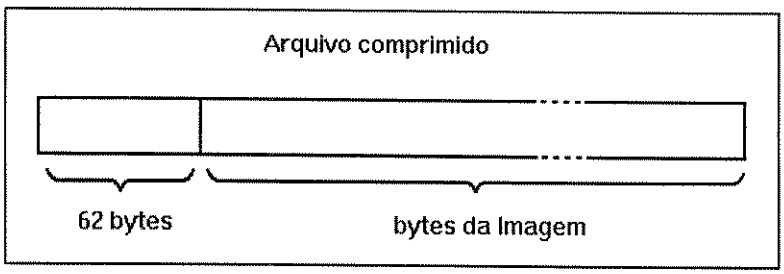


Figura 4.8: Modelo do arquivo comprimido.

Fica implícito que o codificador e o decodificador desse algoritmo precisam utilizar a tabela 4.1 para o mapeamento do arquivo, a fim de não ocorrer nenhum tipo de erro durante a recuperação do arquivo original.

É importante ressaltar também que esse é um método de compressão sem perdas. Isto é, no processo de compressão/descompressão nenhuma informação referente a assinatura é perdida. De fato a única diferença entre a imagem original e a imagem recuperada é que na primeira ainda existem áreas em branco que circundam a assinatura, às quais na prática não possuem nenhuma informação relevante.

Na figura 4.9 mostramos uma imagem original e a imagem que passou por um processo de compressão/descompressão através do método proposto. Observa-se que não existe diferença entre ambas imagens.

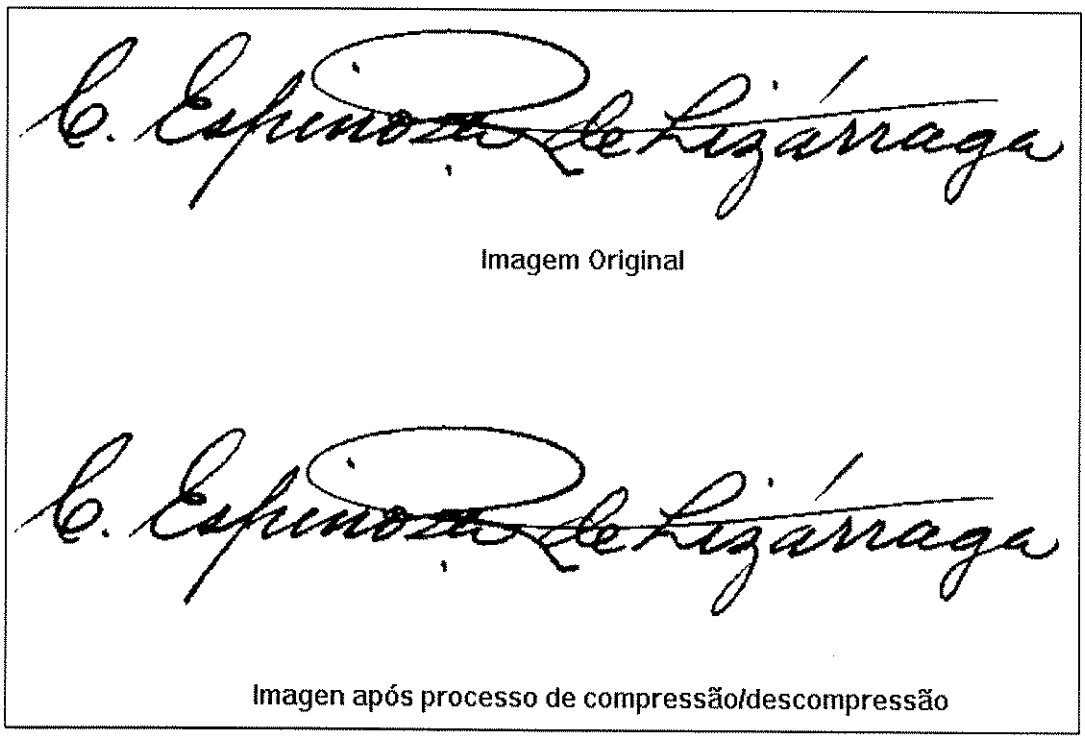


Figura 4.9: Imagem de uma assinatura original e uma assinatura que foi submetida ao processo de compressão/descompressão.

4.5 Análise do método proposto

Os resultados obtidos tomando a média das 250 assinaturas coletadas podem ser vistos na tabela 4.2, onde é mostrado o tamanho médio dos arquivos através das diferentes etapas do método.

	Tamanho médio dos arquivos
Imagem Inicial	90.000 bytes
Enquadramento	26.702 bytes
Redundância	5.553 bytes
Huffman	3.554 bytes

Tabela 4.2: Tamanho médio dos arquivos.

Para termos um parâmetro que permita a comparação entre os tamanhos dos arquivos comprimidos e não comprimidos, definimos como taxa de compressão de um arquivo da seguinte forma [Ranganathan]:

$$\frac{\text{tamanho do arquivo original} - \text{tamanho do arquivo comprimido}}{\text{tamanho do arquivo original}} * 100\%$$

Tomando como referência o tamanho médio do arquivo obtido com o enquadramento, foi conseguido uma taxa de compressão de 86,69%. Essa mesma taxa aumenta para 96,05% quando tomamos como referência o tamanho do arquivo da imagem inicial.

Para avaliar o desempenho do nosso método fizemos um enquadramento das imagens das assinaturas, a fim de retirar os espaços em branco que não contêm informação, e os transformamos em vários formatos de arquivos de imagem (ver tabela 4.3).

Tipos de arquivo de imagem	Tamanho médio dos arquivos
BMP	24.686 bytes
GIF	4.927 bytes
RLE	15.770 bytes
TIF	10.382 bytes
WPG	10.151 bytes
PIC	12.343 bytes
PCX	10.967 bytes

Tabela 4.3: Tamanho médio dos arquivos obtido por alguns tipos de arquivos de imagens.

Constatamos que o menor tamanho médio dos arquivos apresentados foi do tipo GIF, ocupando um espaço de 4.927 bytes. Em comparação com o resultado obtido por nosso método, que é de apenas 3.554 bytes, consegue-se em média uma economia de 27,87% no código a ser armazenado pelas imagens das assinaturas.

A taxa de compressão média máxima obtida é de 96,05%, tendo-se como referência o tamanho do arquivo da imagem inicial. A taxa de compressão média mínima obtida é de 27,87% quando tomamos como referência o tamanho médio dos arquivos de imagens do tipo GIF.

O método foi idealizado para a compressão de imagens de assinaturas visando à sua utilização dentro de um sistema de identificação pessoal. Esse método, porém, pode ser aplicado para qualquer outra finalidade, desde que as imagens que se deseja compactar tenham características semelhantes às assinaturas. Isto é, imagens em preto

e branco onde o número de pixels brancos seja muito superior ao de pixels pretos. Alguns exemplos de imagens que possuem estas características são manuscritos, textos e desenhos.

Capítulo 5

Sistemas de Verificação de Assinaturas

Os sistemas de verificação de assinaturas têm por objetivo determinar se uma assinatura é verdadeira ou falsa. Apesar da aparente simplicidade associada ao fato de se trabalhar apenas com essas duas alternativas, a verificação de assinaturas não pode ser considerada como um problema trivial [Duda]. A principal razão é a variabilidade que existe entre as assinaturas de uma mesma pessoa, tanto por influências de fatores internos quanto de fatores externos. Isso gera uma grande proximidade entre as assinaturas que se deseja classificar (amostras verdadeiras e falsas), exigindo que os classificadores considerem sutis diferenças no processo de separação das duas classes.

5.1 Histórico da detecção de falsificações

A existência de fraudes remonta a épocas muito antigas, conforme atestam fatos e escritores. Champollion já as constatara em textos hieroglíficos, produzidos por generais egípcios. Na Antigüidade, o escritor Quintiliano publicou por volta do ano 94 d.C., algumas normas para apuração da falsidade de documentos. Tal fato prova que já naquela época existia um número de fraudes suficiente para causar preocupação.

Da constatação das primeiras fraudes da escrita e da conseqüente necessidade de prevení-las e reprimí-las surgiu a grafoscopia. A grafoscopia é a técnica que visa verificar a autenticidade de escrituras ou determinar sua autoria, através do estudo das características referentes à maneira como as letras foram escritas.

Mais recentemente, a grafoscopia foi utilizada para verificar a autenticidade de uma assinatura, através de um estudo criterioso na regularidade de sua inclinação, da amplitude de seus laços, da presença ou da ausência de traços estilísticos, da direção da escrita da caneta, de interseções entre os diferentes traços e inclusive da inspeção microscópica dos elementos da tinta.

Embora as características da escrita fossem bem definidas e facilmente identificáveis, a avaliação da escrita só podia ser confiada a um especialista. Esse, no entanto, realizava um trabalho subjetivo baseado na sua experiência.

No início dos anos 60, dois fatores aumentaram o interesse em se desenvolver novos métodos e tecnologias na área. O primeiro, o fato de o computador se tornar uma ferramenta de pesquisa, possibilitando a implementação dos algoritmos desenvolvidos na área de reconhecimento de padrões. O segundo vem dos avanços da eletrônica na área médica, onde se começou a fazer pesquisas em biodinâmica envolvendo a produção dos manuscritos [Wilkinson].

5.2 Parâmetros de desempenho de um sistema de verificação

Para permitir a análise comparativa do desempenho de sistemas de verificação de assinaturas e tentar uniformizar a apresentação de seus resultados, pesquisadores têm utilizado a curva característica de operação de receptor (COR). A seguir apresentaremos uma breve descrição da COR, representada na figura 5.1.

O eixo horizontal da COR indica o erro tipo I ou de falsa rejeição, que é a probabilidade do sistema incorretamente indicar que uma assinatura é falsa, quando de fato é verdadeira. O eixo vertical representa o erro tipo II ou de falsa detecção, que é a

probabilidade do sistema incorretamente indicar que uma assinatura é verdadeira, quando de fato é falsa.

São três os pontos mais importante na curva COR:

1. O ponto onde o erro tipo I e o erro tipo II são iguais é denominado de taxa de erros iguais. Essa taxa de erro indica a separabilidade que o sistema oferece entre as assinaturas autênticas e falsas (vide ponto *a* na figura 5.1).
2. O ponto de menor valor do erro tipo II com erro tipo I igual a zero, indica a probabilidade de incorretamente o sistema aceitar assinaturas verdadeiras como sendo falsas, quando todas as assinaturas falsas são detectadas (veja ponto *b* na figura 5.1).
3. O ponto de menor valor do erro tipo I com erro tipo II igual a zero, indica a probabilidade de incorretamente o sistema aceitar assinaturas falsas como sendo verdadeiras, quando todas as assinaturas verdadeiras são detectadas (veja ponto *c* na figura 5.1).

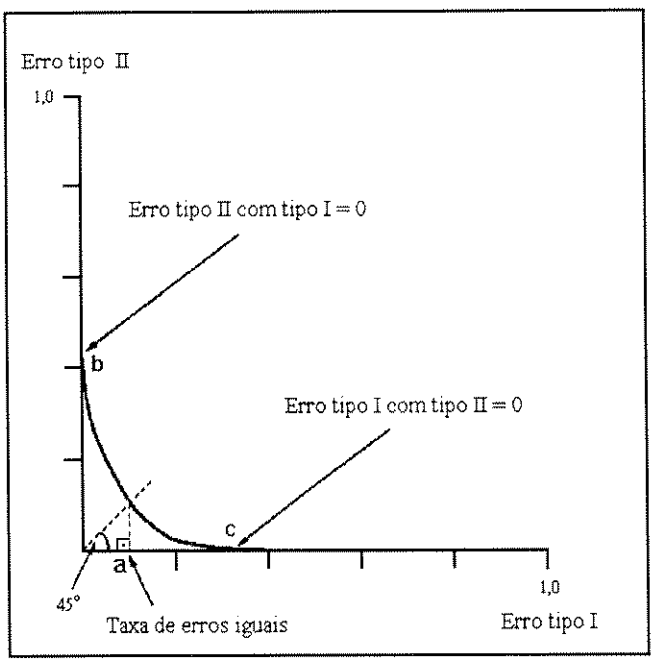


Figura 5.1: Exemplo da curva COR.

No caso ideal, a COR passa pela origem do eixo de coordenadas. Ou seja, os erros de falsa rejeição e de falsa detecção são iguais a zero. Na prática, o objetivo dos sistemas de verificação de assinaturas é minimizar esses três parâmetros de erro, utilizando os mais variados tipos de técnicas.

5.3 Sistemas de verificação de assinaturas dinâmicas

Os métodos de verificação de assinaturas dinâmicas são aqueles que envolvem medidas de várias características de uma assinatura, na hora em que ela está sendo realizada. Uma configuração típica de um sistema de aquisição de assinatura dinâmica é mostrada na figura 5.2.

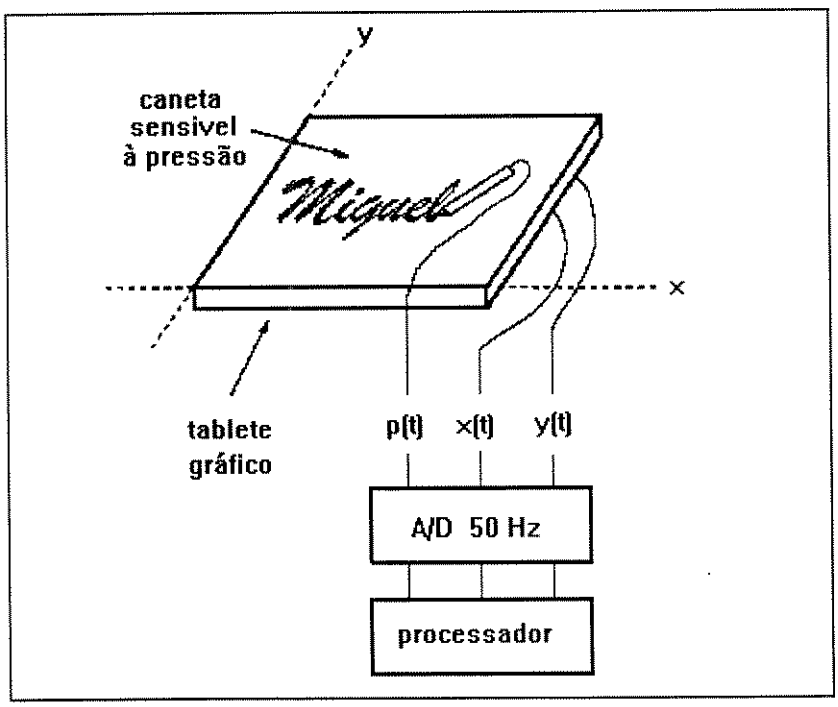


Figura 5.2: Configuração típica de um sistema de aquisição dinâmico de assinaturas.

Geralmente esses sistemas possuem um digitalizador que fornece como saída a posição da caneta em relação a um eixo de coordernadas. A caneta, por sua vez, pode ser sensível à pressão que exerce sobre o equipamento chamado tablete gráfico. Ela pode ainda ser equipada com um dispositivo capaz de fornecer outros tipos de dados dinâmicos, como a magnitude da velocidade e a aceleração. Os dados adquiridos por esses sistemas geralmente são amostrados através de um conversor Analógico/Digital com uma taxa entre 50 e 200 Hz, para depois serem armazenados e analisados [Leclerc][Plamondon].

As técnicas de verificação de assinaturas dinâmicas esbarram num problema principal, que é a maneira como seus dados de entrada são adquiridos. Nesses sistemas o indivíduo é obrigado a ter que assinar sobre o tablete gráfico, o que muitas vezes já implica num grande fator externo de interferência. Por esta razão, a implementação prática desses sistemas *on-line* tem se limitado em pequena escala a aplicações ligadas a segurança, como o *login* de identificação numa rede de computadores, entre outros exemplos.

Por outro lado, as técnicas de verificação de assinaturas estáticas são aquelas que envolvem apenas a imagem da assinatura. Nesse caso, o indivíduo que assina utiliza a sua própria caneta e se acomoda da melhor maneira que lhe convier para reproduzir sua assinatura. A aquisição dos dados dessa imagem pode ser feita de forma descentralizada e só depois ser processada por um servidor central, cabendo a ele tomar a decisão da autenticidade ou não dessa assinatura.

5.4 Métodos de verificação de assinaturas estáticas

Problemas com verificação de assinaturas estáticas são, de um modo geral, mais complicados de se resolver do que os problemas apresentados nos sistemas dinâmicos, pelo simples motivo de que a imagem de uma assinatura pode ser facilmente copiada.

Além disso, a informação dinâmica que pode ser extraída da imagem fica altamente degradada numa amostra estática. Parte dessa informação pode ser recuperada utilizando-se técnicas bastante específicas quando o processo de verificação é manual, mas a maioria desses métodos não pode ser implementada facilmente no computador.

O principal objetivo de um sistema automático de verificação de assinaturas estáticas é possibilitar que o computador assemelhe a capacidade humana de fazer a identificação e extração de características existentes na imagem de uma assinatura, bem como mediante a comparação dessas características com um banco de dados, poder concluir sua autenticidade.

Assim, o sistema automático de verificação de assinaturas deve ser capaz de exibir certas características como:

- Habilidade de extrair informação pertinente sobre detalhes da imagem.
- Capacidade de aprender a partir de exemplos.
- Habilidade de fazer inferência a partir dessas informações.

Um modelo geral de sistema de verificação de assinaturas está representado na figura 5.3.

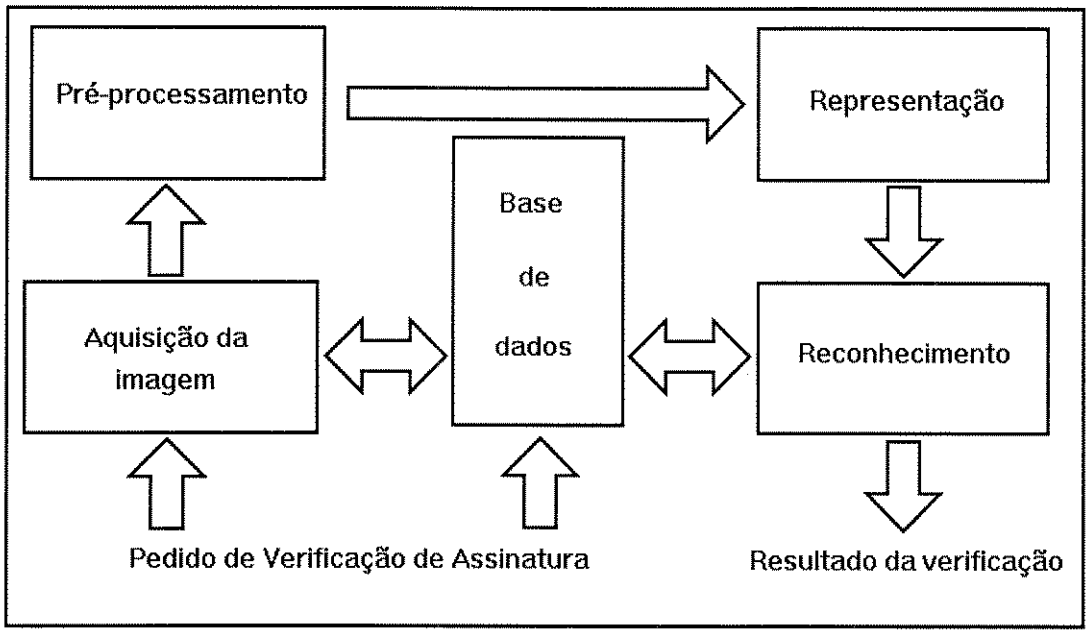


Figura 5.3 Modelo geral de um sistema de verificação de assinaturas.

Tomando como base o modelo da figura 5.3, observamos que esse é composto de cinco blocos básicos:

1. Aquisição da imagem
2. Pré-processamento
3. Representação
4. Reconhecimento
5. Base de dados

A unidade de aquisição da imagem executa a operação de digitalização da imagem diretamente através de um *scanner* ou ainda, recebe diretamente uma imagem que está contida na base de dados. A unidade de pré-processamento recebe esta imagem digital para passar por processos de filtragens, de segmentação e de normalização de tamanho. A unidade de representação é aquela encarregada de extrair as características da assinaturas, construindo um vetor de características para a imagem da assinatura que está sendo analisada. A unidade de reconhecimento é aquela que executa o processo de

classificação da assinatura como sendo falsa ou verdadeira, através da comparação entre o vetor de características fornecido pela unidade de representação e a base de dados. Finalmente, a unidade de base de dados contém informações sobre as assinaturas de referência dos escritores e outros dados relativos.

Como pode ser visto da figura 5.3, a entrada do sistema é um pedido de verificação de uma assinatura, no qual deve constar necessariamente o número de identificação ou o próprio nome do indivíduo a quem ela é atribuída, para assim poder localizar as suas informações de referência junto à base de dados. Sem esses dados o sistema teria que fazer o reconhecimento da assinatura comparando-a uma a uma, entre todas as assinaturas da base de dados, o que não é um processo desejável do ponto de vista de uma aplicação em tempo real. Como resultado desse pedido, obtemos na saída do sistema a indicação de que a assinatura em questão foi considerada verdadeira ou falsa.

Como em qualquer sistema autônomo de reconhecimento de padrões, um sistema de verificação precisa adquirir algum conhecimento sobre as assinaturas verdadeiras de seus escritores, antes de poder executar sua tarefa. Tal processo de aquisição de conhecimento é executado durante a fase chamada de treinamento.

Na fase de treinamento, um certo número de assinaturas verdadeiras é utilizado para gerar um vetor de características, que contém a média de cada uma das características que se definiu extrair da assinatura. Somente depois que esses dados são computados o sistema poderá ser colocado em operação. Então, quando uma assinatura desconhecida é apresentada, é exigido que o sistema determine a sua autenticidade ou não, através de um processo de comparação.

5.4.1. Aquisição da imagem

Os aparelhos mais comuns usados para aquisição de imagens são o *scanner* e câmeras de vídeo CCD. A aquisição da imagem consiste em transformar a imagem existente num documento em imagem digital. Pode-se considerar uma imagem digital como a matriz cujos índices de linhas e colunas identificam um ponto da imagem, enquanto cada elemento da matriz identifica o nível de cinza naquele ponto.

5.4.2. Pré-processamento

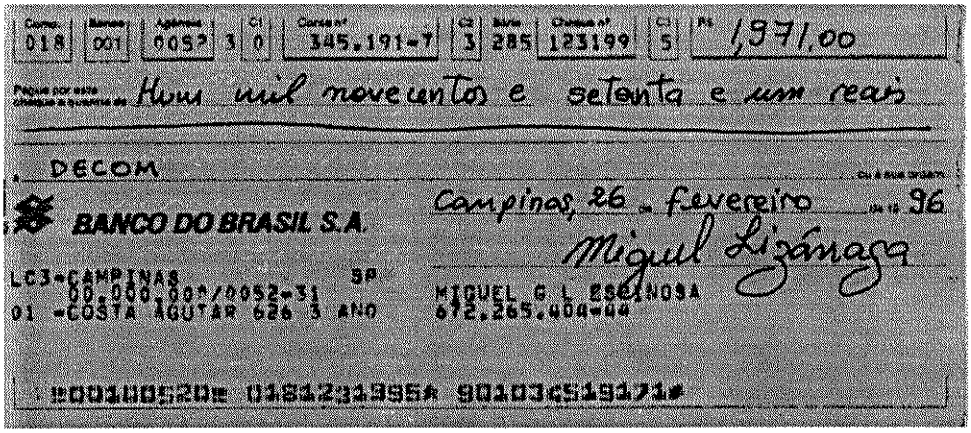
A etapa de pré-processamento se ocupa em obter a imagem da assinatura livre do fundo em que ela está contida.

No caso específico de um cheque bancário, quando o preenchemos realizamos três operações: adicionamos o valor do cheque em algarismo e por extenso, escrevemos a data em que se está preenchendo o cheque e, finalmente, colocamos nossa assinatura. Assim, esse documento uma vez preenchido consta da fusão de dois tipos de dados: a informação que vem impressa previamente no cheque, a qual chamaremos de fundo, e a informação referente ao ato do preenchimento do cheque.

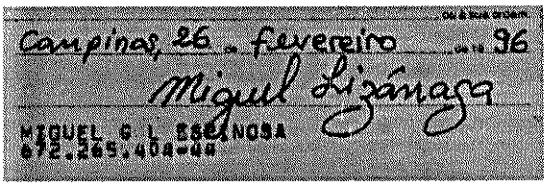
Nesse contexto, o pré-processamento tem por objetivo extrair a imagem da assinatura do fundo em que está contida e transformá-la numa imagem binária, onde os pixels pretos representariam a assinatura propriamente dita e os pixels brancos pertenceriam ao fundo.

Para chegar a esse ponto a imagem do documento passa pelas seguintes etapas: localização, segmentação, filtragem e normalização de tamanho. A figura 5.4 ilustra o resultado de cada uma destas etapas, utilizando como exemplo um cheque bancário.

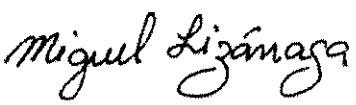
Imagem de entrada



Localização



Segmentação e Filtragem



Normalização

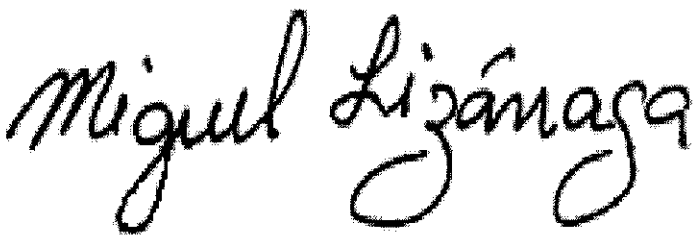


Figura 5.4: Operações da fase de pré-processamento.

5.4.2.1 Localização

Nessa operação se executa a extração da imagem da assinatura. O mesmo processo também pode ser usado para localizar outras regiões de interesse da imagem. No caso específico de cheques bancários, existe uma padronização para as áreas que serão preenchidas manualmente no cheque. Como conseqüência, é possível definir as diferentes áreas que irão conter a informação da assinatura ou ainda o número do banco, o número do cheque, do CIC, o nome do correntista etc.

A região mais importante a ser extraída num sistema automático de verificação é a da assinatura, mas extrai-se também a do nome do correntista ou do número do CIC para incrementar a informação referente ao pedido de verificação.

5.4.2.2 Segmentação

A segmentação é a operação que separa a assinatura propriamente dita do fundo da região em que ela está contida. O método mais comum utilizado para tal propósito é o de limiarização. Esse método transforma a imagem original em níveis de cinza numa imagem binária, através de um mapeamento dos seus pixels, utilizando uma função do tipo degrau, como ilustra a figura 5.5. Todos os pixels que ultrapassarem o valor de limiar L são mapeados para a imagem de saída com o valor *1*. Aqueles com valor abaixo do valor de limiar são mapeados com o valor *0*. Nas imagens binárias, os pixels de valor *1* representam o fundo e os pixels de valor *0* representam a assinatura.

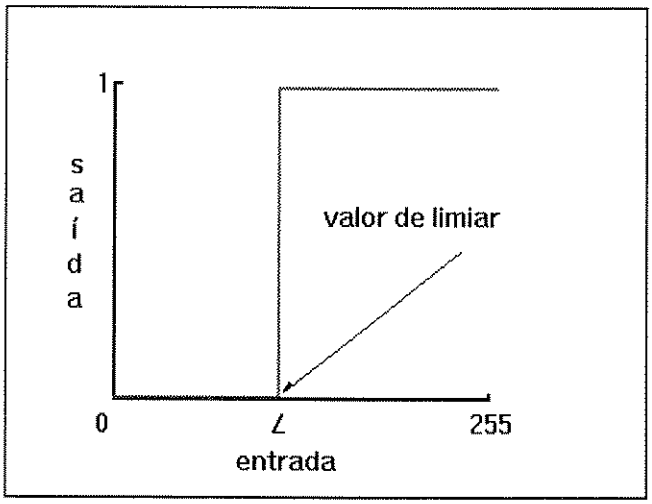


Figura 5.5: Função de mapeamento tipo degrau.

Esse método funciona bem quando a intensidade em níveis de cinza dos pixels pertencentes ao fundo da imagem forem sensivelmente mais claros ou mais escuros do que o valor dos pixels da assinatura. No caso da assinatura num cheque, observa-se que geralmente o fundo do mesmo está preenchido pelo logotipo do banco a que pertence. Ao se fazer a digitalização desse cheque, o fundo toma valores de pixels próximos aos da assinatura. Assim, uma simples limiarização dessa imagem resultlará numa mancha preta ao invés da imagem da assinatura [Ammar86][Weszka].

Para minimizar este efeito, Yoshimura desenvolveu um método que consiste basicamente da subtração entre a imagem de um cheque não preenchido com a imagem de um cheque preenchido, resultando numa imagem em que aparecem apenas os traços que foram feitos com a caneta [Yoshimura]. O método de Yoshimura para segmentação da assinatura compreende, primeiro, em fazer um ajuste no sentido horizontal e vertical entre o cheque preenchido e o cheque não preenchido, a fim de se conseguir o melhor casamento entre o fundo de ambas as imagens. A seguir, na imagem do cheque não preenchido é passado um filtro. Esse filtro faz com que certas porções da imagem que

contenham letras, linhas e números fiquem escuras, e o restante do cheque fique claro. O histograma da imagem filtrada se caracteriza por ter aproximadamente a aparência ilustrada na figura 5.6. Aproveitando a forma bimodal desse histograma, Yoshimura define um valor de limiar C_b que se encontra no mínimo dos dois modos. Os valores de pixels menores que C_b passam a ser iguais a *0*, enquanto os valores maiores ou iguais a C_b são iguais a *1*.

A eliminação do fundo da imagem do cheque que contém a assinatura é feita através da diferença entre a imagem filtrada e imagem do cheque não preenchida.

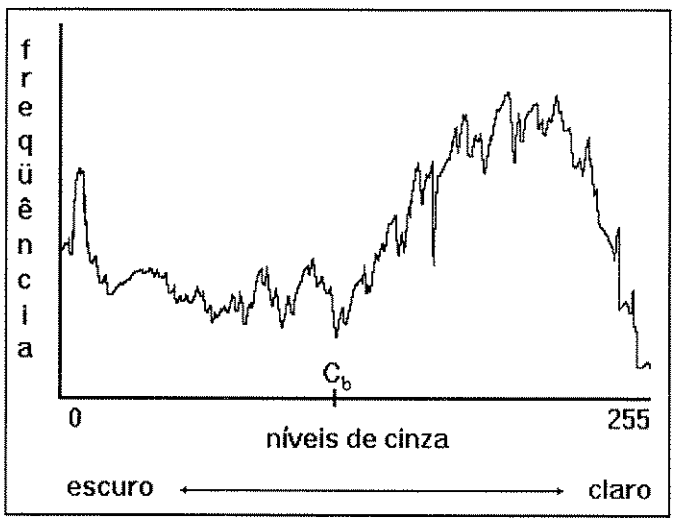


Figura 5.6: Histograma bimodal.

5.4.2.3 Normalização de tamanho

Esse é um processo de transformação que muda basicamente o tamanho original da imagem. Ele pode também mudar sua orientação ou posição, dessa forma alterando as características geométricas originais da imagem.

A normalização de tamanho da assinatura tem por objetivo estabelecer um tamanho padrão para as assinaturas e dessa forma facilitar a sua comparação.

Nemceck normalizou as imagens das assinaturas para enquadrá-las numa área retangular de 256 pixels por 128 pixels [Nemceck]. Pender utilizou uma técnica de redução de resolução para enquadrar as imagens das assinaturas em uma área retangular de 128 pixels x 64 pixels [Pender]. Wilkinson fez uma redução das imagens para serem enquadradas num retângulo de 256 pixels por 128 pixels [Wilkinson].

5.4.3 Representação

A representação da assinatura envolve a extração de propriedades da imagem ou ainda a relação existente entre partes da mesma. Cada uma dessas propriedades, ou relações, é chamada de característica. O conjunto das características extraídas de cada assinatura é denominado como vetor de características.

O processo de representação de uma assinatura na maioria das vezes não é reversível. Isto é, a assinatura não pode ser reconstruída a partir do seu vetor de características. Por exemplo, se o vetor de características envolve apenas dados da proporção entre as componentes contextuais da assinatura, a reconstrução não é possível. Por outro lado, quando é utilizado algum tipo de transformação de imagem, como a transformada de Fourier ou Hadamard, e os coeficientes dessas transformadas são utilizados para compor o vetor de características, a reconstrução da imagem original pode ser feita a partir desses dados.

A abordagem da representação da assinatura adotada por pesquisadores no campo da verificação de assinaturas, é caracterizada como sendo global ou local [Qi]. A representação global é conveniente quando se estuda as características da imagem da assinatura como um todo. Um exemplo de tal abordagem é o uso dos coeficientes da transformada de uma imagem ou ainda a média da inclinação de vários segmentos da

assinatura. A representação local é conveniente quando se requer um detalhamento maior entre os componentes da assinatura. Nesse caso geralmente a assinatura é dividida em regiões onde são extraídas características referentes apenas àquela região, independentemente do contexto geral da imagem.

Numa abordagem global, Ammar formou seu vetor de características com a inclinação e a razão existente entre o comprimento e a altura da assinatura, assim como a razão entre suas zonas alta, média e baixa [Ammar90][Powalka]. Uma ilustração das diferentes zonas em que Ammar dividiu uma assinatura está mostrada na figura 5.7.b.

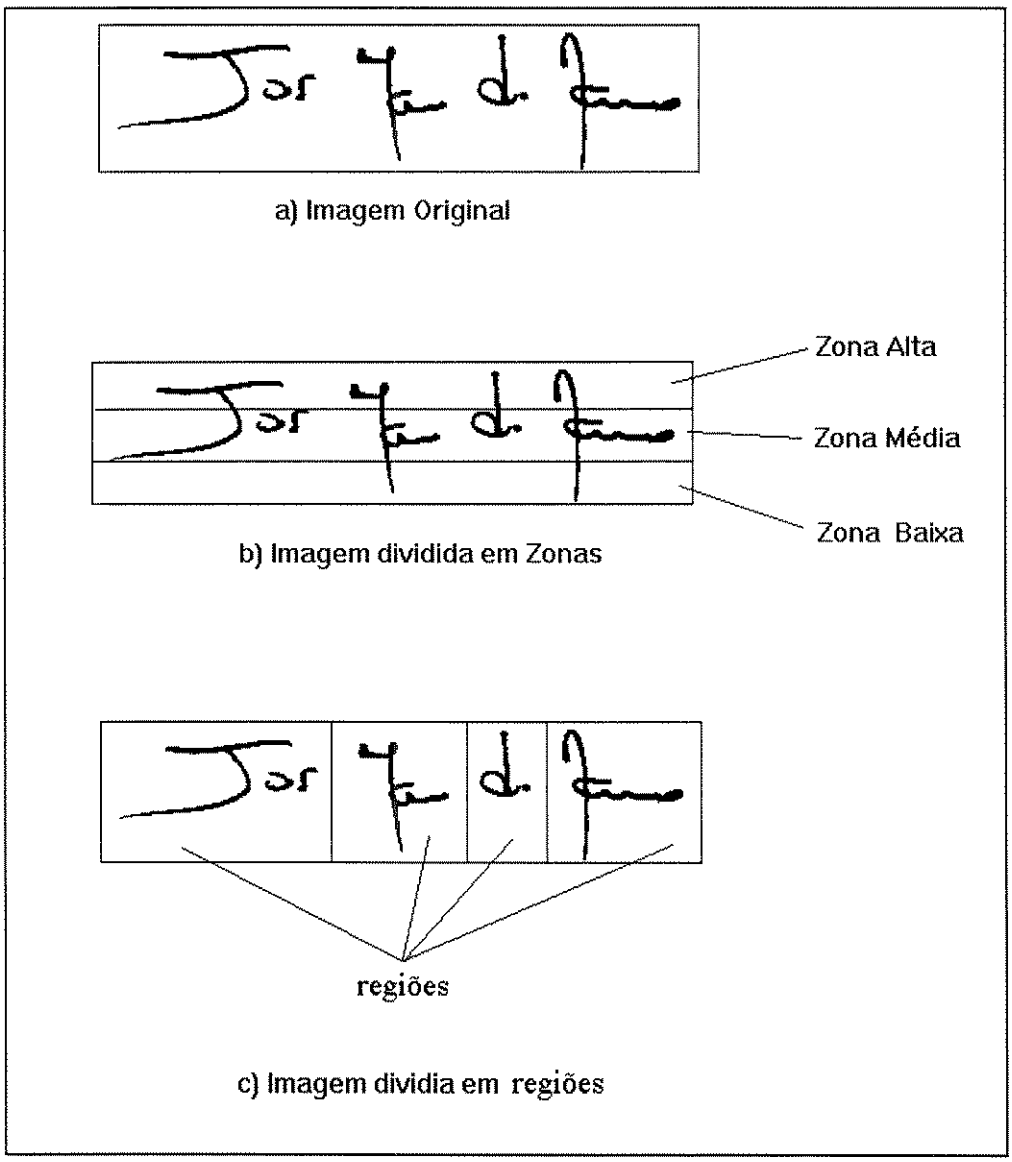


Figura 5.7: Imagem dividida em zonas e regiões.

Na abordagem local, ele tomou o cuidado de dividir a imagem da assinatura em regiões, cada uma geralmente constituída por uma palavra (ver figura 5.7.c). A partir daí extraiu as características para cada uma delas.

De maneira semelhante a Ammar, Nagel também dividiu a imagem da assinatura em zonas alta, média e baixa [Nagel]. Dessa forma conseguiu diferenciar as letras que possuem hastes para cima (como as letras *t* e *d*) e as letras que tem hastes que se projetam para baixo (assim como as letras *j* e *g*). Definiu como letras longas aquelas que extrapolam a zona média e como letras curtas aquelas que estão todas contidas na zona média. Para poder facilitar esse reconhecimento, o autor recorreu as informações contidas na sua base de dados.

Na abordagem global, o autor extraiu a proporção entre o comprimento total da assinatura e altura das letras longas, bem como a proporção entre o comprimento total da assinatura e a altura das letras curtas. Na abordagem local foi utilizada a proporção entre a altura de uma letra longa com a altura da letra curta que lhe segue, bem como a inclinação das letras longas.

Nemcek utilizou a transformada de Hadamard como meio para extrair as características da imagem [Nemcek]. Ao contrário de Ammar e Nagel, este método não depende de nenhuma informação contextual que deve ser conhecida sobre a assinatura. Nessa implementação, cada um dos coeficientes da transformação de Hadamard é uma das características que representa essa imagem.

Brocklehurst utilizou um método de descrição de assinatura cujas características extraídas são o comprimento global da assinatura, a distância existente entre o ponto inicial no qual a assinatura começa a ser escrita e a área designada a ela, a inclinação do traço e a concavidade [Brocklehurst].

No caso de Pender, as características extraídas da imagem para formar o vetor de características são, na verdade, uma matriz formada por todos os pixels pertencentes à imagem da assinatura.

5.4.4 Reconhecimento

O processo de reconhecimento consiste em classificar, através do seu vetor de características, se a assinatura é verdadeira ou falsa. Ou seja, nos deparamos com um problema de classificação de apenas dois padrões, um deles sendo as assinaturas verdadeiras e o outro, qualquer conjunto que não tenha as características da assinatura genuína.

No caso ideal, as assinaturas verdadeiras e as falsas estariam muito bem definidas e poderiam ser separadas em duas classes. Uma ilustração desse comportamento pode ser vista na figura 5.8a.

Na prática — devido à própria variabilidade que existe numa mesma assinatura, assim como a habilidade que pessoas têm de falsificar assinaturas —, os vetores de características das assinaturas verdadeiras e falsas podem chegar a valores muito próximos. Porém, dependo do limiar que se escolha para a classificação das assinaturas, poderá ocorrer um erro de classificação.

No exemplo da figura 5.8b, aparece um conjunto que é composto de uma superposição de assinaturas verdadeiras e falsificações. Para o limiar utilizado nessa figura, a porção esquerda desse conjunto contém assinaturas verdadeiras corretamente classificadas, mas também assinaturas falsas, as quais representam o erro tipo II. A porção direita do conjunto contém assinaturas falsas corretamente classificadas e também assinaturas verdadeiras, as quais representam o erro tipo I.

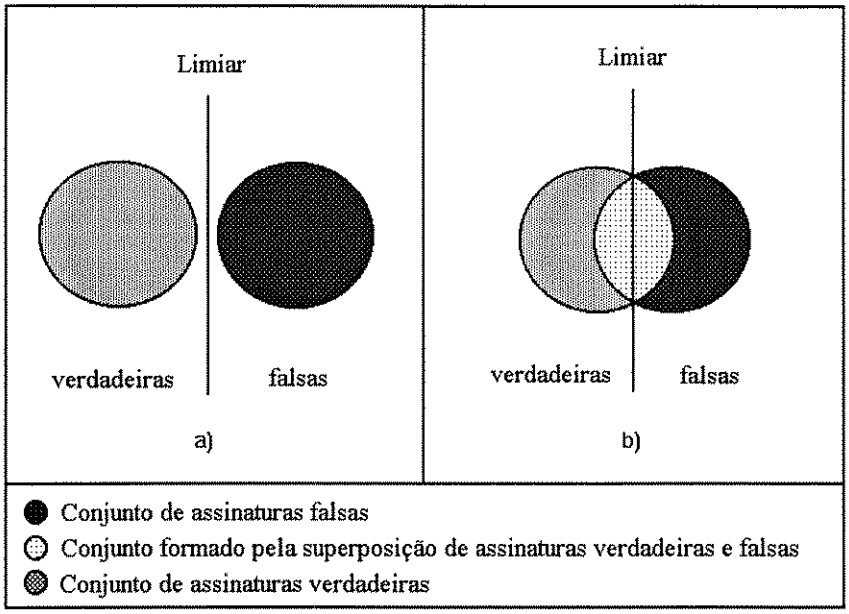


Figura 5.8:Classificação de assinaturas.

A tabela 5.1 mostra os resultados obtidos por vários pesquisadores na área de verificação *off-line* de assinaturas [Plamondon][Leclerc].

Pesquisador	Erro Tipo I	Erro Tipo II	Erros iguais
Chuang (1977)	20 %	20 %	-
Nagel (1977)	12 %	0 %	-
Ammar (1986)	6 %	4 %	-
Martins (1995)	21 %	29 %	-
Qi (1994)	0 %	0 %	0 %
Wilkinson (1990)	-	-	7 %
Pender (1991)	-	-	3 %
Cardot (1994)	2 %	4 %	-
Yoshimura (1994)	-	-	13 %

Tabela 5.1:Resultados de sistemas de verificação *off-line*.

- = dado não diponível.

Capítulo 6

Morfologia Matemática

Dentro do nosso sistema de verificação de assinaturas, nos servimos de propriedades que provêm da Morfologia Matemática para extrair o vetor de características das assinaturas. Por este motivo decidimos dedicar esse capítulo para uma breve introdução sobre os conceitos e as propriedades básicas dessa ferramenta.

6.1 Histórico da morfologia matemática

Por volta do ano de 1964, na *École Nationale Supérieure des Mines* de Paris, George Matheron e Jean Serra decidiram experimentar uma abordagem singular para resolver problemas de análise de imagens: extrair informações de imagens a partir de transformações de formas, realizadas através de duas transformações elementares que eles denominaram como dilatação e erosão [Serra]. As transformações produzidas pelas dilatações e erosões em imagens binárias são dependentes de pequenas imagens com padrões pré-definidos, os quais foram chamados de elementos estruturantes.

A palavra morfologia provém do grego, onde *morfo* significa forma e *logia* significa estudo. Portanto, morfologia matemática (MM) é o estudo das formas de uma imagem através da sua análise matemática. Com esse instrumento muitos problemas práticos de análise de imagens foram resolvidos, o que motivou um grande impulso nessa área de pesquisa.

As bases teóricas da MM para imagens binárias foram formalizadas pelos próprios Serra e Matheron nos primeiros anos de sua pesquisa. Estudando as

dilatações e as erosões, eles descobriram uma coleção de propriedades interessantes e chegaram ao seguinte resultado: as dilatações e as erosões são os elementos fundamentais para construir uma ampla classe de operadores, todos eles derivados das composições desses dois.

Posteriormente, essas idéias estabelecidas para imagens binárias foram estendidas para operadores sobre imagens em níveis de cinza.

6.2 Álgebra e imagens binárias na MM

Em análise de imagens, os objetos mais simples que manipulamos são as imagens binárias. Essas imagens são representadas matematicamente por subconjuntos ou, de maneira equivalente, por funções binárias.

Seja E um conjunto não vazio. Um elemento genérico de E é denotado por a, Temos então $a \in E$. Uma subconjunto de E é denotado genericamente por A. A coleção de todos os subconjuntos de E é denotada por Q. Temos então $A \in Q(E)$

Definição 6.1 (Função Binária) - Uma função binária definida sobre E é um mapeamento de E em $\{0,1\}$, isto é, para cada elemento de E, a função binária toma um único valor *0* ou *1*.

Uma função binária definida em E é denotada genericamente por $f : E \rightarrow \{0,1\}$. Denota-se por $f(a)$ o elemento de $\{0,1\}$ associado ao ponto a de E através de f. O conhecimento de $f(a)$, para todo a em E, define a função f que passa então a ser denotada por $f: a \mapsto f(a)$.

O gráfico de uma função é o conjunto de todos os pares $(a, f(a))$. O gráfico de uma função f indica qual o valor tomado por f em cada ponto a de E. A figura 6.1 mostra o gráfico de uma função binária f particular

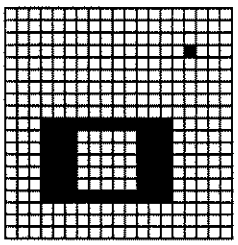


Figura 6.1: Uma função particular f.

No caso de uma representação onde a função binária f de E em $\{0,1\}$, que toma o valor *0* na posição dos pixels pretos e o valor *1* na posição dos pixels brancos, a função binária f é então chamada de imagem para todo a em E [Banon].

6.3 Operadores

Definição 6.2 (*Operador*) - Um operador sobre Q é um mapeamento de Q em Q.

Um operador sobre Q transforma um subconjunto $A \in Q$, num subconjunto $B \in Q$ pelo elemento estruturante e. Um operador sobre Q é denotado genericamente por ψ (ver figura 6.2). A seguir descreveremos os operadores que são utilizados nesse trabalho.

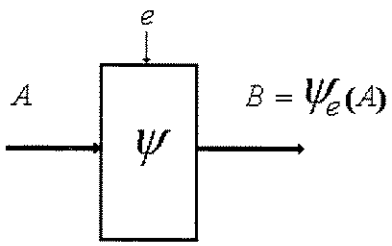


Figura 6.2: Representação de um operador.

Operador Dilatação:

Caracterizamos as operações de dilatação de uma imagem (ver figura 6.3) através de um elemento estruturante e por $\delta_e(A)$, onde:

$$\delta_e(A) = \{ a \in E : e(a) \cap A \neq 0 \} \qquad (A \in Q)$$

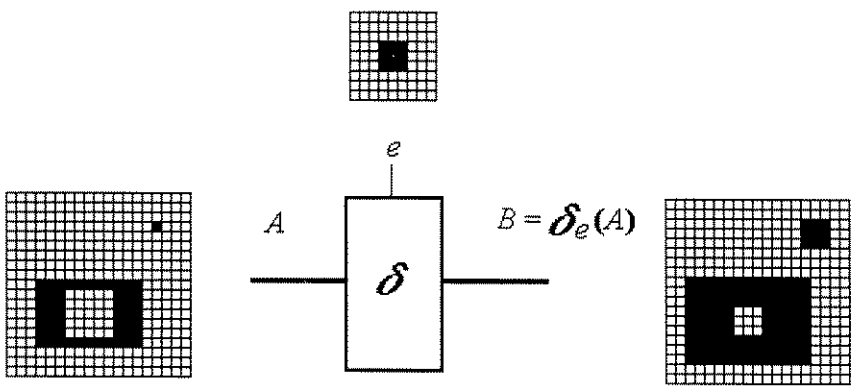


Figura 6.3: Exemplo da operação de dilatação.

Operador Erosão:

Caracterizamos as operações de erosão numa imagem (ver figura 6.4) através de um elemento estruturante e por $\varepsilon_e(A)$, onde:

$$\varepsilon_e(A) = \{ a \in E : e(a) \subset A \} \quad (A \in Q)$$

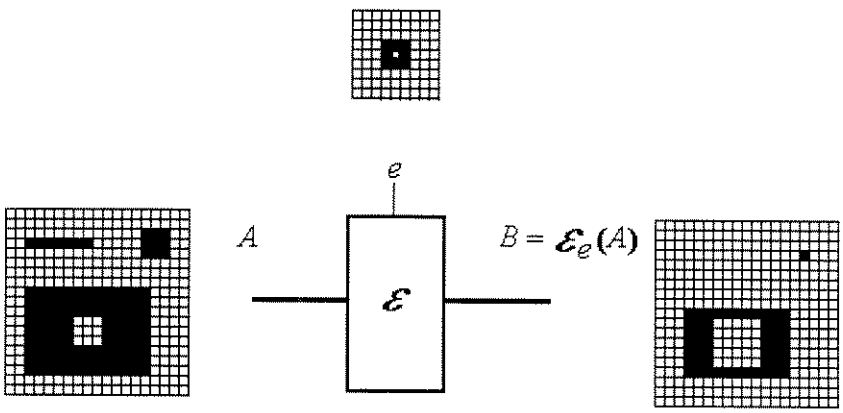


Figura 6.4: Exemplo da operação de erosão.

Além desses dois operadores básicos, acrescentamos mais duas operações entre imagens que são úteis para se compor novos operadores.

Operador União:

Dados os subconjuntos A de pixels $(a, f(a))$ e B de pixels $(b, f(b))$ em E, a operação de união das duas imagens será dada pelo mapeamento de cada um desses pixels no subconjunto C de pixels $(c, f(c))$ em E dado por:

$$f(c) = \begin{cases} 1, \text{ se } f(a) = f(b) = 1 \\ 0, \text{ caso contrário} \end{cases}$$

A figura 6.5 mostra um exemplo da operação de união.

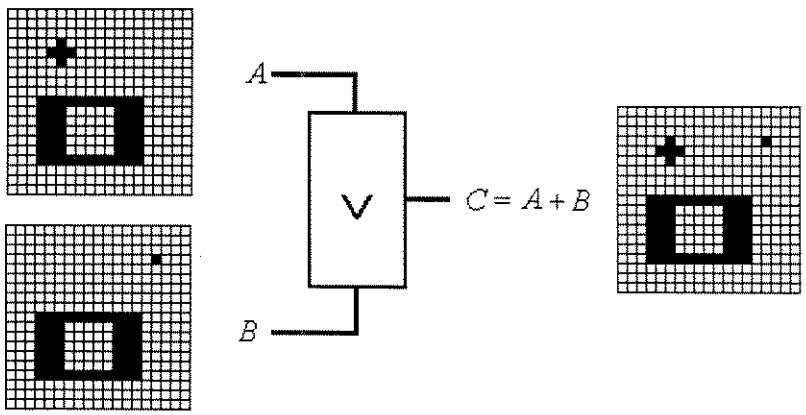


Figura 6.5: Exemplo da operação de união.

Operador Diferença:

Dados dois subconjuntos A de pixels $(a, f(a))$ e B de pixels $(b, f(b))$ em E, a operação de diferença entre as duas imagens será dada pelo mapeamento de cada um desses pixels no subconjunto C de pixels $(c, f(c))$ em E dado por:

$$f(c) = \begin{cases} 1, \text{ se } f(a) = f(b) \\ 0, \text{ caso contrário} \end{cases}$$

A figura 6.6 mostra um exemplo da operação de diferença.

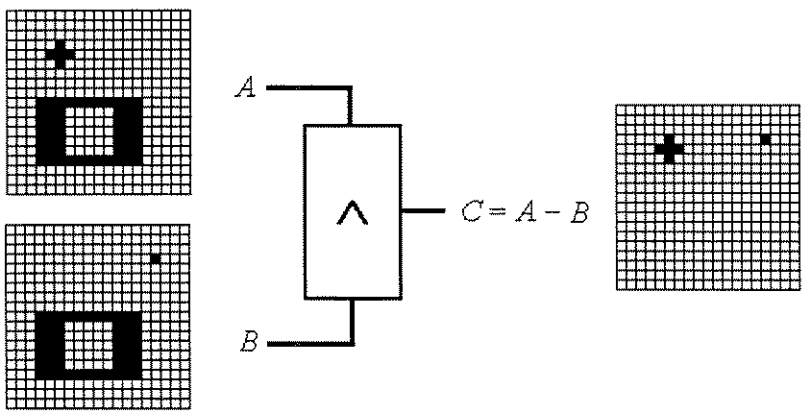


Figura 6.6: Exemplo da operação de diferença.

A partir de operações elementares de erosão e de dilatação, mais as operações de união e diferença, podemos construir uma série de outros operadores, entre os quais destacamos o operador extrator de contornos.

Operador Extrator de Contornos:

Esse operador realiza a operação de dilatação de uma imagem por um elemento estruturante *e*, e a seguir faz a diferença da imagem dilatada com a imagem original (ver figura 6.7).

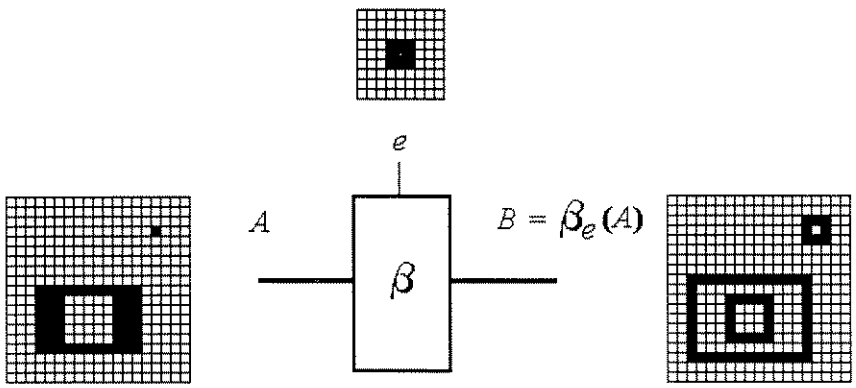


Figura 6.7: Exemplo da operação de extração de contornos.

6.4 Elementos estruturantes

Elementos estruturantes (EEs) são, na prática, pequenas imagens utilizadas pelos operadores de morfologia matemática para desempenhar o papel de extratores de característica da imagem. A utilização de tipos específicos de EEs é o que nos permite extrair consistentemente uma determinada característica de uma imagem.

Cada elemento estruturante (EE) possui uma coordenada de origem, a qual serve como ponto de referência durante sua utilização numa operação. Dependendo dessa origem, os EEs podem ser classificados como simétricos ou não-simétricos.

A figura 6.13 mostra alguns elementos estruturantes clássicos.

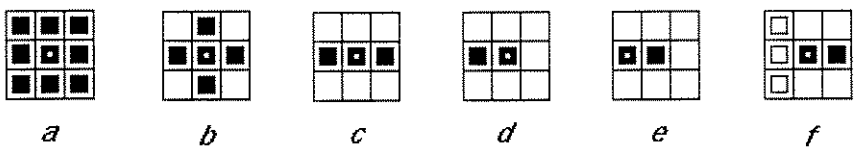


Figura 6.8: Exemplos de elementos estruturantes.

Na notação utilizada cada um dos elementos está colocado dentro de uma grade 3 x 3 para facilitar sua representação. O quadrados pretos dentro da grade indicam a presença de pixels pretos, enquanto os quadrados brancos representam pixels brancos e os espaços vazios da grade representam o estado irrelevante (*don't care state*). Temos ainda que a coordenada (0,0) dessas imagens se encontra representada pelo ponto branco dentro de um dos quadrados pretos.

Na figura 6.8 os elementos *a*, *b*, e *c* são exemplos de elementos simétricos, isto é, se fizermos uma reflexão dessas imagens sobre suas origens, elas continuarão as mesmas. Em contrapartida, os elementos *c*, *d*, e *e* são elementos não-simétricos, isto é,

se fizermos uma reflexão dessas imagens sobre suas origens, obteremos imagens diferentes das originais.

No caso específico dos EEs *d* e *e*, observamos que possuem a mesma configuração de pixels, porém com origem de coordenadas diferentes. Ao realizar uma operação de dilatação em cada um desses elementos estruturantes, obtemos imagens iguais, mas deslocadas de um pixel. Uma representação para esse caso é ilustrado na figura 6.9, onde após as operações de dilatação se faz uma operação de diferença entre as duas imagens obtidas. Como resultado se consegue uma imagem contendo pixels pretos, o que indica a não igualdade entre as duas imagens de entrada.

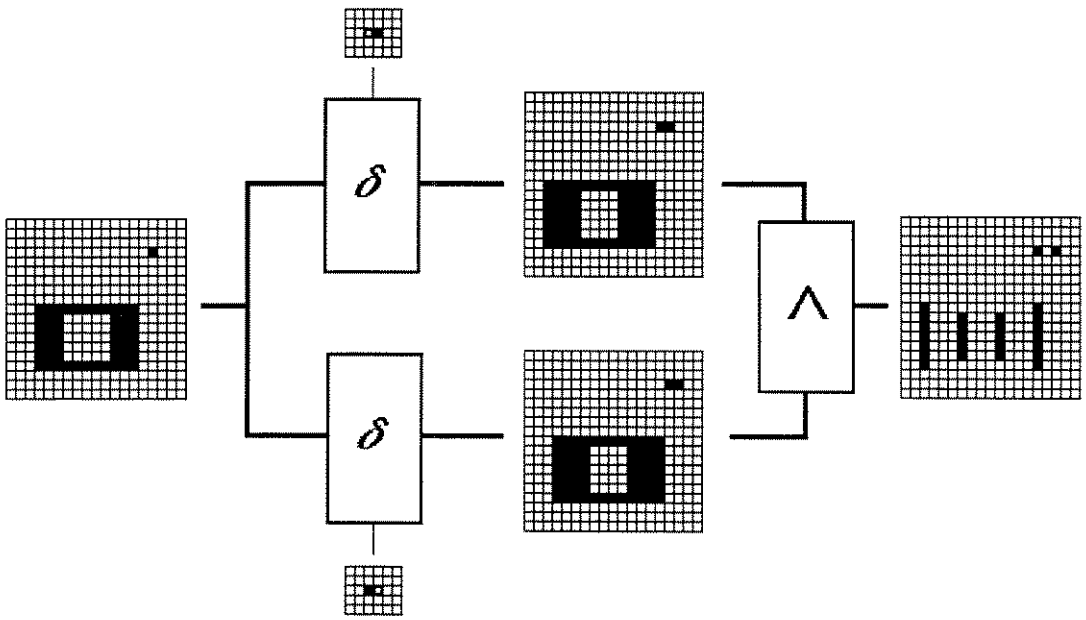


Figura 6.9: Diferença entre imagens obtidas pela dilatação de elementos estruturantes que possuem a mesma configuração de pixels, mas coordenadas de origem diferentes.

O EE *f* da figura 6.8, no qual se define tanto a posição dos pixels brancos como dos pixels pretos, é geralmente utilizado para detectar algum tipo de traço

particular dentro de uma imagem. A figura 6.10 apresenta um exemplo de como pode ser utilizado o EE *f* para detectar bordas laterais de uma imagem.

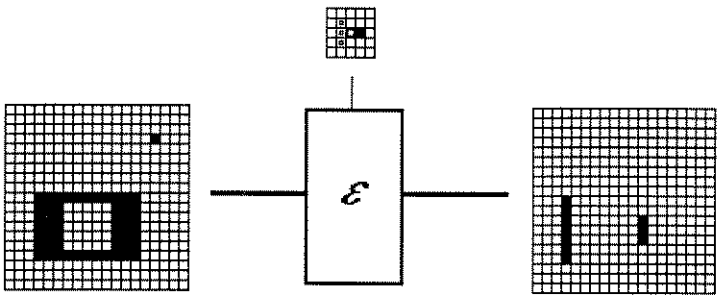


Figura 6.10: Exemplo de detecção de bordas laterais através de uma operação de erosão pelo elemento estruturante *f*.

Capítulo 7

Um Método de Verificação de Assinaturas Estáticas

Nesse capítulo descreveremos o nosso método *off-line* de verificação de assinaturas, com o qual introduzimos um novo método de extração de características. Nele, tomamos a imagem da assinatura como um todo, sem nos preocupar com o seu conteúdo textual. A construção do vetor de características dessa imagem é feita a partir da inclinação das linhas pertencentes a assinatura.

Existem três requisitos básicos que consideramos para a implementação do nosso sistema. Primeiro, a técnica tem que ser robusta no sentido de que apenas um pequeno número de assinaturas seja necessário para treinar o classificador.

Segundo, a técnica proposta deve obter um resultado rápido, após ter sido feito o pedido de verificação. Isto é, uma vez que a imagem da assinatura tenha sido obtida, qualquer tipo de pós-processamento deve ser otimizado.

Finalmente, é claro que a técnica proposta deve ser eficiente, proporcionando uma taxa de erro de classificação muito pequena ou nula.

A figura 7.1 mostra o diagrama de blocos dos processos referentes ao nosso método de verificação. Baseado nesse modelo iremos detalhar cada um dos seus processos.

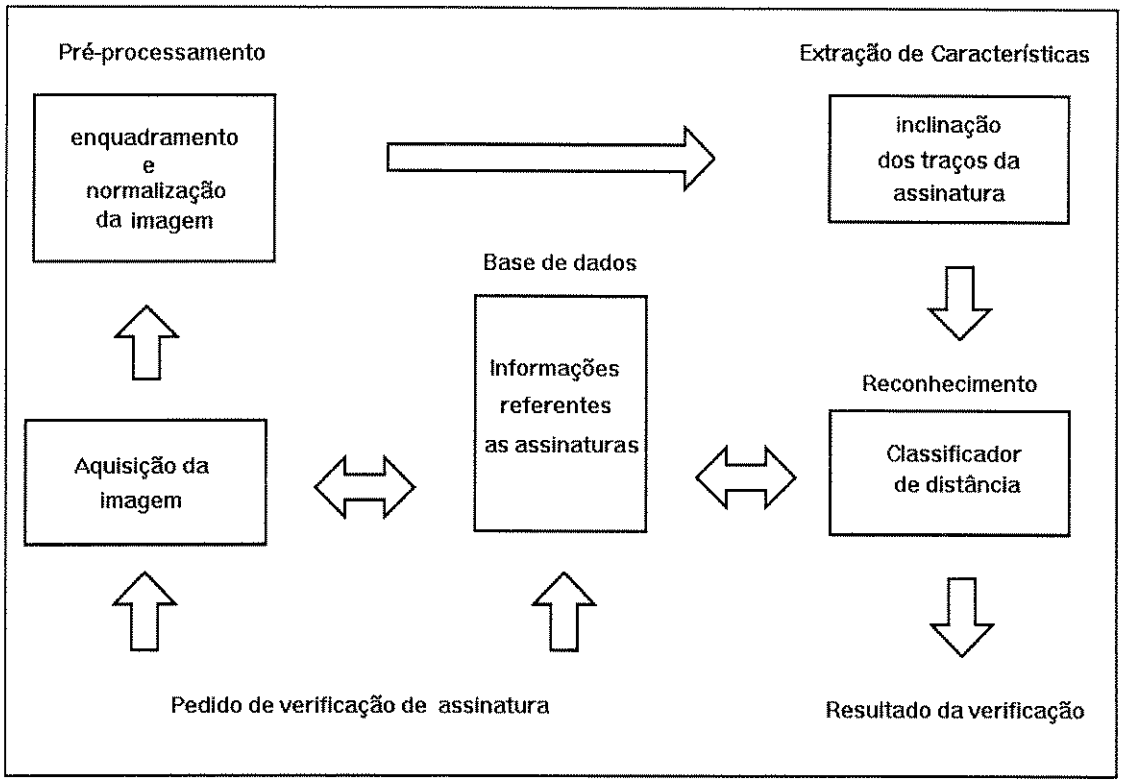


Figura 7.1: Diagrama de blocos do modelo utilizado para implementação do nosso sistema de verificação de assinaturas.

7.1 Aquisição da imagem da assinatura

A aquisição das imagens das assinaturas foi feita através de um *scanner* de mesa. Como descrito na seção 3.2, o banco de assinaturas consta de um total de 950 assinaturas, divididas em três grupos: verdadeiras, falsificações habilitadas e falsificações aleatórias. Essas assinaturas foram coletadas sobre folhas de papel de cor branca, o que elimina as etapas de localização e de segmentação da fase de pré-processamento.

7.2 Pré-processamento da imagem da assinatura

No pré-processamento temos por objetivo obter uma imagem que contenha apenas os traços da assinatura. A figura 7.2 mostra um diagrama com as duas etapas que compõem esse processo: corte de traços estilísticos e redução de escala.

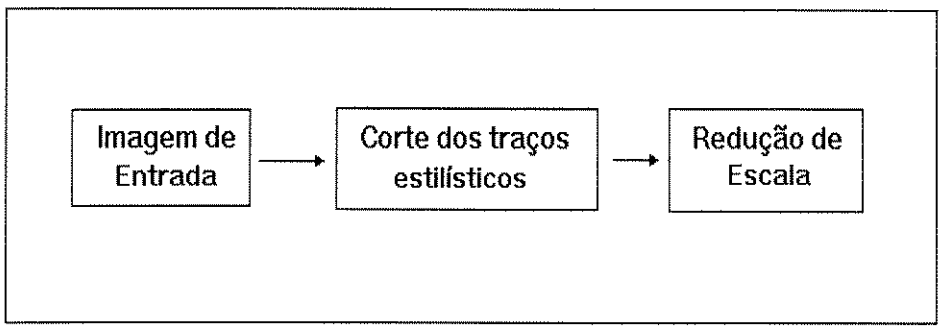


Figura 7.2: Diagrama de blocos das etapas de pré-processamento.

7.2.1 Corte de traços estilísticos

As assinaturas manuscritas têm menos consistência no seu início e final. Isto significa que, ao começarmos a assinar, os primeiros traços tendem a variar bastante, o mesmo acontecendo nos últimos. Constamos também que, para aquelas assinaturas que representam um sinal gráfico, muitos dos traços que se prolongam para cima e para baixo da linha de base da assinatura costumam possuir um comprimento muito variável. Na figura 7.3 mostramos uma assinatura que apresenta algumas dessas características.

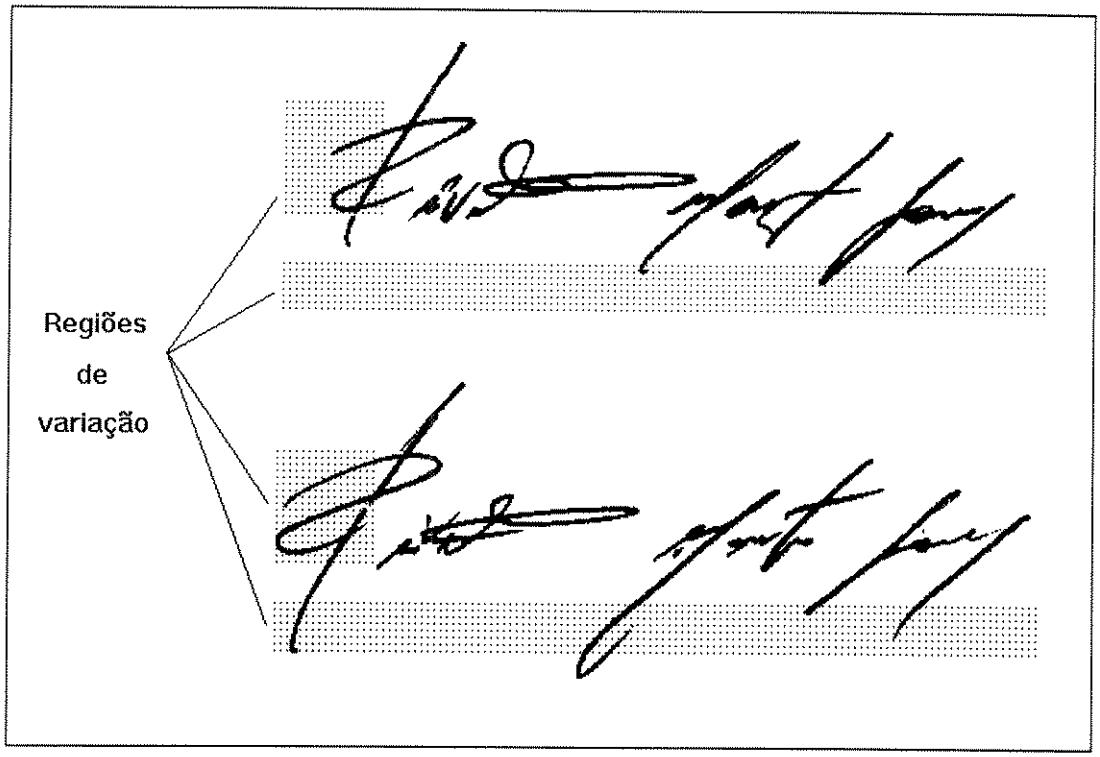


Figura 7.3: Regiões de variação de uma assinatura.

Levando em consideração esses problemas, optamos por fazer um tratamento na imagem de forma a tentar minimizar a existência desses traços.

O algoritmo para o corte dos traços estilísticos é feito da seguinte forma: Primeiramente são calculadas as projeções nos eixos verticais e horizontais da imagem definidas por:

$$P_v[j] = \sum_i I_{ij} \quad \text{para } j = 0, 1, ..., N - 1$$

$$P_h[i] = \sum_i I_{ij} \quad \text{para } j = 0, 1, ..., M - 1$$

onde:

$P_v[j]$ = vetor de projeção no eixo vertical.

$P_h[i]$ = vetor de projeção no eixo horizontal .

$I_{ij} \in \{ 0 ,1 \}$ = nível do pixel na i-ésima linha e j-ésima coluna.

N = comprimento da imagem da assinatura.

M = altura da imagem da assinatura.

Uma representação gráfica da projeções $P_h[i]$ e $P_v[j]$ para uma dada imagem de assinatura é mostrada na figura 7.4.

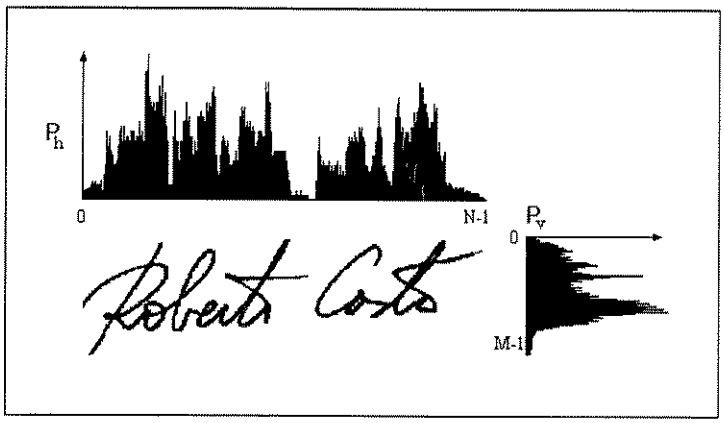


Figura 7.4: Exemplo das projeções horizontais e verticais.

Com a ajuda das projeções encontradas, são calculadas as coordenadas que definem o enquadramento da imagem. Esse enquadramento faz com que sejam cortados os chamados traços estilísticos pertencentes à assinatura.

As coordenadas são compostas por quatro valores que chamaremos x_ini, x_fin, y_ini e y_fin. A seguir, mostramos como determinar cada um desses valores:

1. x_ini = i para o primeiro $P_h[i] = 10$ dado i = 0, 1, ... N -1
2. x_fin = i para o primeiro $P_h[i] = 10$ dado i= N-1, N-2, ... 0

3. y_ini = j para o primeiro $P_v[j] = 10$ dado j = 0, 1, ... M - 1

4. y_fin = j para o primeiro $P_v[j] = 10$ dado j = M-1, M-2, ... 0

Deve ser observado que, algumas vezes, já o início e o final da assinatura possuem mais de 10 pixels de espessura. Nesses casos, x_ini, x_fin, y_ini e y_fin coincidem com o início e o final da assinatura e nenhum traço é cortado.

A figura 7.5 mostra a região obtida pelo enquadramento através das coordenadas das projeções dos eixos vertical e horizontal.

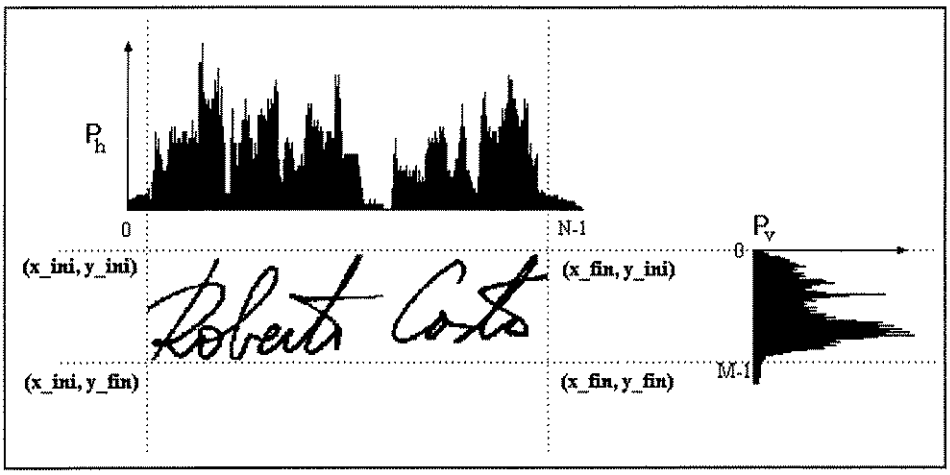


Figura 7.5: Imagem de assinatura após enquadramento e retirada dos traços estilísticos.

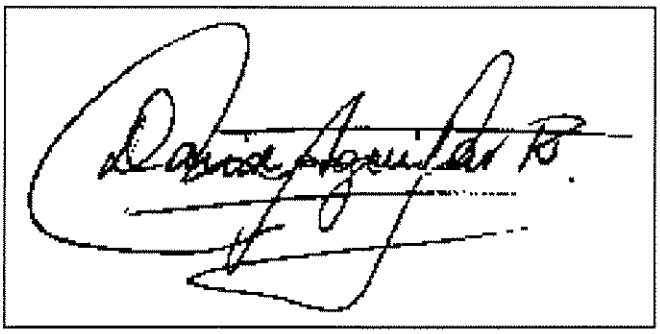
7.2.2 Normalização

Um passo crucial no desenvolvimento de sistemas automáticos de verificação de assinaturas é encontrar a representação digital, que possa maximizar a distância entre os vetores de características de indivíduos diferentes.

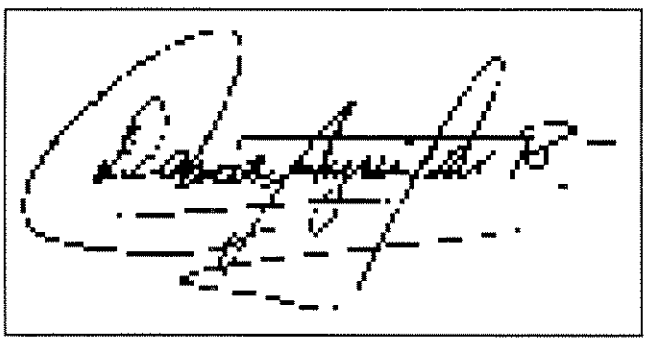
Constatamos que numa escala de resolução baixa todas as assinaturas são semelhantes. Por outro lado, em escalas muito altas, assinaturas de um mesmo indivíduo podem apresentar variações bastante significativas. Portanto, não podemos trabalhar em nenhum desses dois extremos. Pois, se a escala de resolução é baixa, o

sistema tende a errar pela falta de poder de discriminação. Em contrapartida, numa escala muito detalhada, o sistema pode rejeitar assinaturas genuínas pela variabilidade existente entre elas.

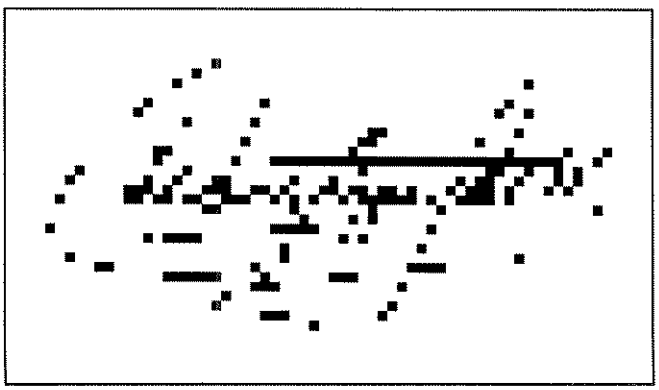
A figura 7.3 apresenta uma mesma assinatura em várias escalas de resolução, mostrando perda da qualidade da imagem à medida em que a resolução vai diminuindo.



256 x 118 pixels



128 x 59 pixels



64 x 30 pixels

Figura 7.6: Imagens de assinaturas em diferentes resoluções.

Decidimos fazer a normalização do tamanho das assinaturas fixando o valor do comprimento da assinatura em 256 pixels e sua altura sendo proporcional ao comprimento, de tal forma que a altura da assinatura é dada por (256*y_sing)/x_sing onde:

x_sing = x_fin - x_ini

y_sing = y_fin - y_ini

A figura 7.7 mostra um exemplo da normalização de uma assinatura.

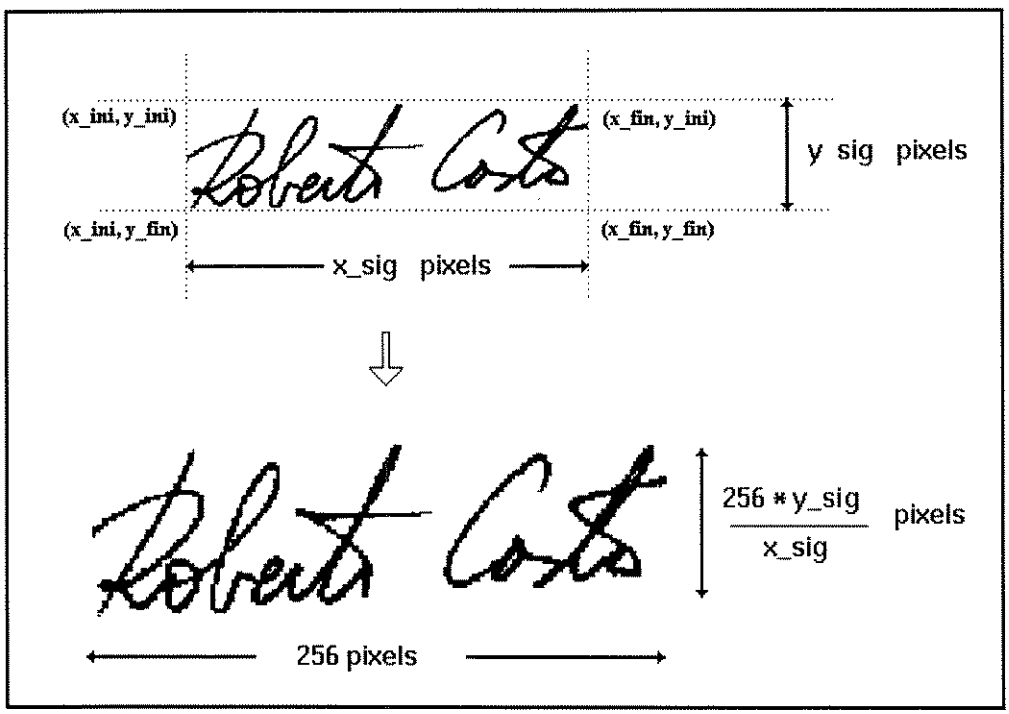


Figura 7.7: Normalização da assinatura.

7.3 Extração de características

Para um bom desempenho do sistema, é essencial ter um vetor de características que represente da melhor maneira possível a imagem da assinatura. Para compor esse vetor, nosso método utiliza características de inclinação dos traços da assinatura e de inclinação de seus contornos. A extração dessas características é feita através de técnicas de morfologia matemática.

7.3.1 Descrição dos elementos estruturantes utilizados na extração da inclinação dos traços da assinatura

Na extração da inclinação dos traços da assinatura são utilizados 32 elementos estruturantes. A figura 7.8 mostra os 32 EEs, onde cada um deles foi denominado seqüencialmente de EE-1 até EE-32.

Os 32 EEs escolhidos representam segmentos de retas compostos de cinco pixels. Cada um desses EE representa uma inclinação diferente. A diferença do ângulo de inclinação entre um elementos estruturante e o seu sucessor é de aproximadamente 11 graus. O elemento estruturante EE-1, por exemplo, representa um segmento de reta com ângulo de inclinação de 0 grau em relação ao eixo horizontal. Da mesma forma o EE-6 representa o segmento de reta com ângulo de aproximadamente 56 graus em relação ao eixo horizontal. Uma representação da medida desse ângulo é mostrada na figura 7.9.

Deve ser observado que o formato dos elementos estruturantes compreendidos entre EE-1 e EE-16 são semelhantes a elementos estruturantes compreendidos entre EE-17 e EE-32, porém a coordenada de origem entre eles é diferente. Isso se deve a

que os últimos representam segmentos de reta com ângulo de inclinação maior do que 180 graus.

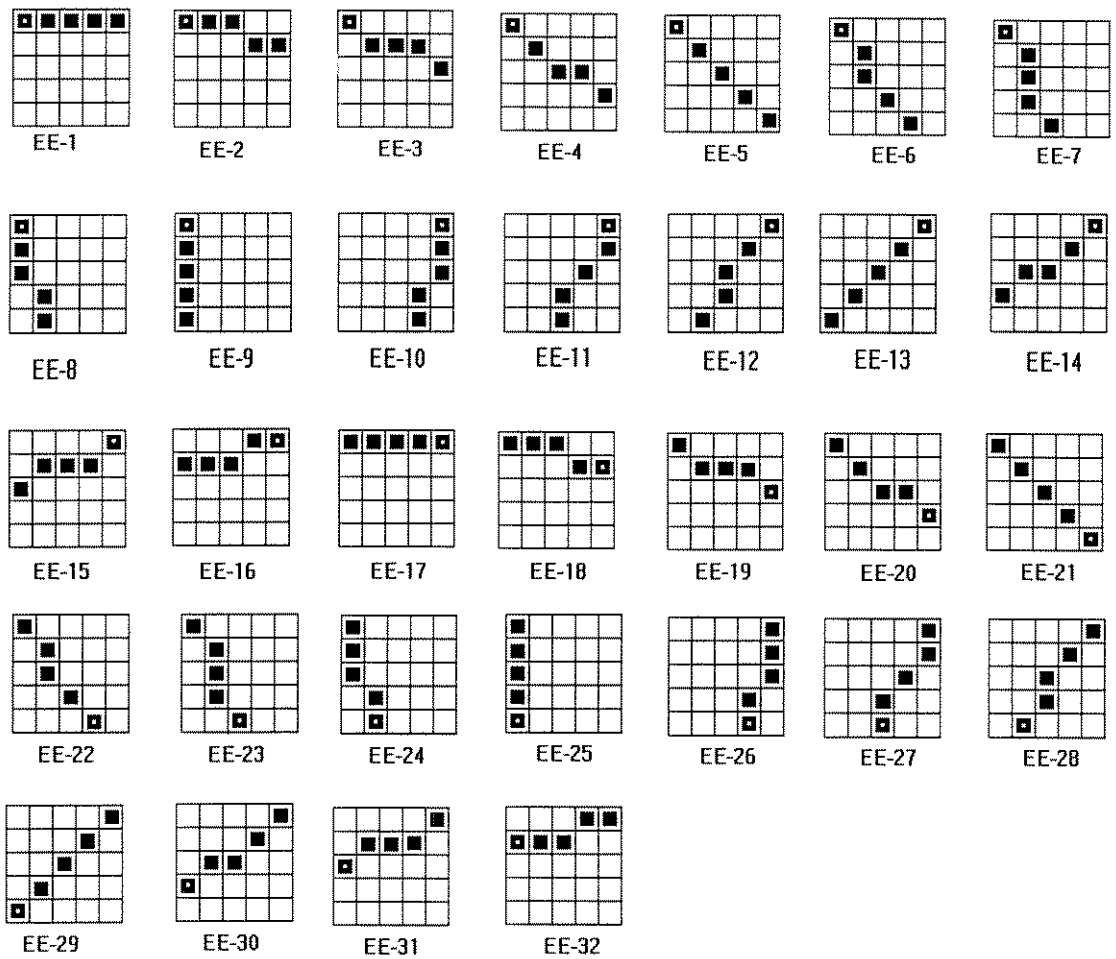


Figura 7.8: Os 32 elementos estruturantes utilizados para extração de características de inclinação dos traços da assinatura.

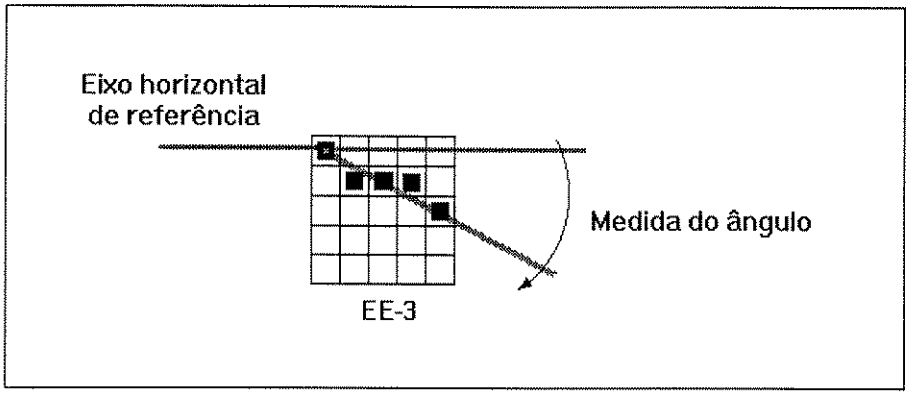


Figura 7.9: Medida do ângulo de inclinação dos segmentos de reta que compõe os EEs.

7.3.2 Descrição da técnica de extração das características de inclinação dos traços da assinatura

Para uma imagem de assinatura A, tomamos um EE e fazemos a operação de erosão. Sobre a imagem resultante B é feita a contagem de todos os seus pixels. O número de pixels de B indica quantas vezes aquele EE esteve contido na imagem A. Essa operação é repetida para cada um dos 32 EEs, sempre tomando a imagem da assinatura A como entrada.

A figura 7.10 mostra a operação de erosão feita pelo EE-13 em cima de uma imagem genérica. Nesse exemplo, a imagem resultante consta de quatro pixels pretos.

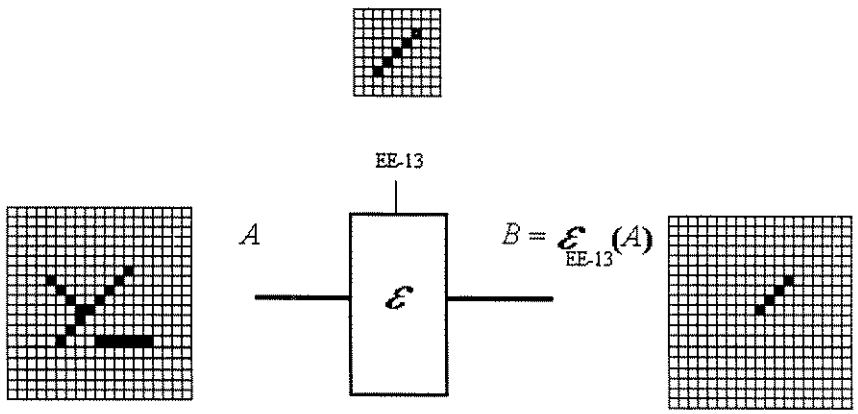


Figura 7.10: Exemplo de uma imagem erodida pelo EE-13.

Na figura 7.10 observa-se claramente que os pixels que fazem parte de segmentos de reta que não possuem a mesma inclinação que EE-13, não possuem nenhum pixel mapeado na imagem *B*.

Se utilizarmos um outro elemento estruturante, por exemplo EE-1, e fizermos uma nova erosão em *A*, obteremos três pixels mapeados em *B*, porém em posições diferentes daquelas obtidas com EE-13. Dessa forma, observa-se que para cada um dos diferentes EEs obteremos uma imagem erodida com um número particular de pixels mapeados.

Esse tipo de observação nos levou a concluir que o número de pixels mapeados na imagem erodida é uma característica bastante representativa da imagem da assinatura.

Fizemos ainda uma comparação entre o número de pixels mapeados pelos 32 EEs em assinaturas de indivíduos diferentes. O resultado dessa comparação mostra que o número de pixels mapeados pelos EEs é bastante diferente (ver figura 7.11).

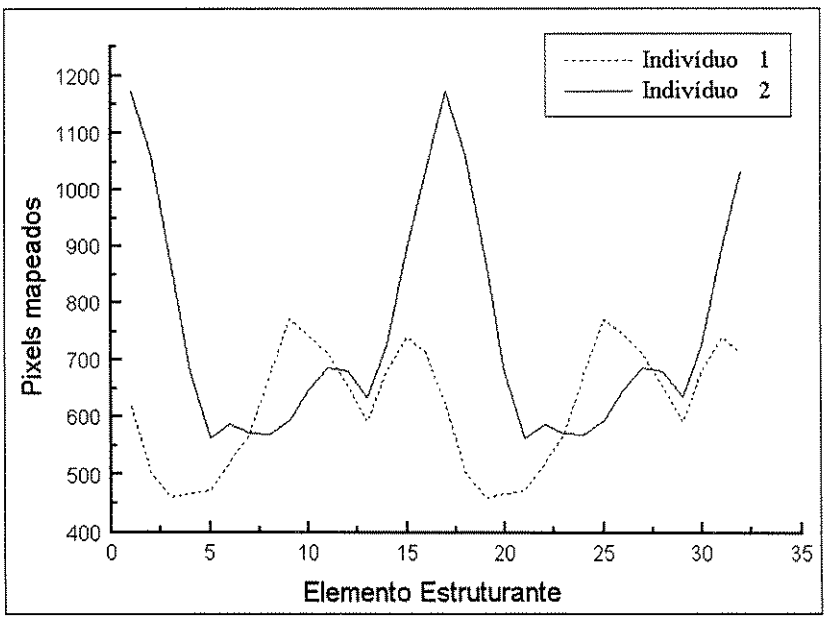


Figura 7.11: Comparação de pixels mapeados entre assinaturas diferentes.

Por outro lado, ao fazermos a comparação com assinaturas provenientes de uma mesma pessoa, verificamos que a diferença entre o número de pixels mapeados é bem menor (ver figura 7.12).

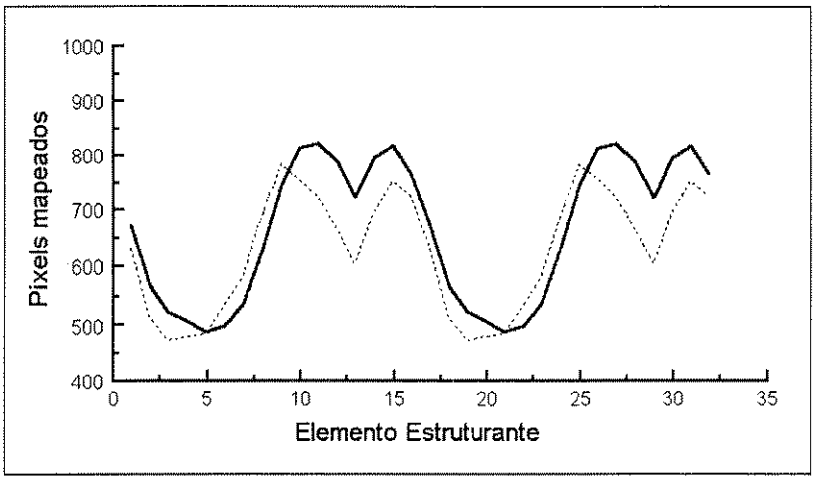


Figura 7.12: Comparação de pixels mapeados entre assinaturas da mesma pessoa.

Definimos, para compor nosso vetor de características da imagem, o número de pixels resultante da operação de erosão para cada um dos 32 EEs apresentados na figura 7.8.

7.3.3 Descrição dos elementos estruturantes da extração de características de contorno de uma imagem de assinatura

Primeiramente, definimos o elemento estruturante EE-33 como sendo um quadrado de 3 x 3 pixels pretos e de coordenada de origem no seu centro (ver figura 7.13).

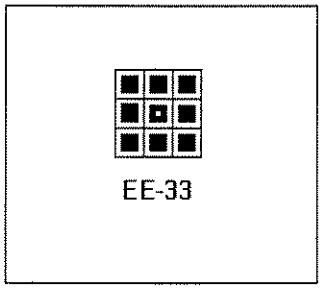


Figura 7.13: Elemento estruturante de 3 x 3 pixels pretos.

Ao realizar a operação de extração de contorno pelos elementos estruturantes EE-33 sobre uma imagem qualquer, obteremos uma imagem composta principalmente de linhas de espessura de um pixel. Para exemplificar nossa observação, tomamos a imagem de entrada da figura 7.10 e aplicamos sobre ela a operação de extração de contorno pelo EE-33. Essa operação é ilustrada na figura 7.14.

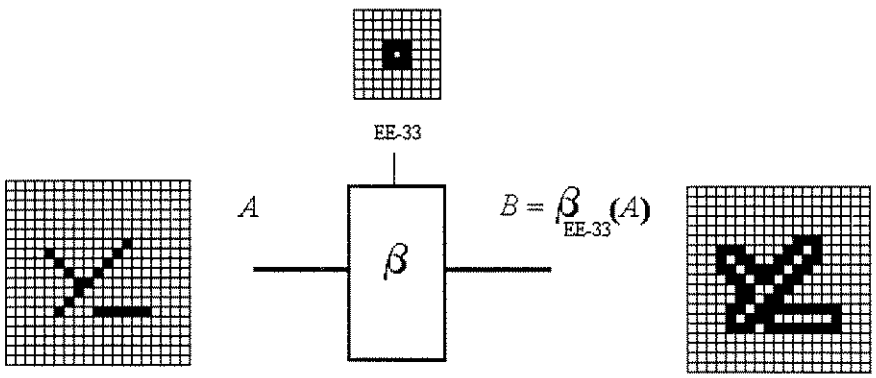


Figura 7.14: Exemplo da aplicação do EE-33 sobre uma imagem.

Para acharmos a inclinação da imagem do contorno, definimos os elementos estruturantes EE-34, EE-35, EE-36, EE-37, EE-38 e EE-39 como se vê na figura 7.15.

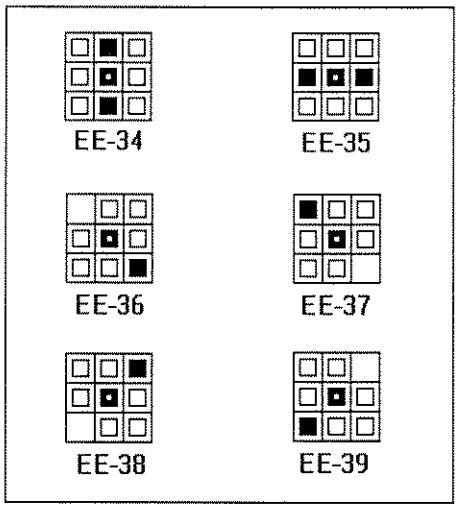


Figura 7.15: Elementos estruturantes para extração da inclinação do contorno de uma imagem.

Seguindo o mesmo princípio descrito na seção 7.3.2, em operações de erosão esses EEs, podem ser utilizados para detectar a inclinação de segmentos de reta. O EE-34 detecta segmentos de retas verticais e o EE-35 detecta segmentos de retas horizontais. Os EE-36 a EE-37 detectam variações de pixels na direção diagonal.

7.3.4 Descrição da técnica de extração das características de inclinação dos contornos da assinatura

Para uma imagem de assinatura A, tomamos EE-33 e fazemos a operação extração de contorno obtendo B. Sobre a imagem resultante B, aplicamos a operação de erosão pelos elementos estruturantes EE-34 a EE-39. O número de pixels mapeados através de cada um desses EEs representa uma característica. A seguir, fazemos uma adição entre as A e B, obtendo a imagem C, que na verdade é a imagem da assinatura A dilatada por EE-33. A ilustração desse processo é mostrada na figura 7.16.

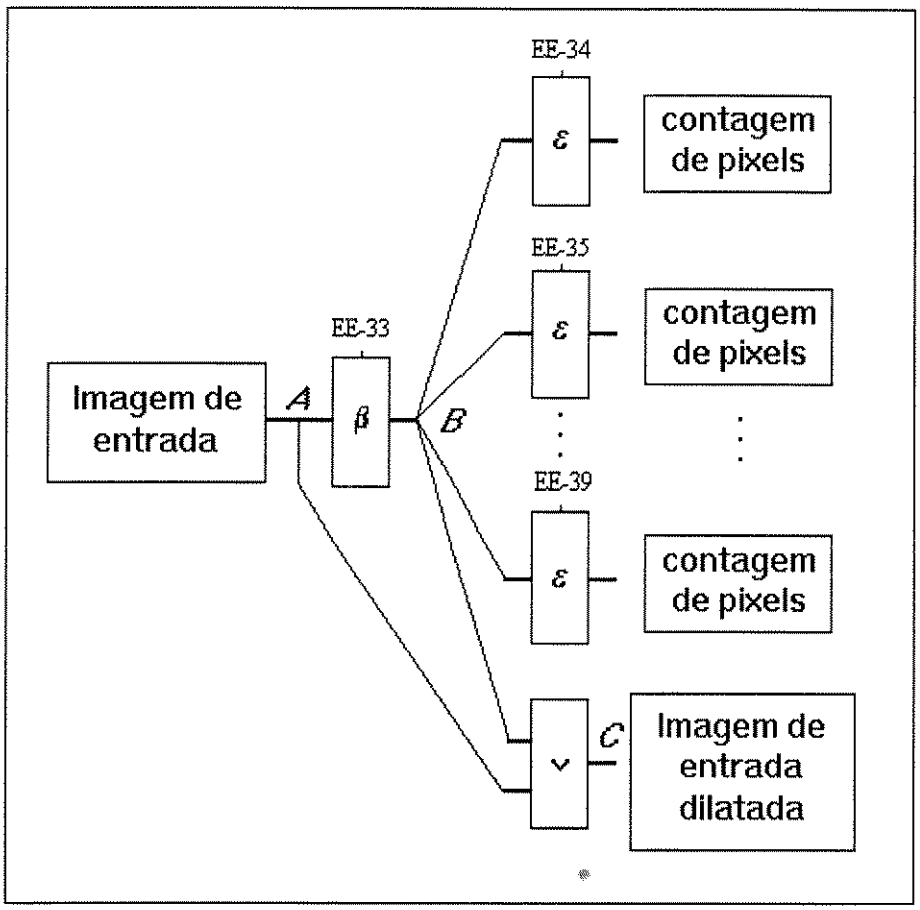


Figura 7.16: Processo da extração das características de inclinação dos contornos da assinatura.

Esse ciclo é repetido quatro vezes mais, com a diferença de que para cada nova repetição, a imagem de entrada passa a ser a imagem dilatada *C* do ciclo anterior. Como esse processo é composto por cinco ciclos, obteremos no final desse processo 30 características.

A figura 7.17 mostra a composição final do vetor de características K, composto das características k_1, k_2, k_3, ... k_{62}.

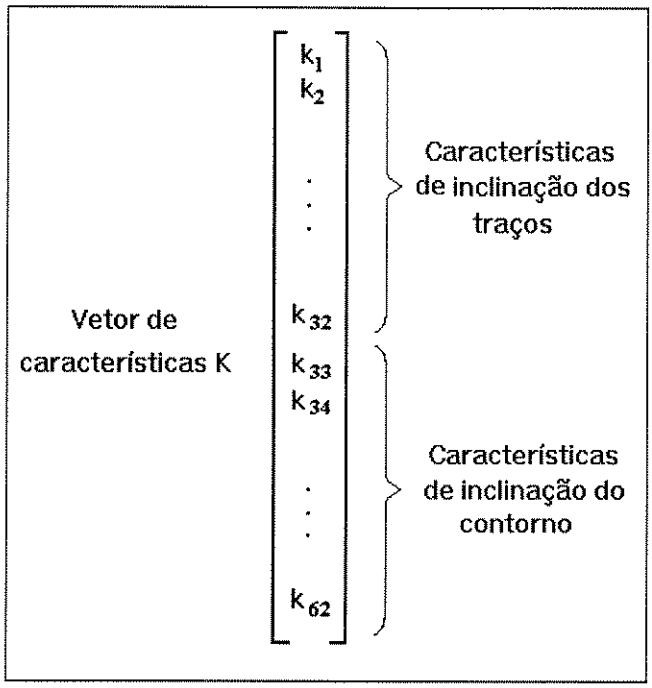


Figura 7.17: Composição do vetor de características.

7.4 Reconhecimento de assinaturas

O classificador utilizado para fazer a verificação da assinatura é um classificador de distância, dado pela equação 7.1:

$$dist = \frac{1}{\sigma_j} \sum_{j=1}^{NC} \left| k_j - u_j \right| \tag{7.1}$$

onde:

k_j: a j-ésima característica da assinatura desconhecida

u_j: a média da j-ésima característica, calculada sobre um conjunto de dez assinaturas verdadeiras que fazem parte da base de dados.

σ_j: a variância da j-ésima característica, calculada sobre um conjunto de dez assinaturas verdadeiras que fazem parte da base de dados.

NC: número de características que compõem o vetor de características da assinatura.

7.5 Resultados experimentais

Para os testes do nosso método, primeiramente foi calculado o vetor de características médio das assinaturas verdadeiras dos cinco indivíduos que tomamos como referência. Esse vetor é formado pela média aritmética de dez vetores de assinaturas verdadeiras. Essas assinaturas foram escolhidas aleatoriamente entre as 110 assinaturas verdadeiras que compõe nossa base de dados.

No teste realizado para avaliar o desempenho do nosso sistema de verificação, utilizamos a equação 7.1 para calcular a distância das 100 assinaturas verdadeiras, 60 habilitadas e 100 aleatórias de cada indivíduo em relação ao vetor de características de cada indivíduo. A partir dessas distâncias plotamos, para cada um dos cinco indivíduos, a COR para o caso em que o universo de assinaturas contém assinaturas verdadeiras e falsificações habilitadas, e para o caso em que o universo de assinaturas contém assinaturas verdadeiras e falsificações aleatórias.

A seguir apresentaremos os resultados dos testes realizados para cada um dos cinco indivíduos através dos gráficos da COR.

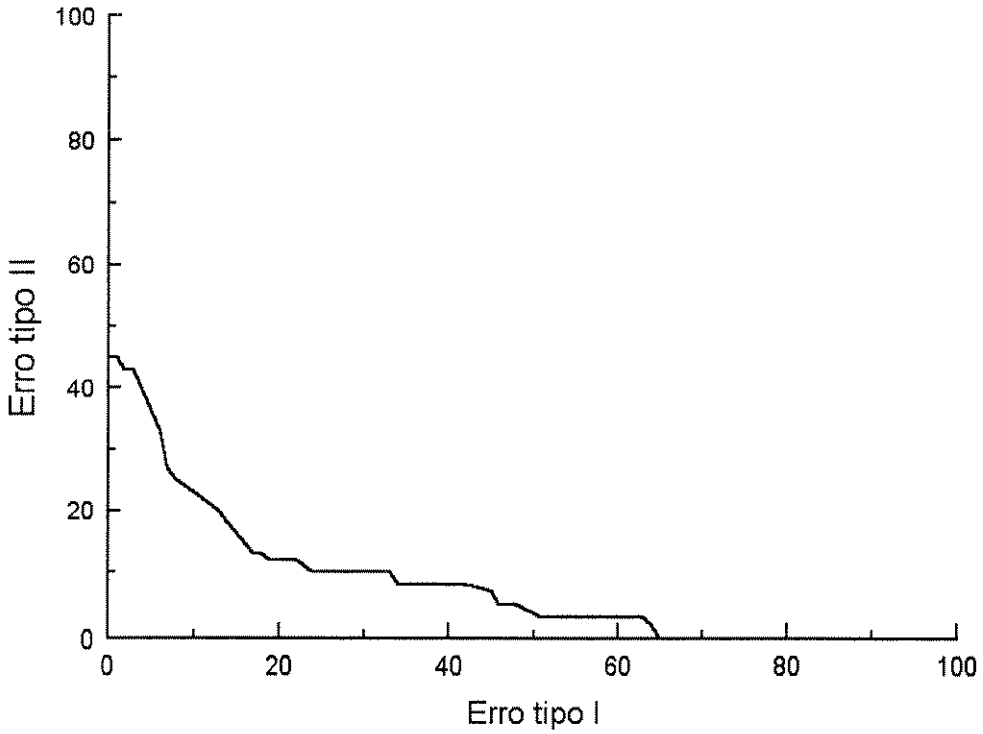


Figura 7.18: Resultado obtido com falsificações habilitadas para o indivíduo 1.

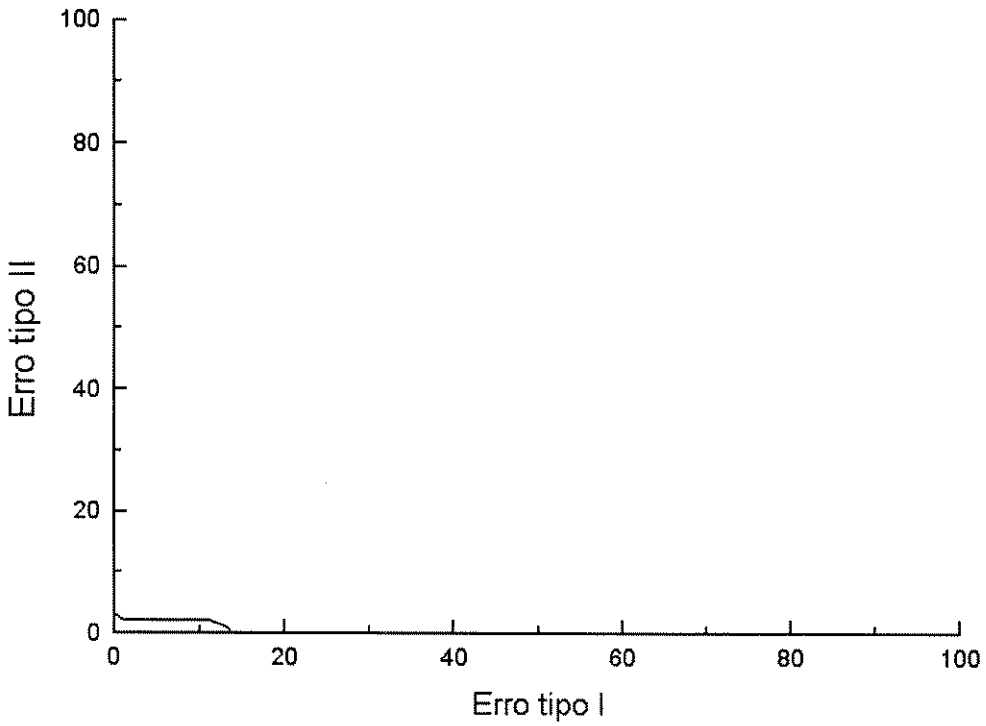


Figura 7.19: Resultado obtido com falsificações aleatórias para o indivíduo 1.

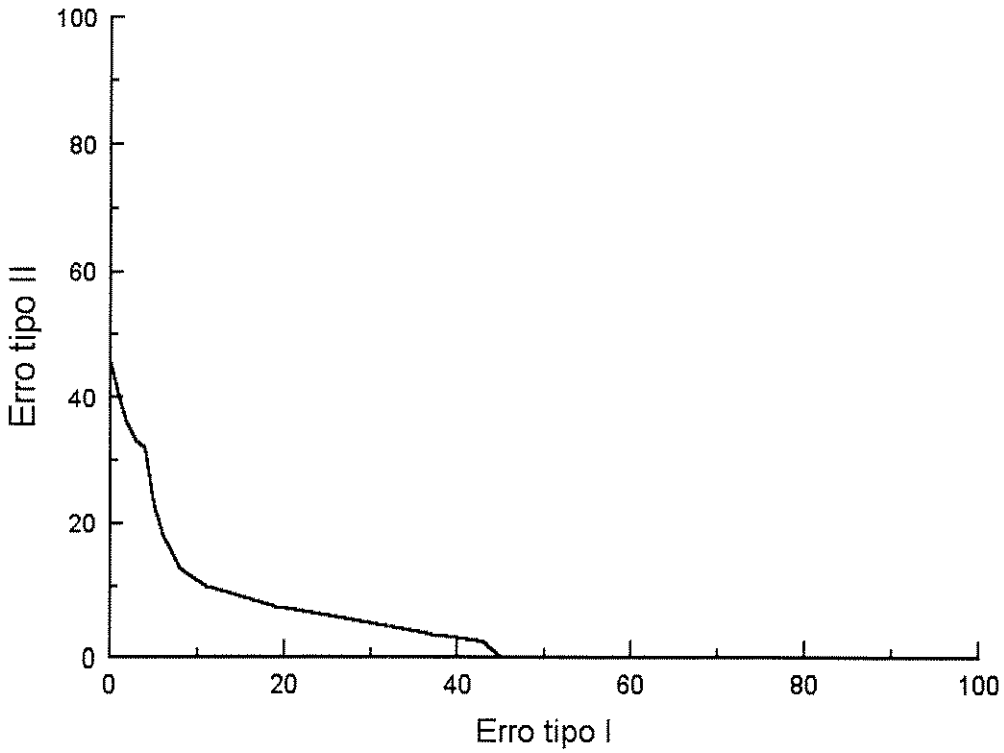


Figura 7.20: Resultado obtido com falsificações habilitadas para o indivíduo 2.

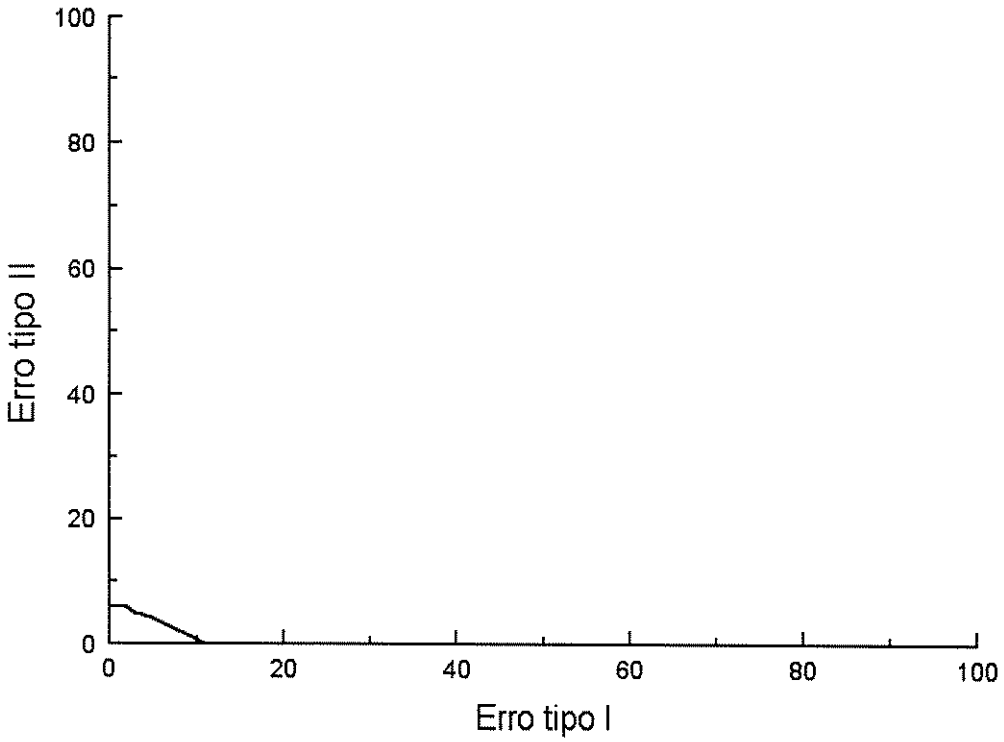


Figura 7.21: Resultado obtido com falsificações aleatórias para o indivíduo 2.

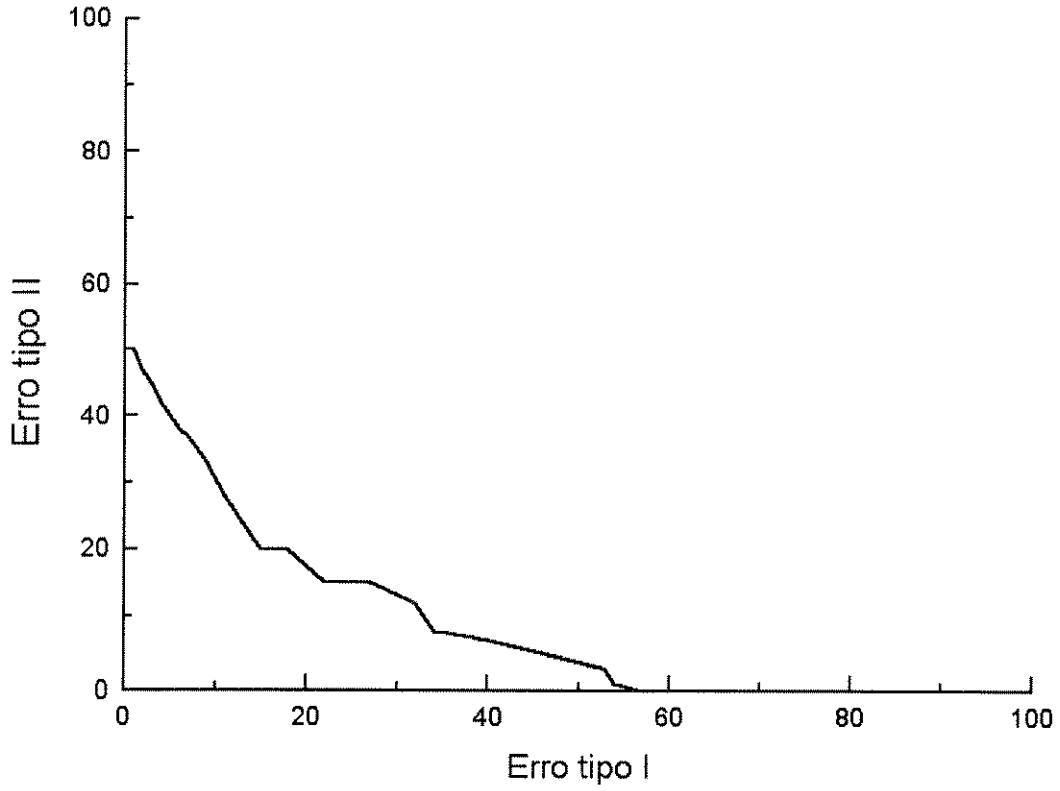


Figura 7.22: Resultado obtido com falsificações habilitadas para o indivíduo 3.

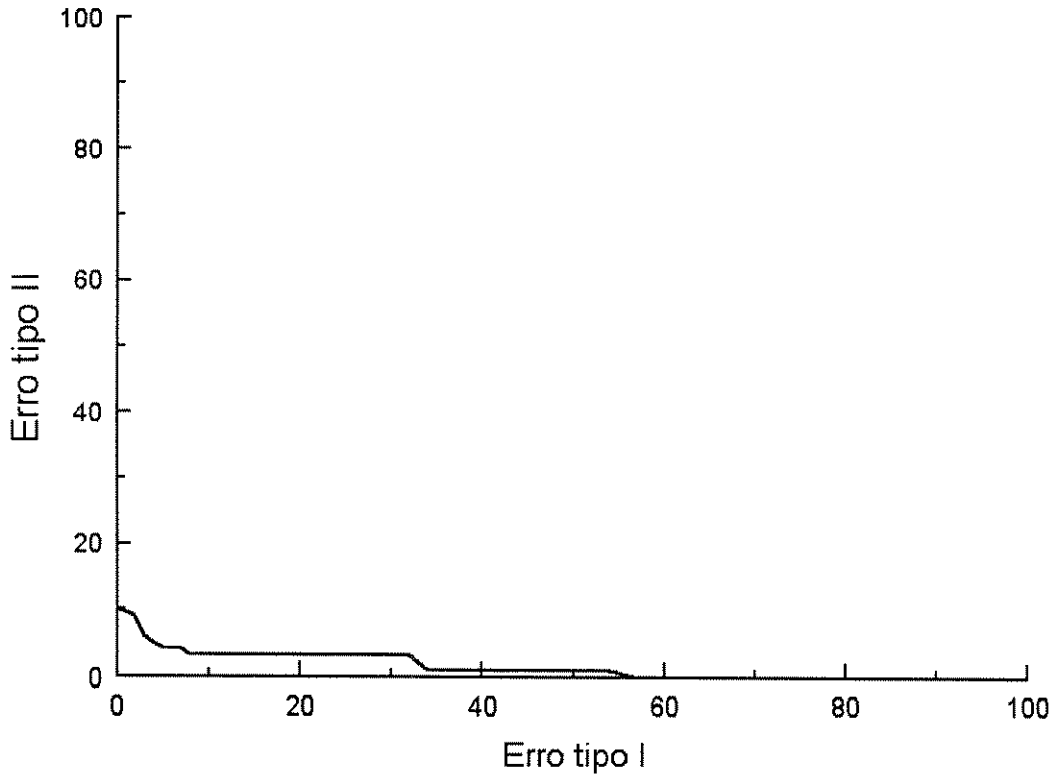


Figura 7.23: Resultado obtido com falsificações aleatórias para o indivíduo 3.

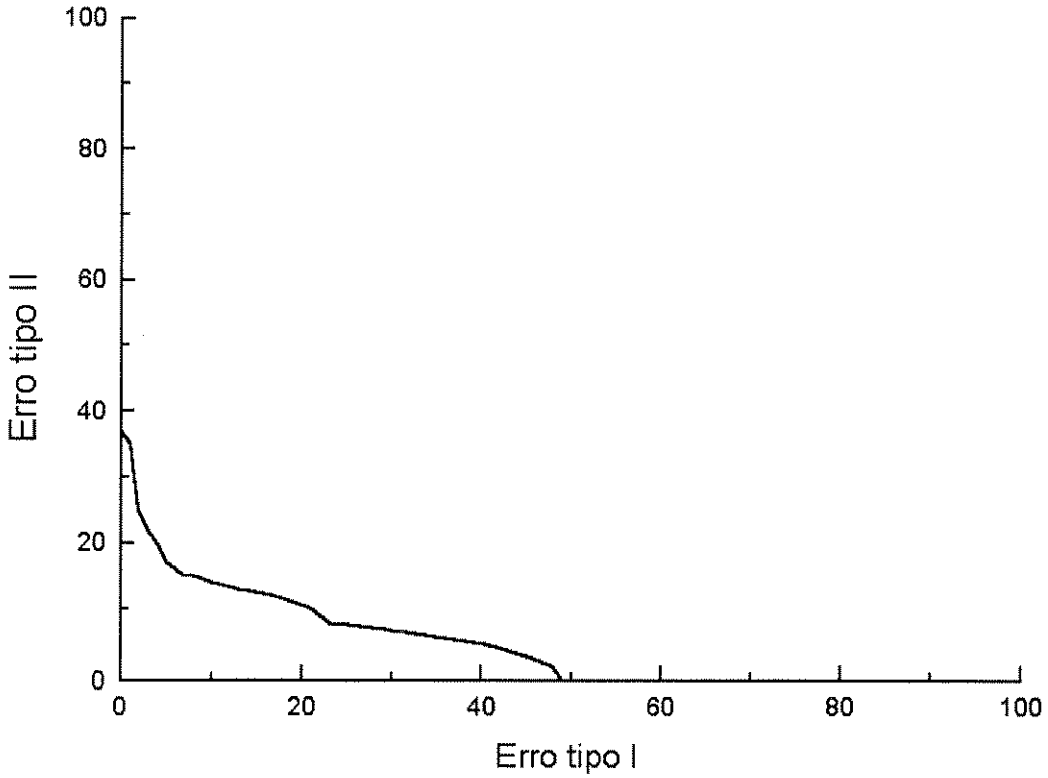


Figura 7.24: Resultado obtido com falsificações habilitadas para o indivíduo 4.

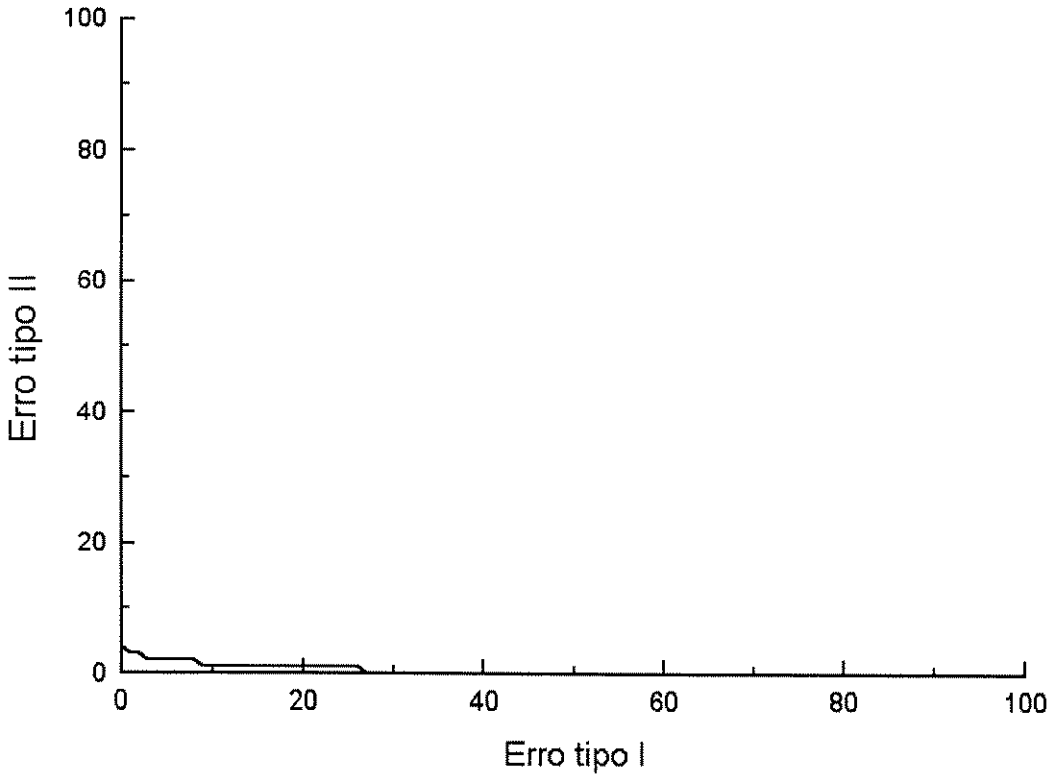


Figura 7.25: Resultado obtido com falsificações aleatórias para o indivíduo 4.

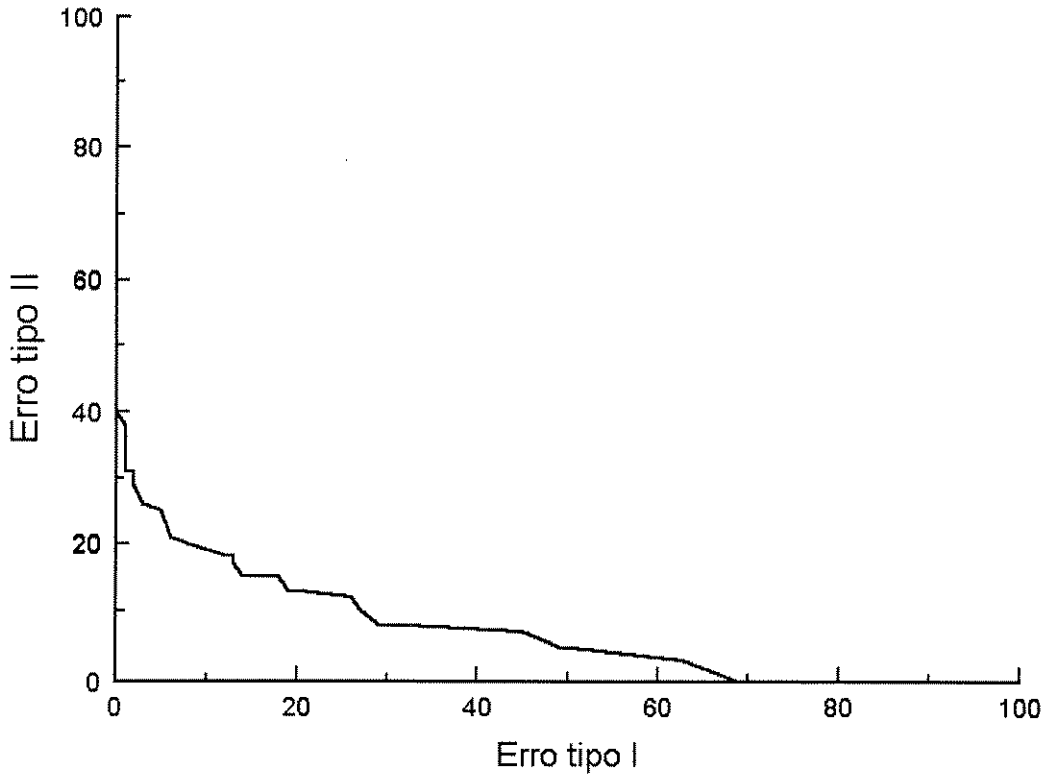


Figura 7.26: Resultado obtido com falsificações habilitadas para o indivíduo 5.

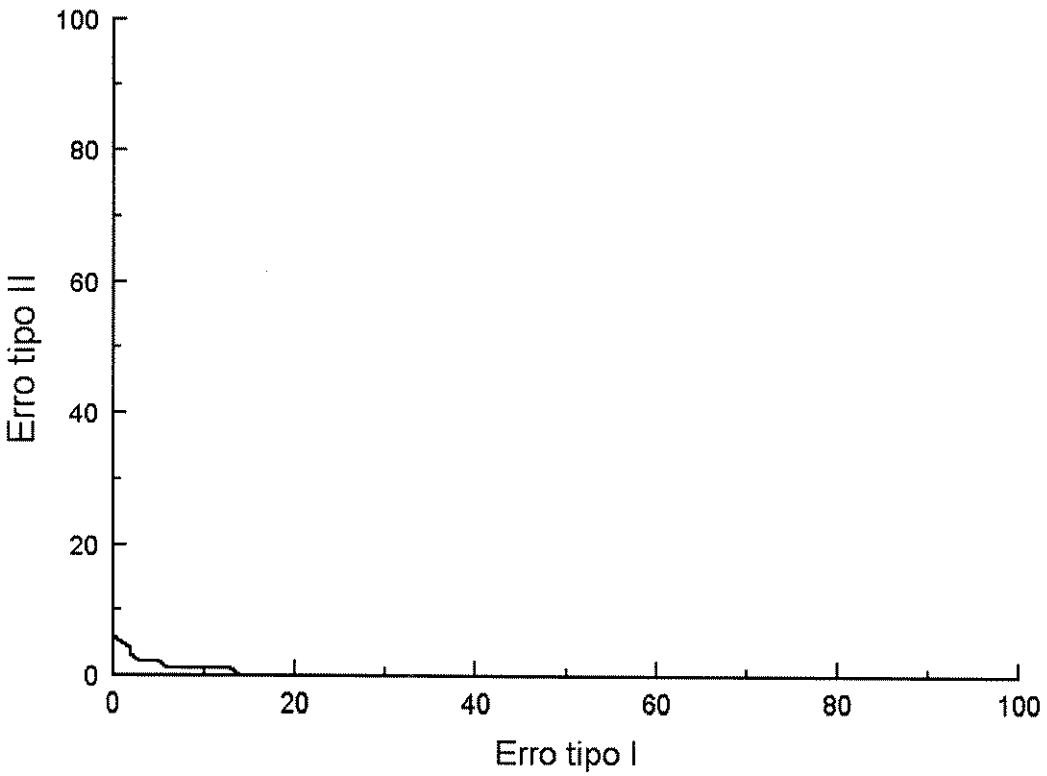


Figura 7.27: Resultado obtido com falsificações aleatórias para o indivíduo 5.

A partir da análise das CORs construímos as tabelas 7.1 a 7.5, onde apresentamos a taxas de erro obtidas para cada um dos indivíduos.

Indivíduo 1

	Habilitadas	Aleatórias
Erro tipo I, com tipo II = 0	65 %	14 %
Erro tipo II, com tipo I = 0	45 %	3 %
Taxa de erros iguais	16 %	1 %

Tabela 7.1: Taxas de erro do sistema no indivíduo 1.

Indivíduo 2

	Habilitadas	Aleatórias
Erro tipo I, com tipo II = 0	45 %	11 %
Erro tipo II, com tipo I = 0	45 %	6 %
Taxa de erros iguais	10 %	4 %

Tabela 7.2: Taxas de erro do sistema no indivíduo 2.

Indivíduo 3

	Habilitadas	Aleatórias
Erro tipo I, com tipo II = 0	57 %	57 %
Erro tipo II, com tipo I = 0	50 %	10 %
Taxa de erros iguais	19 %	5 %

Tabela 7.3: Taxas de erro do sistema no indivíduo 3.

Indivíduo 4

	Habilitadas	Aleatórias
Erro tipo I, com tipo II = 0	48 %	26 %
Erro tipo II, com tipo I = 0	37 %	4 %
Taxa de erros iguais	13 %	3 %

Tabela 7.4: Taxas de erro do sistema no indivíduo 4.

Indivíduo 5

	Habilitadas	Aleatórias
Erro tipo I, com tipo II = 0	68 %	14 %
Erro tipo II, com tipo I = 0	40 %	6 %
Taxa de erros iguais	15 %	2 %

Tabela 7.5: Taxas de erro do sistema no indivíduo 5.

7.6 Análise dos resultados do método de verificação proposto

Através dos dados obtidos, percebemos a melhor performance do sistema sobre as falsificações aleatórias do que sobre as falsificações habilitadas. Esse fato era esperado, visto a semelhança existente entre as amostras de assinaturas verdadeiras com as falsificações habilitadas.

No caso em que o sistema é testado com falsificações habilitadas, a taxa de erro tipo I chegou 69 % e a de erro tipo II a 50 %. Já nos testes com falsificações aleatórias essas taxas de erro baixaram para 57 % no tipo I e para 10 % no tipo II.

Por outro lado, a taxa de erros iguais, que é o parâmetro mais importante na análise do desempenho de um sistema de verificação, obteve no caso de falsificações habilitadas o valor mínimo de 10 % e no caso de falsificações aleatórias o valor mínimo de 1 %.

A tabela 7.6 apresenta a média das taxas de erros dos cinco indivíduos analisados.

	Habilitadas	Aleatórias
Erro tipo I, com tipo II = 0	56,6 %	24,4 %
Erro tipo II, com tipo I = 0	43,4 %	5,8 %
Taxa de erros iguais	14,6 %	3,0 %

Tabela 7.6: Média das taxas de erro.

Considerando apenas os resultados frente a falsificações aleatórias, constatamos que as médias das taxas de erro do nosso sistema possuem valores próximos aos apresentados por outros pesquisadores (vide tabela 5.1, pag. 58), frente ao mesmo tipo de falsificações.

Quanto à média da taxa de erros iguais que nosso sistema obteve com falsificações habilitadas, consideramos que o valor de 14,6 % é bastante satisfatório, visto a dificuldade de discernimento entre as assinaturas verdadeiras e falsas, mesmo quando a avaliação é feita de forma manual.

Vale salientar também que a obtenção do valor de 3 % para a média da taxa de erros iguais frente a falsificações aleatórias é significativa, devido aos resultados de outros pesquisadores e da sugestão que este índice nos oferece em podermos chegar a taxas de erros nulas, através de algumas melhorias no atual sistema.

Capítulo 8

Discussões e Conclusões

Nesse capítulo colocaremos alguns comentários sobre o trabalho apresentado, enfatizando as contribuições oferecidas e indicando melhorias que podem ser feitas no sistema.

8.1 Contribuições

O sistema desenvolvido é um sistema completo, isto é, nos preocupamos em desenvolver um protótipo que englobasse todas as etapas de um processo de verificação de assinaturas.

O software implementado para suporte do sistema, oferece uma interface homem/máquina de fácil manuseio e permite a verificação de assinaturas de forma manual e automática. Além disso, o software permite a transmissão de dados via rede de computadores, o que possibilita a utilização de bancos de dados e de terminais remotos para o armazenamento e a verificação de assinaturas.

O método de compressão proposto para arquivos de assinatura estáticas, consegue as maiores taxas de compressão, quando comparado com outros tipos de arquivos de armazenamento de imagens.

O método de verificação de assinaturas introduz uma nova técnica de extração de características de assinaturas, através da utilização das operações de erosão, dilatação, adição e subtração da morfologia matemática.

Tanto o classificador como as operações de MM utilizadas, possuem algoritmos simples de ser implementados no computador e são de rápido processamento.

Como parâmetros de desempenho do nosso sistema de verificação, obtivemos os valores de 14,6 % e 3,0 % de taxas de erros iguais frente a falsificações habilitadas e falsificações aleatórias, respectivamente.

8.2 Discussões

Nessa seção apresentaremos algumas colocações sobre o método de compressão de imagens e o método de verificação de assinaturas.

8.2.1 Discussão sobre o método de compressão de imagens de assinaturas estáticas

O método apresentado utiliza algoritmos clássicos de compressão de imagens aplicados a imagens de assinaturas. Porém, esse método pode chegar a taxas de compressão maiores se utilizarmos técnicas de quantização vetorial, o que permitiria melhorar a codificação de áreas específicas das imagens de assinaturas.

8.2.2 Discussão sobre o método de verificação de assinaturas estáticas

Constatamos que as características que compõem o vetor de representação de uma assinatura são consistentes, porém acreditamos que essas características se tornariam mais representativas se fizéssemos algumas modificações na etapa de pré-processamento da imagem. A principal mudança que deveria ser feita é utilizar as projeções vertical e horizontal da imagem para definir seu centro de gravidade. A partir daí, definiríamos uma área fixa em torno dela, na qual seria feita a extração de

características. Essa mudança deve melhorar o desempenho do sistema, diminuindo principalmente as taxas de erro frente a falsificações aleatórias.

Outro ponto importante que devemos modificar para melhorar o desempenho do sistema é a utilização de classificadores com maior poder de discriminação, tais como os implementados através de redes neurais [Lee93], ou neuro-*fuzzy*. A utilização desses tipos de classificadores deve diminuir as taxas de erro frente a falsificações habilitadas.

8.3 Conclusões

O sistema automático de verificação de assinaturas estáticas descrito nesse trabalho, apresenta um novo método de compressão e uma nova técnica de extração de características de imagens de assinaturas estáticas.

O método de compressão se mostra eficiente para minimizar o problema de armazenamento de arquivos de imagens de assinaturas, assim como para diminuir o tempo de transmissão desses arquivos através de redes de computadores.

A técnica de extração de características de inclinação dos traços e das bordas das assinaturas, é composto de algoritmos simples que implicam numa fácil implementação e processamento rápido.

As taxas de erro obtidas pelo sistema de verificação se encontram dentro dos resultados encontrados na literatura. Em específico, conseguimos o valor de 3,0 % de taxas de erros iguais frente a falsificações aleatórias e 14,6 % frente a falsificações habilitadas.

8.4 Continuação do trabalho e pesquisas futuras

Como continuação do trabalho aqui apresentado, investigaremos técnicas que possam ser utilizadas para aumentar as taxas de compressão de imagens de assinaturas em preto e branco, assim como em níveis de cinza. Também é nossa intenção investigar métodos de decisão baseados em redes neurais, que permitam classificar de maneira mais contundente os vetores de características de assinaturas estáticas.

Bibliografia

[Pender] Pender, Dorothy A., *Neural networks and handwritten signature verification.* Ph.D. thesis, Standford University, Standford, California, 1991

[Wilkinson] Wilkinson, Timothy S., *Novel techniques for handwritten signature verification.* Ph.D. thesis, Standford University, Standford, California, 1990

[Qi] Qi, Yingyong; e Hunt, Bobby R., "Signature verification using global and grid features," *Pattern Recognition*, Vol. 27, Nº 12, pp 1621-1629, 1994

[Nagel] Nagel, Roger N.; e Rosenfeld Azriel., "Computer detection of freehand forgeries," *IEEE Trans. on Computer*, Vol C-26, Nº 9, pp 895 - 905, 1977

[Ammar90] Ammar, Maan; et all., "Structural description and classification of signature images," *Pattern Recognition*, Vol. 23, Nº 7, pp 697-710, 1990

[Chuang] Chuang, Ping C., "Machine verification of handwritten signature image," *Proc. 1977 Int. Conf. on Crime Countermeasures - Sci. and Eng*, pp 105 - 109, Lexington (1977).

[Plamondon] Plamondon, Réjean; e Lorette, Guy, "Automatic signature verification and writer identification - the state of art," *Pattern Recognition*, Vol. 22, Nº 2, pp 107-131, 1989

[Weszka] Weszka, Joan; e Rosenfeld, Azriel, "Histogram modification for threshold selection," *IEEE Trans. on Systems, Man. and Cybernatics*, Vol. SMC-9, Nº 1, 1979

[Brocklehurst] Brocklehurst, Er, "Computer methos of signature verification," *Journal of the Forensic Science Society*, Vol 25, pp 445-457, 1985

[Nemcek] Nemcek, Walter F; Lin, Wen C., "Experimental investigation of automatic signature verification," *IEEE Trans. on Systems, Man, and Cybernatics*, Vol. SMC-4, Nº 1, 1974

[Gomes] Gomes, Herman Martins et all., "Detecção de falsificações habilidosas na verificação estática de assinaturas via MLP-Backpropagation," *II Simpósio Brasileiro de Redes Neurais*, pp 28 - 33, São Carlos, (1995)

[Lizárraga] Lizárraga, Miguel G; e Lee, Luan L., "Um Método de compressão de imagens de assinaturas estáticas para um sistema de identificação pessoal," *Anais do VIII Simposio Brasileiro de computação gráfica e processamento de imagens*, pp 67 - 71, São Carlos, (1995)

[Ammar86] Ammar, Maan; et all., "A new effective approach for off-line verification of signatures by using pressure features," *Proc. 8th Int. Conf. on Pattern Recognition*, pp 566-569, Paris, 1986

[Serra] Serra, Jean., "Introduction to mathematical morphology," *Computer vision, graphics, and imagem procesing*, Vol. 35, pp 283 - 332, 1986

[Searfoss] Searfoss, Glenn, "Bounding box data compression," *Dr. Dobb's Journal*, april, 1990

[Boccignone] Boccignone, G. A; et all., "Recovering dynamic information from static handwriting," *Pattern Recognition*, Vol. 26, Nº 3, pp 409 - 418, 1993

[Banon] Banon, Gerald J; e Barrera, Junior, *Bases da morfologia matemática, IX Escola de Computação*, Recife, (1994)

[Leclerc] Leclerc, F.; e Plamondon, R., "Automatic signature verification: the state of art - 1989-1993," *Int. Journal of Pattern Recognition and Art. Intelligence*, Vol 8, Nº 3, pp 643 - 660, 1994

[Cardot] Cardot, Hubert; e Revenu, Marinette, "A static signature verification system based on a cooperating neural networks architecture," *Int. Journal of Pattern Recognition and Art. Intelligence*, Vol 8, Nº 3, pp 679 - 692, 1994

[Yoshimura] Yoshimura, Isao; e Yoshimura, Mitsu, "Off-line verification of japanese signatures fater elimination of background patterns," *Int. Journal of Pattern Recognition and Art. Intelligence*, Vol 8, Nº 3, pp 693 - 708, 1994

[Gonzales] Gonzales, R. C; e Woods, R. E., *Digital Image Processing*. MA: Addison Wesley, 1992

[Lee92] Lee, Luan Ling, *On-line system for human siganture verification*, Ph.D. thesis, Cornell University, 1991

[Huffman] Huffman, D. A, "A method for construction of minimum redundancy codes," *Proc. IRE*, Vol 40, Nº 10, pp 1098-1101, 1952.

[Pentland] Pentland, Alex; e Horowitz, Bradley, *A practical approach to fractal-based imagem compression*, M.I.T Media Lab. vision and Modelling Group, Technical Report Nº 152.

[Mantas] Mantas, J., "Methodologies in pattern recognition and image analysis - A brief survey," *Pattern Recognition*, Vol 20, Nº 1, pp 1-6, 1987.

[Arazi] Arazi, Benjamin, "Automatic handwriting identification based on the external properties of the samples," *IEEE Trans. on System, Man, and Cybernatics*, Vol. SMC-13, Nº 4, pp 635-642, 1983.

[Lindgren] Lindgren, Nilo, "Machine recognition of human language - Part III - Cursive script recognition," *IEEE Spectrum*, May 1965.

[Powalka] Powalka, R. K; et all, "Feature extraction: on the importance of zoning information in cursive script recognition," *Progress in Image Analysis and Processing III*, pp 342-349, 1994.

[Eden] Eden, Murray. "Handwriting and pattern recognition," *IRE Trans. on Inf. Theory*, IT-8, February 1962.

[Senior] Senior, A. W., *Off-line handwriting recognition: a review and experiments*. Technical Report CUED/F-INFENG/TR 105

[Duda] Duda, R.; Hart, P. E., *Pattern classification and Scene analysis*, New York, Wiley, 1973.

[Lee93] Lee, Luan Ling; Berger T., "On two patterns classification using neural network," *Int. Conf. Signal Processing - ICSP'93*, Beijing - China, 1993.

[Ranganathan] Ranganathan, N.; et all., "A lossless image compression algorithm using variable block size segmentation," *Int. Conf. on Pattern Recognition - 12th ICPR*, Jerusalem, Israel, 1994