PROTEÇÃO DA PROVA DOCUMENTAL IMPRESSA E DIGITALIZADA COM A UTILIZAÇÃO DE *WATERMARKING*

FELIPPE PIRES FERREIRA

DISSERTAÇÃO DE MESTRADO EM ENGENHARIA ELÉTRICA
DEPARTAMENTO DE ENGENHARIA ELÉTRICA

FACULDADE DE TECNOLOGIA

UNIVERSIDADE DE BRASÍLIA

UNIVERSIDADE DE BRASÍLIA
FACULDADE DE TECNOLOGIA
DEPARTAMENTO DE ENGENHARIA ELÉTRICA

Proteção da Prova Documental Impressa e Digitalizada com a Utilização de *Watermarking*

Felippe Pires Ferreira

ORIENTADOR: WARLEY GRAMACHO DA SILVA

DISSERTAÇÃO DE MESTRADO EM ENGENHARIA ELÉTRICA
ÁREA DE CONCENTRAÇÃO INFORMÁTICA FORENSE E SEGURANÇA DA INFORMAÇÃO

PUBLICAÇÃO: PPGENE.DM - 619/2016

BRASÍLIA / DF: 11/2016

UNIVERSIDADE DE BRASÍLIA
FACULDADE DE TECNOLOGIA
DEPARTAMENTO DE ENGENHARIA ELÉTRICA

PROTEÇÃO DA PROVA DOCUMENTAL IMPRESSA E DIGITALIZADA COM A UTILIZAÇÃO DE *WATERMARKING*

FELIPPE PIRES FERREIRA

DISSERTAÇÃO DE MESTRADO SUBMETIDA AO DEPARTAMENTO DE ENGENHARIA ELÉTRICA DA FACULDADE DE TECNOLOGIA DA UNIVERSIDADE DE BRASÍLIA, COMO PARTE DOS REQUISITOS NECESSÁRIOS PARA A OBTENÇÃO DO GRAU DE MESTRE PROFISSIONAL EM INFORMÁTICA FORENSE E SEGURANÇA DA INFORMAÇÃO.

APROVADA POR:

WARLEY GRAMACHO DA SILVA, Dr., UFT
(ORIENTADOR)

FLÁVIO ELIAS GOMES DE DEUS, Dr., ENE/UNB
(EXAMINADOR INTERNO)

ARI HENRIQUE MORAIS DE OLIVERIA, Dr., UFT
(EXAMINADOR EXTERNO)

BRUNO WERNECK PINTO HOELZ, D.R. ENE/UNB
(SUPLENTE)

DATA: BRASÍLIA/DF, 07 DE NOVEMBRO DE 2016.

FICHA CATALOGRÁFICA

FERREIRA, FELIPPE PIRES
Proteção da Prova Documental Impressa e Digitalizada com a Utilização de Watermarking [Distrito Federal] 2016.
xxv, 86p., 297 mm (ENE/FT/UnB, Mestre, Engenharia Elétrica, 2016).

Dissertação de Mestrado – Universidade de Brasília, Faculdade de Tecnologia. Departamento de Engenharia Elétrica.

1. Marca d'água 2. Watermarking
3. Cópia de Documento 4. Digitalização
5. Fonte de Texto 6. Documento Sigiloso

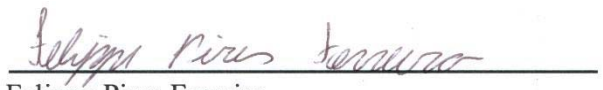
I. ENE/FT/UnB. II. Título (Série)

REFERÊNCIA BIBLIOGRÁFICA

FERREIRA, Felippe Pires. (2016). Proteção da Prova Documental Impressa e Digitalizada com a Utilização de Watermarking. Dissertação de Mestrado, Publicação PPGENE.DM - 619/2016, Departamento de Engenharia Elétrica, Universidade de Brasília, Brasília, DF, 84p.

CESSÃO DE DIREITOS

NOME DO AUTOR: Felippe Pires Ferreira
TÍTULO DA DISSERTAÇÃO: Proteção da Prova Documental Impressa e Digitalizada com a Utilização de Watermarking.
GRAU/ANO: Mestre/2016.



Felippe Pires Ferreira
Universidade de Brasília
Campus Universitário Darcy Ribeiro – Asa Norte
CEP 70.910-900 – Brasília – DF - Brasil

À minha esposa Marta. Amor, não poderia descrever a moção que me toma ao registrar estas palavras. Sem a sua ajuda, eu não teria alcançado tal objetivo.

A meus pais Wilck e Filinha e a meus irmãos. Eu os amo profundamente. Todos os momentos que vivemos juntos são um privilégio concedido por Deus.

Amados pais, eu sigo o caminho da dignidade, da luta e da fé que sempre buscaram ensinar-me.

Amados irmãos, juntos, a vida pode nos vergar, mas jamais romperá a resistência que a união familiar nos conferiu.

AGRADECIMENTOS

Ao meu orientador Prof. Dr. WARLEY GRAMACHO DA SILVA, pelo constante apoio e incentivo para o desenvolvimento deste trabalho e para o meu desenvolvimento como pesquisador.

À minha família pelo apoio nas etapas cansativas e desafiadoras deste Mestrado Profissional, que me apoio em momentos difíceis.

A todos, os meus sinceros agradecimentos.

O presente trabalho foi realizado com o apoio do Departamento Polícia Federal, com recursos do Programa Nacional de Segurança Pública com Cidadania – PRONASCI, do Ministério da Justiça.

RESUMO
PROTEÇÃO DA PROVA DOCUMENTAL IMPRESSA E DIGITALIZADA COM A UTILIZAÇÃO DE WATERMARKING

Autor: Felippe Pires Ferreira
Orientador: Warley Gramacho da Silva
Programa de Pós-graduação em Engenharia Elétrica
Brasília, 11 de 2016

Neste trabalho é proposto um método para disponibilização de documentos sigilosos durante inquéritos policiais, processos judiciais, ou que exijam compartimentalização das informações, introduzindo o elemento de segurança conhecido como *watermark* nas cópias dos documentos. O principal objetivo é permitir vincular este elemento a uma cópia de documento a seu destinatário inicial, e em casos de vazamento de informação permitirá identificar a origem da cópia. O método é baseado na semelhança entre caracteres de diferentes fontes de texto, os quais serão utilizados para criação de uma codificação identificadora da origem do documento, e possibilitar a inclusão de uma *watermark* em um documento eletrônico editável, bem como recuperá-la em documentos impressos ou digitalizados, bastando apenas um fragmento do texto.

ABSTRACT
PROTECTION OF DOCUMENTARY EVIDENCE PRINTED AND SCANNED WITH WATERMARKING

Author: Felippe Pires Ferreira
Supervisor: Warley Gramacho da Silva
Programa de Pós-graduação em Engenharia Elétrica
Brasília, November of 2016

This work proposed a method for available classified documents during the police investigation, judicial proceedings, or requiring compartmentalization of information, introducing the security element known as watermarking in copies of documents. This element will link a document copy to its initial recipient, and in cases of information leakage will identify the origin of the copy. The method is based on the similarity between characters of different fonts of text, which will be used to create a code identifying of the origin document, and include a watermark in an editable electronic document and retrieve it in printed or scanned documents, just by a fragment of text.

SUMÁRIO

LISTA DE TABELAS

LISTA DE FIGURAS

LISTA DE SÍMBOLOS, NOMENCLATURA E ABREVIAÇÕES

LSB (*LEAST SIGNIFICANT BIT***)** – ALGORITMO UTILIZADO PRINCIPALMENTE EM ESTEGANOGRAFIA;

DCT (*DISCRETE COSINE TRANSFORM***)** - ALGORITMO PARA PROCESSAMENTO DE IMAGENS;

DWT (*DISCRETE WAVELET TRANSFORM***)** – ALGORITMO PARA PROCESSAMENTO DE IMAGENS;

***PAYLOAD* –** DADOS EFETIVAMENTE UTILIZADOS DURANTE O TRANSPORTE DE UMA MENSAGEM OU PACOTE DE DADOS**;**

PSNR (*PEAK SIGNAL TO NOISE RATIO*) – MÉTODO PARA DEFINIR A RELAÇÃO ENTRE UM SINAL E O RUÍDO QUE AFETA SUA REPRESENTAÇÃO FIDEDIGNA;

MSE (*MEAN SQUARE ERROR*) **–** MEDIDA ESTATÍSTICA DA MÉDIA DO QUADRADO DOS ERROS;

RMSE (*ROOT MEAN SQUARE ERROR*) – RAÍZ QUADRADA DO MSE;

SSIM (*STRUCTURAL SIMILARITY INDEX*) – MÉTODO PARA AVALIAR A QUALIDADE PERCEBIDA DE IMAGENS E VÍDEOS;

JPEG (*JOINT PHOTOGRAPHIC EXPERTS GROUP*) – MÉTODO DE COMPRESSÃO COM PERDAS DE IMAGENS DIGITAIS;

LINE SHIFT CODING – MÉTODO DE WATERMARKING COM DESLOCAMENTO DE LINHAS;

WORD SHIFT CODING – MÉTODO DE WATERMARKING COM DESLOCAMENTO DE PALAVRAS;

CHARACTER CODING – MÉTODO DE WATERMARKING COM ALTERAÇÃO DE FORMATAÇÃO DE ELEMENTOS TEXTUAIS;

OCR (*OPTICAL CHARACTER RECOGNITION*) **–** MECANISMO QUE PERMITE CONVERTER DOCUMENTOS DIGITALIZADOS EM DOCUMENTOS INDEXÁVEIS;

***TRADE-OFF* –** SITUAÇÃO EM QUE HÁ CONFLITO DE ESCOLHA;

DOCX – EXTENSÃO DE ARQUIVOS DE TEXTO DO SOFTWARE PROPRIETÁRIO MICROSOFT WORD A PARTIR DA VERSÃO 2007;

CALADEA – FONTE TEXTUAL UTILIZADA EM EDITORES DE TEXTO;

TIMES NEW ROMAN – FONTE TEXTUAL UTILIZADA EM EDITORES DE TEXTO;

BASE64 – MÉTODO DE CODIFICAÇÃO DE DADOS PARA TRANSFERÊNCIA NA INTERNET;

ASCII (*AMERICAN STANDARD CODE FOR INFORMATION INTERCHANGE*) – PADRÃO DE CODIFICAÇÃO DE CARACTERES QUE UTILIZA 8 BITS PARA CADA SÍMBOLO;

DPI (*Dots per inch*) – Relaciona o número de pontos presentes em uma polegada linear na superfície onde a imagem é apresentada;

Pixel – Menor elemento formador de uma imagem digital;

Open-Source – Modelo de desenvolvimento de software que permite a distribuição de seu código-fonte;

Tesseract OCR – *Engine* OCR *open-source* que pode ser adicionada em softwares;

ImageJ – Software *open-source* em linguagem Java que permite processamento e análise de imagens;

SUB – Função de subtração, do software ImageJ, entre pixels na mesma posição de duas imagens;

Java – linguagem de programação interpretada que utiliza uma máquina virtual para execução de seu código;

DSCQS (*Double Stimulus Quality Scale Method*) – Método para avaliar o nível de qualidade de duas imagens ou vídeos;

MOS (*Mean Opinion Score*) – Método subjetivo de teste de qualidade;

GAECO (Grupo de Atuação Especial de Repressão ao Crime Organizado) – Unidade de investigação dirigida por Promotores de Justiça para combater o Crime Organizado.

RGB – Abreviatura do sistema de cores aditivas formado por Vermelho (**R**ed), Verde (**G**reen) e Azul (**B**lue).

1. INTRODUÇÃO

A difusão da informação com o auxílio dos avanços da tecnologia foi inicialmente aceita como grande revolução na comunicação. A facilidade de se difundir conhecimento por meio de documentos e publicações por pessoas a quilômetros de distância, permitindo rapidez e dinamismo ao processo de comunicação, modificou os caminhos e as formas da comunicação (Panah, 2016). Entretanto, a crescente difusão de conhecimento também proporciona a prática de publicação de material não autorizado por meio da Internet. Diversos livros, artigos e documentos de trabalho também foram objeto dessa popularização e disseminação da prática de compartilhamento de documentos on-line (Ahmadi, 2014).

Além da publicação não autorizada de propriedade intelectual, o vazamento de informações sigilosas é uma consequência da disseminação de informação sem controle, e também foco de noticiários, como pode ser observado nas reportagens de Skodowski (2015) e Oliveira (2016) sobre vazamento de documentos de investigações policiais relacionadas a uma operação da Polícia Federal. Diferentes documentos oficiais sigilosos relacionados a investigações policiais ou processos judiciais são publicados, o que pode gerar prejuízos aos procedimentos e às partes envolvidas.

Documentos como inquéritos policiais e processos judiciais, por tramitarem em diferentes órgãos e envolverem várias pessoas, podem ser acessados por diferentes partes, como advogados, servidores públicos, estagiários, entre outros. Isto aumenta o risco de comprometimento da informação, aumentando a dificuldade de controle de acesso a tais documentos.

Neste novo cenário, surgiu a necessidade de criação de um mecanismo de proteção à produção intelectual dos autores e dos documentos. Entretanto, essa proteção precisa ser robusta o suficiente para que não seja removível, capaz de ser recuperável, além de identificar integralmente o material. Segundo Ahmadi (2014), dessa necessidade de proteção da propriedade intelectual foi criado o conceito de *watermarking*, ou termo traduzido marca d'água.

Segundo Katariya (2012)*, watermarking* é o processo de inserção de informações acerca do objeto no próprio objeto, de forma que essa informação possa ser extraída posteriormente para ser verificada e validada. Ou seja, uma mensagem é criada a partir de informações de um documento, por exemplo, e esta mensagem é introduzida no documento, de forma oculta ou não, podendo ser extraída posteriormente. Diferente da esteganografia, que tem como objetivo

a ocultação da informação, a *watermark* não procura ser totalmente eficiente contra detecções, mas objetiva identificar um material, e impossibilitar que este elemento seja removida ou alterada por pessoas não autorizadas (Zhang, 2010).

De acordo com Cox (2008) e Woo (2007), algoritmos de *watermarking* possuem diferentes aplicações, dentre elas a de permitir a identificação de proprietários de materiais, de forma a proteger a sua distribuição em outros formatos multimídia (áudio, imagens, textos, vídeos). Muitas vezes a *watermark* não está oculta e apresenta informações sobre o proprietário do material. A autenticidade do material pode ser verificada, com outros mecanismos de segurança, como a criptografia, de forma a contribuir para a confirmação da origem da informação e sua veracidade. Caso ocorra alguma modificação do material, a verificação da integridade da *watermark* pode indicar que houve manipulação não autorizada sobre este. É possível realizar o controle de cópias personalizando as *watermarks* de acordo com o destinatário do material, possibilitando o rastreio do material em caso de vazamentos que são divulgações não autorizadas de materiais.

Para Cox (2008), o procedimento de *watermarking* contém propriedades que devem estar presentes quando aplicada a um objeto, a fim de torná-la útil. Os autores Ahmadi (2014) e Mohanty (1999) citam algumas características que *watermarks* devem conter: a robustez, deste modo ser resistente a manipulação do material e ainda permanecer neste; Deve ser imperceptível a visão humana, sendo visível apenas durante processos de extração da informação; Ser segura, assim apenas o proprietário do material poderá recuperá-la, alterá-la ou removê-la; E por fim, deve ser capaz de armazenar informação/mensagem em um objeto.

Outro aspecto são os diferentes suportes/materiais em que podem ser inseridas. De acordo com o tipo de arquivo de mídia são utilizadas técnicas diferentes. É possível utilizá-la em arquivos de texto, imagens, áudio e vídeo. Cada tipo de arquivo possui técnicas adequadas a seu contexto, mas todas devem buscar as propriedades que tornam as *watermarks* "fortes" como os autores Cox (2008) e Mohanty (1999) descrevem.

Não há registro de bibliografia referente à utilização de *watermarks* em documentos produzidos em inquéritos policiais ou processos judiciais. Quando esse elemento é utilizado nestes documentos não existe o objetivo de se ocultar esta informação. A *watermark* é visível e tem a função de identificar o documento por meio desta marcação. Dessa maneira, o objetivo do trabalho é propor um processo de *watermarking* que permita a inserção do elemento de segurança em um documento digital eletrônico, de modo que não seja perceptível ao leitor do

documento, e posteriormente, seja recuperável em uma cópia impressa ou digitalizada do documento.

A dissertação foi dividida em 8 capítulos, a fim de organizar a explanação sobre o tema e apresentar a metodologia proposta. O capítulo 1 apresentou uma visão geral do que será abordado no trabalho, contextualizando, justificando e traçando os objetivos da solução proposta. No capítulo 2 é apresentado o termo *watermarking*, além de suas características e aplicações. No capítulo seguinte são apresentadas as metodologia de *watermarking* para documentos textuais, além de trabalhos correlatos na área. O capítulo 4 cita as características apontadas por diferentes autores como sendo importantes em algoritmos de *watermarking*, portanto tais características devem ser observadas em novas técnicas.

O método proposto é apresentado no capítulo 5, ilustrando os algoritmos de inserção e recuperação das *watermarks*, além dos aspectos principais da técnica proposta. Para validação e mensuração do método proposto, o capítulo seguinte descreve diversos testes aplicados à técnica, e consequentemente a análise sobre os resultados obtidos em cada um dos testes. Um estudo de caso foi inserido no capítulo 7, a fim de observar a metodologia em um ambiente real com documentos sigilosos. Por fim, são apresentados as conclusões obtidas e expectativas para trabalhos futuros na área.

2. *WATERMARKING*

A utilização de mídias ou documentos digitais se tornou comum por certas vantagens, tais como: eficiência na armazenagem, duplicação, manipulação e transmissão de documentos, além de possibilitar a realização de cópias sem perda de dados. Podemos citar como exemplos de mídias digitais arquivos de imagens, áudio, vídeo e documentos textuais (Katariya, 2012). Entretanto, a disseminação desses materiais resultou no "surgimento" de um conjunto de problemas e, consequentemente, um grande número de desafios. Dentre os problemas pode-se dar destaque ao aumento de cópias não autorizada de arquivos, falsificação, remoção de identificações de autores em materiais, entre outros.

A violação de direitos de propriedade intelectual e a disseminação de conteúdo não autorizado pela Internet criou a necessidade de um mecanismo de proteção dos direitos autorais sobre as produções intelectuais. Uma das soluções propostas foi introduzir uma estrutura visível ou invisível e que permanecesse nas mídias digitais mesmo após processos de transmissão de dados. A estrutura foi conhecida como "*Digital Watermark*" e o processo de incluí-la nas mídias de "*Digital Watermarking*" (Katariya, 2012).

A *Watermark* é um sinal digital ou padrão inserido em um documento digital (texto, imagem, multimídia) com a finalidade de introduzir um elemento de segurança dentro de um documento com informações sobre o próprio documento (Berghel, 1997). Desta forma, com a *watermarking* é possível inserir uma mensagem dentro de um arquivo e para, posteriormente, realizar a recuperação desta mensagem para fins diversos, por exemplo, para a verificação da autenticidade integridade do arquivo ou da própria mensagem. Tao (2014) defende que a *watermark* possibilita a proteção da propriedade intelectual e garante proteção contra adulterações, devido a ela ser de difícil discernimento e remoção por pessoas não autorizadas.

Um sistema de *Watermarking,* segundo Mohanty (1999) e ilustrado pela Figura 2.1 – **Etapas para criação de um sistema de *Watermarking*.**, pode ser descrito em três etapas: geração da *watermark*, inclusão do elemento na mídia e recuperação da *watermark*. Um dos propósitos da *watermark* é proteger a propriedade intelectual que está em um formato digital, além de permitir a identificação do proprietário, autenticar o conteúdo da mídia, controlar as cópias do material, entre outras funções (Katariya, 2012).

Figura 2.1 – Etapas para criação de um sistema de *Watermarking*.

2.1. CRITÉRIOS DE CLASSIFICAÇÃO DE ALGORITMOS DE *WATERMARKING*

Autores como Katariya (2012) e Cox (2008) classificam *Watermarking* de acordo com características presentes no mecanismo ou no contexto em que ela será inserida (tipo de mídia). Algumas classificações sugeridas pela literatura são listadas a seguir (Katariya, 2012):

Robustez – Pode ser classificada de duas formas distintas, segundo o critério de robustez: frágil ou robusta. Uma *watermark* robusta é capaz de resistir a ataques sem sofrer alterações ou ser retirada do documento onde está inserida. A frágil, por definição, é o oposto da robusta, sendo passível de remoção ou alteração. Mesmo que não resista a um processo de edição ou compressão, *watermarks* frágeis ainda possuem aplicações. Ela poderia ser utilizada em processos de verificação de integridade do conteúdo, uma vez que uma simples alteração poderia impactar a *watermark* inserida. Desta forma, seria possível descobrir alterações no documento, de acordo com o estado de uma *watermark* frágil, devido a sua alta sensibilidade a manipulações;

Tipo de mídia – diferentes tipos de arquivos podem ser utilizados para introduzir uma *watermark*, entretanto para cada tipo são utilizados algoritmos e técnicas diferentes. Além

disso, os ataques e características que cada mídia pode suportar e apresentar também podem ser diferentes. Por exemplo, ataques de rotação podem destruir *watermarks* em imagens, entretanto não afetariam arquivos de texto. Além disso, a utilização da técnica LSB (*Least Significant Bit*), por exemplo, em arquivos de áudio pode não ser eficiente quando comparado a arquivos de imagem ou vídeo;

Perceptibilidade – as *watermarks* podem ser invisíveis ou visíveis dependendo da aplicação e objetivos pela qual ela foi desenvolvida e inserida no documento. A aplicação de *watermarks* visíveis é encontrada em materiais disponibilizados na Internet, como imagens, as quais são introduzidas com a finalidade de preservar a propriedade intelectual do autor. Enquanto, *watermarks* invisíveis podem ser utilizadas para detectar utilizações ou compartilhamentos indevidos de documentos e provar a real propriedade do material (Mohanty, 1999).

Existem ainda outras formas de classificação de algoritmos de *watermarking*. Mohanty (1999) classifica as *watermarks* em 04 diferentes grupos, conforme apresentado na Figura 2.2: Domínio de trabalho, tipo de documento, percepção humana e aplicação. O grupo de *watermarks* de domínio possui duas subclassificações: espacial ou frequência. Nas *watermarks* espaciais a informação é introduzida através de modificações de valores de bits ou pixels, como o algoritmo LSB em imagens, onde cada alteração não apresenta relação com alterações anteriores ou futuras. O domínio da frequência utiliza transformações matemáticas em trechos do arquivo, como as técnicas DCT (*Discrete Cosine Transform*) e DWT (*Discrete Wavelet Transform*), as quais antes de realizarem as alterações analisam diversos aspectos das características do documento, como a relação dos *pixels* presentes no arquivo.

A categorização por Tipo de documento é baseada no suporte que irá receber a *watermark*, logo a metodologia e as propriedades da *watermarking* irão depender do tipo de documento utilizado. A classificação por Percepção humana se baseia nos sentidos humanos, principalmente visão e audição. E por fim, a classificação por Aplicação possui *watermarks* Baseado na Origem, em que todas as cópias dos documentos recebem as mesmas *watermarks,* o que pode auxiliar na autenticação dos materiais, e Baseado no Destino, em que o documento recebe uma *watermark* de identificação específica para cada comprador/destinatário, assim permitindo a identificação do comprador em casos de venda ou cópias não autorizadas (Mohanty, 1999).

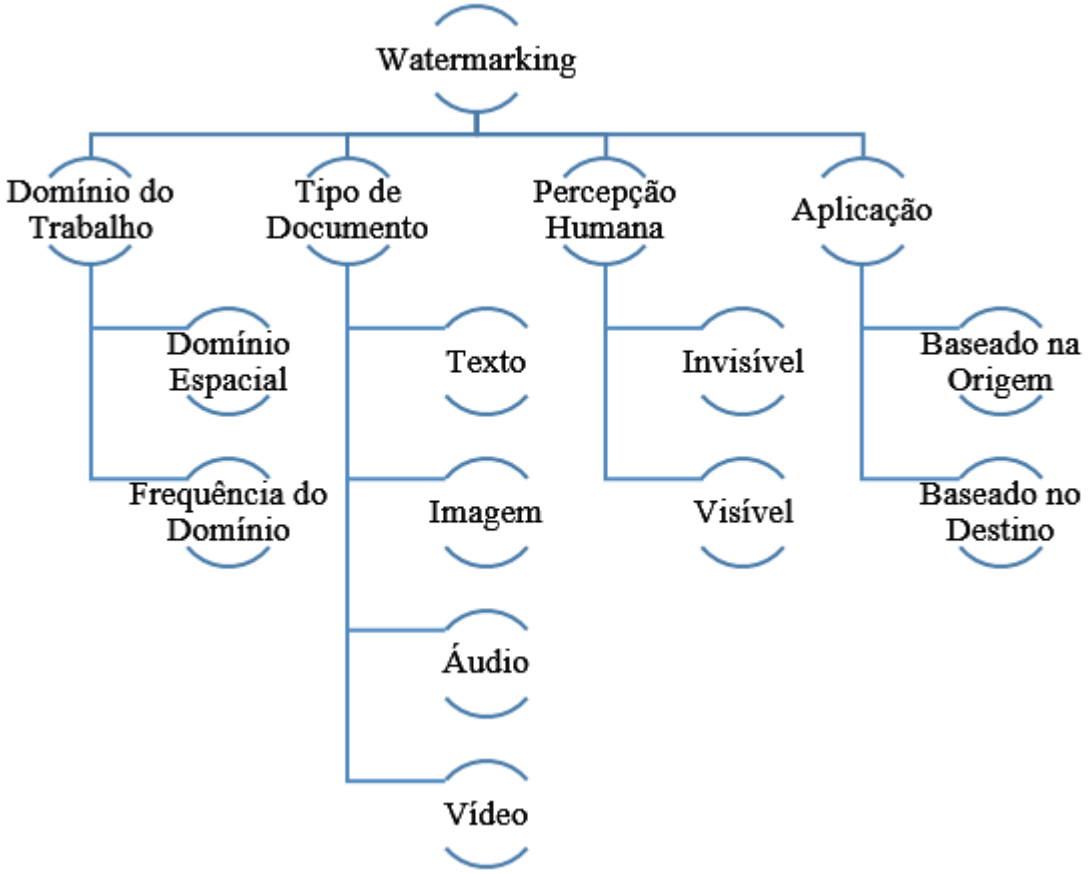


Figura 2.2 - Classificações de *watermarks* (Mohanty, 1999).

2.2. ESTEGANOGRAFIA E *WATERMARKING*

Watermarking é uma técnica que possui uma origem comum com a esteganografia, a ocultação da informação (Figura 2.3). O uso de *watermarks* é quase tão antigo quanto à fabricação de papel. Os povos antigos introduziam materiais entre as fibras do papel e água nos moldes de fabricação, e aplicavam sobre eles grandes pressões (Berghel, 1997).

A esteganografia e a *watermarking* são subgrupos dentro da categoria de ocultação de informação (Figura 2.3). A distinção basicamente é feita por suas características e aplicações conforme explicado a seguir.

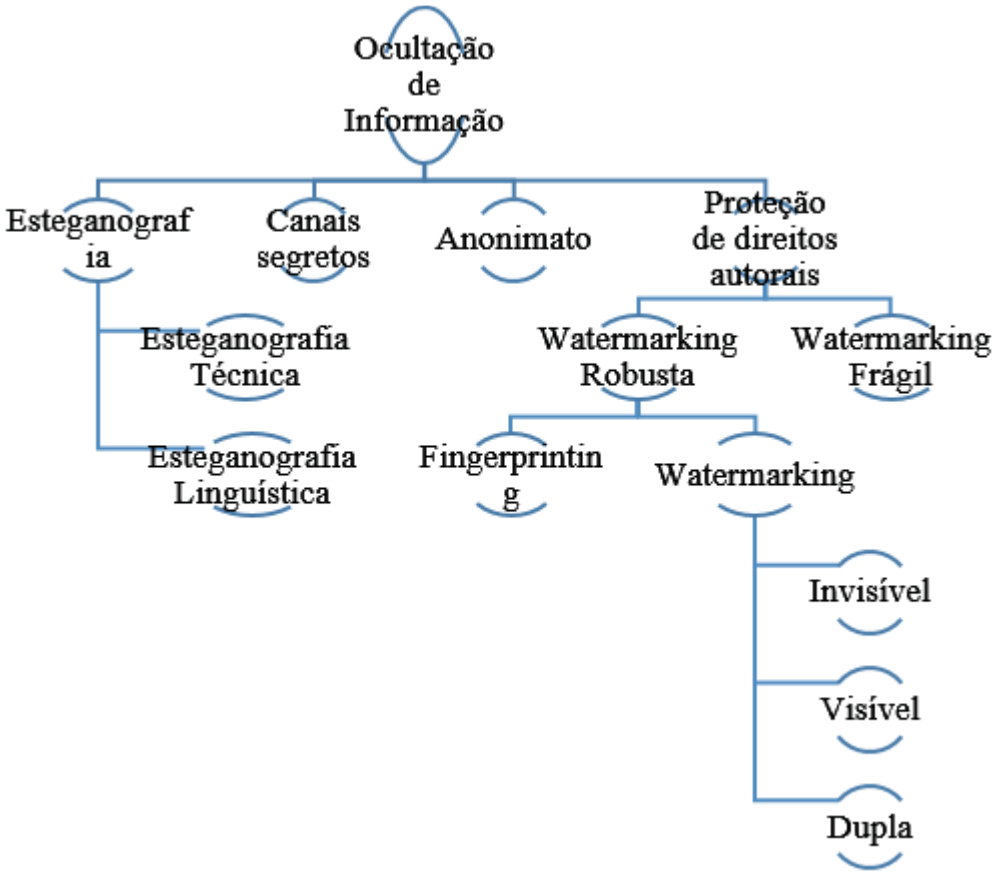


Figura 2.3 - Subclassificações de técnicas de ocultação de informação (Mohanty, 1999).

A distinção entre *watermarking* e esteganografia é feita com base no propósito de sua utilização e quão perceptível é a mensagem introduzida no objeto. Segundo Cox (2008), as duas técnicas são classificadas como "ocultação de informações". Enquanto a *watermarking* é a prática de realizar alterações pouco perceptíveis em um conteúdo, acrescentando a ele uma mensagem com referências ao próprio conteúdo ou autor. A esteganografia tem por objetivo tornar imperceptível uma mensagem dentro de um conteúdo (Cox, 2008).

Segundo Tao (2014), uma *watermarking* digital surge com a finalidade de atuar nas limitações da criptografia e da esteganografia, garantindo e protegendo os direitos da propriedade intelectual. Quando comparada com a criptografia, a *watermark* é inserida sobre o material original, não impedindo que usuários ouçam, visualizem ou manipulem o conteúdo do material, enquanto a criptografia impossibilita o acesso ao conteúdo sem a chave criptográfica. E ao contrário da esteganografia, *watermarkings* são usadas para identificar informações e evitar fraudes sobre esses materiais.

Conforme abordado na seção 2.2, a *watermarking* pode ser classificada de acordo com o nível de perceptibilidade de sua mensagem como: invisível ou visível. Enquanto a

esteganografia pode ser classificada como: de mensagem secreta e de mensagem não necessariamente secreta. Segundo (Mohanty, 1999), a *watermark* possui algum significado relacionado ao objeto em que ela está inserida. Enquanto, a esteganografia não precisa manter relação com o objeto no qual a mensagem foi inserida.

.

Um sistema genérico de utilização de *watermarking* ou esteganografia pode ser representado conforme o esquema descrito na Figura 2.4 **- Sistema genérico para inclusão e detecção de mensagens aplicável à *watermarking* e esteganografia (Cox, 2008).**4:

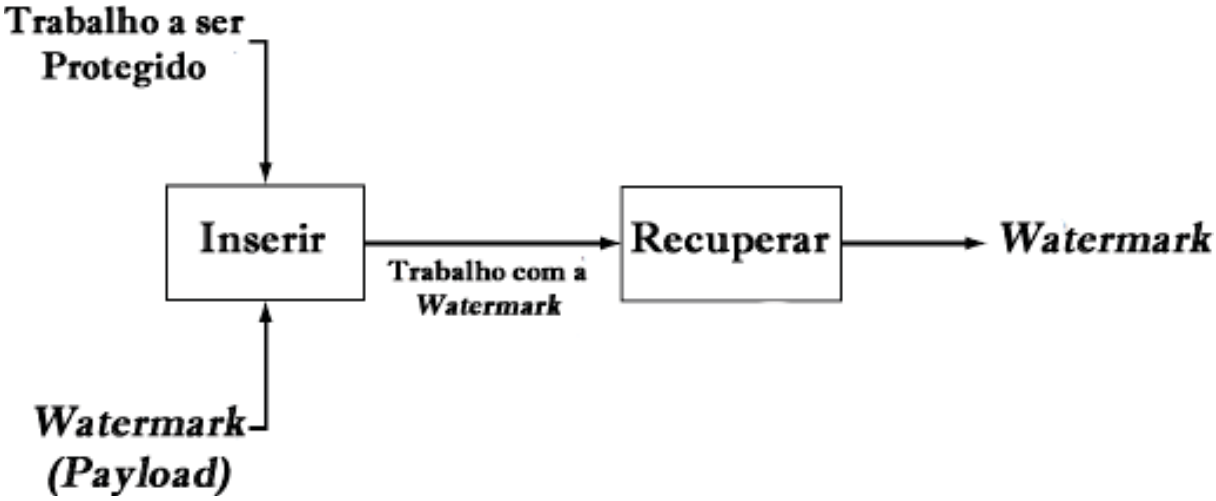


Figura 2.4 - Sistema genérico para inclusão e detecção de mensagens aplicável à *watermarking* e esteganografia (Cox, 2008).

De acordo com Cox (2008), um *payload*/mensagem é adicionado a um objeto, produzindo um arquivo com uma informação oculta. Então um terceiro habilitado para encontrar a mensagem oculta extrairia o *payload* inserido no objeto. Portanto, este sistema possui pelo menos duas etapas: a inclusão da mensagem oculta e sua extração.

Na década de 90 a utilização de métodos de *watermarking* se tornou comum em diversos arquivos, principalmente, áudio e vídeo. Alguns dos objetivos dessa utilização eram identificar o proprietário de determinado arquivo, sinalizar que o proprietário do objeto possuía direito de cópia sobre a informação ou verificar se o conteúdo não sofreu nenhum tipo de alteração (Cox, 2008).

2.3. APLICAÇÕES MAIS FREQUENTES DE *WATERMARKING*

Assim como a esteganografia, a *watermarking* possui diferentes contextos de aplicação os quais buscam objetivos diferentes. Ameaças presentes em um novo contexto da utilização da Internet contribuíram para o desenvolvimento do tema "Gerenciamento de Direitos Digitais" (Woo, 2007). Podemos citar como alguns exemplos de ameaças: o aumento de conteúdo digitalizado e distribuído ilegalmente; avanços nos mecanismos de comunicação que permitem compartilhamento de grandes quantidades de informação de forma mais eficiente e rápida; e softwares de manipulação de conteúdos digitais. Estes são exemplos que motivaram a aplicação de mecanismos de controle sobre a propriedade intelectual digital. Nas próximas subseções são listadas algumas funções em que *watermarks* podem ser utilizadas.

2.3.1. Identificação do Proprietário

Criadores de obras de arte, produções literais ou científicas, quando publicam seus trabalhos à comunidade, buscam realizar essas distribuições sem perder seus direitos sobre seu trabalho. É preciso introduzir um mecanismo que garantam seus direitos sobre as cópias distribuídas. As produções intelectuais quando transformadas em um registro físico, normalmente, recebem alguma forma de identificação para proteger a obra artística ou científica. Entretanto, mesmo com a inclusão de mecanismo de identificação do proprietário em trabalhos e produções artísticas ou cientificas, alguns desses produtos ainda são passíveis de serem alterados e terem suas identificações suprimidas ou removidas dos trabalhos originais. Isto ocorre principalmente em documentos textuais ou de imagens que contenham símbolos de identificação do autor. Estes registros podem ter suas identificações suprimidas durante processos de fotocópia ou por softwares de edição de imagens (Cox, 2008).

Segundo Tao (2014), essa foi uma das primeiras aplicações de *watermarks* em arquivos digitais. Os metadados do material continham informações do detentor dos direitos da propriedade intelectual, e imperceptivelmente essas informações são inseridas no material através de uma *watermarking*.

Mohanty (1999) cita a possibilidade de utilização de *watermarks* visíveis e invisíveis para identificação da propriedade intelectual. Segundo o autor, as *watermarks* visíveis são utilizadas em materiais disponibilizados livremente, principalmente pela Internet, sem pagamento de *royalties*, cujo objetivo é apenas publicidade sob o conteúdo. Enquanto, as

watermarks invisíveis estão em materiais comercializados, mas que mantém o direito de propriedade do autor.

2.3.2. Comprovação da Propriedade

Diferente de apenas indicar quem seria o possível autor de determinado documento, a *watermark* pode ser utilizada para comprovar a autoria de fato do trabalho. Um mecanismo de identificação, mas de fácil remoção, torna-se uma brecha para a existência de fraudes e cópias não autorizadas. Segundo Song (2012), uma *watermark* pode ser embutida em um material para garantir a proteção da propriedade intelectual do autor. Desta forma, quando for necessário comprovar a autoria do material, a *watermark* será extraída e analisada.

Para que haja uma forma de comprovação da autoria de um trabalho, ou o autor possui rascunhos do trabalho, e até mesmo o trabalho original, ou os procedimentos de remoção e geração da *watermark* não possam ser reproduzidos por outra pessoa que não o autor da obra. É importante que o mecanismo de comprovação da propriedade não seja facilmente removido ou criado, dificultando alterações no trabalho (Cox, 2008).

2.3.3. Autenticação e Integridade do Conteúdo

A presença de *watermark* em textos, imagens ou arquivos de áudio pode ser utilizada para verificar a autenticidade do conteúdo do arquivo. A *watermark* pode ser criada com base no conteúdo do arquivo, desta forma alterações no conteúdo do arquivo seriam descobertas com base na *watermark* associada (Cox, 2008).

Para Woo (2007), a utilização de *watermarking* para autenticação possui diferença quando comparado à criptografia. Quando utilizado na criptografia o objetivo é verificar a identidade do material e garantir sua originalidade. No contexto de algoritmos de *watermarking* o objetivo é garantir a integridade da mensagem, garantindo que não houve alterações em nenhum momento após a inserção da *watermark*.

O autor cita ainda, duas vantagens da utilização de autenticação através de *watermarks*. Primeiramente, a *watermark* estará na imagem e não poderá ser removida facilmente. Além disso, não é preciso a alocação de recursos adicionais para armazenar informações sobre a marca, uma vez que a própria *watermark* poderá transportar tais informações.

Conforme citado por Katariya (2012) acerca das características presentes em *watermarks*, uma *watermark* frágil poderia ser aplicada à função de integridade, uma vez que pequenas manipulações sobre os mecanismos comprometeriam a marcação, desta forma agindo como um sinalizador de possíveis mudanças no documento original.

No trabalho apresentado por Song (2012) é utilizado um algoritmo de *watermarking* para verificar a integridade de imagens médicas, a fim de identificar adulterações e os locais na imagem em que foram inseridas.

2.3.4. Controle de Cópias

O controle de cópia é uma maneira preventiva de evitar violações de direitos autorais. Uma das formas de controle proposta por Cox (2008) é a criptografia. Apenas um usuário com a chave certa pode acessar a informação oculta presente no material disponibilizado. Entretanto, o custo de gerenciamento de chaves pode ser um problema para a distribuição do material. Uma proposta paralela é a adoção de *watermarks* juntamente com os métodos usados para sua detecção nos documentos digitais. Esse método permiti identificar se uma cópia foi legalmente produzida ou se é uma cópia não autorizada. No entanto, Woo (2007) propõe que a *watermarking* seja robusta a ponto de ser de difícil remoção ou caso seja removida torne o material inutilizável.

O autor propõe, ainda, um esquema de associação entre criptografia e *watermarking,* desta forma o conteúdo oculto que será inserido deverá ser criptografado e introduzido no material.

2.3.5. Fingerprinting

Tao (2014) denomina *fingerprinting* a utilização de *watermarking*, a fim de criar uma *watermark* única para cada destinatário. Então, a cópia que cada destinatário receber conterá uma *watermark* associado a ele. Esse tipo de algoritmo deve ser robusto contra ataques que objetivem alterar essa identificação de destinatário contida nas cópias.

Para Kashyap (2014) a adoção de *fingerprintings* em cópias permite identificar casos de violação de licenças de utilização e distribuição de conteúdo. Além de auxiliar a identificação dos responsáveis por tais violações.

2.4. PROPRIEDADES DA WATERMARKS

Segundo Cox (2008), um dos parâmetros de mensuração do desempenho de um *watermarking* é a quantidade de propriedades presentes no método. Uma *watermark* em uma cédula de dinheiro tem a propriedade de robustez pelo fato da sua dificuldade de ser removida, mas não possui a propriedade da imperceptividade. Ao passo que a *watermark* em uma imagem que utiliza um algoritmo semelhante ao LSB (*Least Significant Bit*) se torna imperceptível, entretanto não apresenta a propriedade de robustez por ser facilmente corrompida com a modificação da imagem.

É possível encontrar diferentes propriedades em *watermarks*, entretanto a importância de cada propriedade é associada à aplicação do mecanismo ao caso concreto. Diferentes aplicações possuem diferentes propósitos (Katariya, 2012). É possível dividir as propriedades presentes em duas categorias: propriedades associadas ao processo de inserção da *watermark* e propriedades associadas com o processo de detecção. A primeira categoria contempla atributos como eficácia, fidelidade e carga útil de dados. Enquanto a segunda, contempla ocultação da informação e robustez. Além disso, ainda é possível adicionar propriedade de segurança utilizando chaves secretas no processo de *watermarking*.

2.4.1. Eficácia

A propriedade é definida como a capacidade de detectar a *watermark* no trabalho final produzido, após este trabalho ser submetido à inserção deste elemento. Neste caso, o procedimento de *watermarking* precisa ser capaz de embutir a mensagem oculta no material (Cox, 2008). Portanto, um algoritmo que insere uma *watermark* em um objeto, e este algoritmo não consegue recuperar a mensagem oculta sobre este objeto, o qual não sofreu nenhuma alteração após a execução do algoritmo de inserção, é classificado como ineficaz.

2.4.2. Fidelidade

Esta propriedade realiza a comparação do grau de similaridade entre um objeto antes e após a inclusão de uma *watermark*. Quanto menor a quantidade de divergências, mais fidedigna é a *watermark*. Em alguns tipos de arquivos por apresentarem baixa qualidade, como imagens e sons, a inserção de *watermarks* produz um resultado de baixa percepção, diferente de arquivos

de alta resolução que podem sofrer distorções no arquivo final após a inserção de uma *watermark* (Cox, 2008).

Um sinônimo para essa propriedade seria imperceptibilidade, conforme definido por Woo (2007), que também se refere à propriedade denominada transparência perceptual. Essa propriedade explora, principalmente, características da visão humana. Como os olhos têm menor sensibilidade a variações de cores em regiões com maior quantidade de tons quando comparado a regiões com apenas um tom, as *watermarks* devem ser inseridas em regiões de grande variação de tons. Quando é utilizado o termo perceptível, este é aplicado principalmente em relação aos sentidos da visão e audição humana (Katariya, 2012).

Apesar de ser um mecanismo de segurança, a utilização de *watermarks* em arquivos produz ruído no arquivo final, mesmo que pouco perceptível. A degradação presente no arquivo é um indicativo da qualidade do processo de *watermarking* utilizado. Uma métrica utilizada para realizar comparação e mensuração da propriedade de imperceptibilidade (Woo, 2007) é o PSNR (*Peak-Signal-to-Noise-Ratio*). O PSNR procura quantificar a similaridade entre dois arquivos, podendo ser vídeos ou imagens, entretanto a métrica também utiliza o MSE (*Mean Square Error*), o qual quantifica o grau de divergência entre os arquivos, segundo descreve Almohammad (2010). As medidas de PSNR e o MSE são obtidas por meio da aplicação das Equações 1 e 2.

$$\text{PSNR} = 10.\log_{10}\frac{I^2}{MSE}\ db, \text{ e} \tag{1}$$

$$\text{MSE} = \left(\frac{1}{MN}\right)\sum_{i=1}^{M}\sum_{j=1}^{N}\left(X_{ij} - \bar{X}_{ij}\right)^2, \text{ onde} \tag{2}$$

I é o valor máximo que um pixel pode assumir a depender da quantidade *n* de bits utilizado para sua representação, por exemplo, em uma imagem em escala de cinza de *8* bits o valor assumido por *I* é dado por $I = 2^n-1$, portanto *255*. Os valores *M* e *N* representam, respectivamente, o número de linhas e colunas da matriz de pixels da imagem analisada. O parâmetro *Xij* representa os valores dos pixels na posição *ij* da imagem original e da imagem alterada. A qualidade da imagem cresce inversamente ao valor de MSE.

Os métodos objetivos de avaliação de qualidade de imagens, como o PSNR, são mais rápidos e de custo efetivo melhor que os métodos subjetivos. Entretanto, imagens com o mesmo

PSNR podem ter avaliações diferentes de qualidade, quando submetidos ao julgamento humano. Os métodos subjetivos apresentam melhor confiabilidade por serem executados pelos destinatários finais (Almohammad, 2010). Outro aspecto dos métodos objetivos é a falta de padronização dos resultados obtidos. Para Almohammad (2010), a quantificação do resultado é de difícil qualificação dentro de um índice de avaliação.

Uma terceira métrica objetiva é o SSIM (*Structural Similarity*), que se baseia em algumas informações da percepção humana, e tem como proposta tentar mensurar as mudanças destas informações entre duas imagens. Essa métrica baseia-se em propriedades como a iluminação, contraste e estruturação da imagem para produzir coeficientes de similaridade entre as imagens comparadas. O método busca um grau maior de proximidade com a percepção humana, diferente dos métodos PSNR e MSE (Wang, 2009).

Para Wang (2009), a iluminação é tratada como a dificuldade de visibilidade em regiões das imagens. O contraste torna mais nítido as formas e contornos presentes. Enquanto a estruturação é a ideia que os pixels possuem uma relação de interdependência quando próximos, assim carregando informações sobre os objetos da cena. A medida do SSIM é obtida aplicando-se a Equação 3:

$$\mathrm{SSIM(x,y)} = \frac{(2\mu_{x\mu_y} + c_1)(2\sigma_{xy} + c_2)}{(\mu_x^2 + \mu_y^2 + c_1)(\sigma_x^2 + \sigma_y^2 + c_2)} \quad (3)$$

Na equação de SSIM *x* e *y* são as imagens de referência com as mesmas dimensões. As variáveis μ, σ e σ_{xy} são, respectivamente, média, variância e covariância das imagens. Os termos *c1* e *c2* são constantes positivas utilizadas para estabilizar a equação. Os valores produzidos pela equação 3 estão compreendidos no intervalo $-1 \leq SSIM(x,y) \leq 1$ (Wang, 2009), sendo que $SSIM(x,y) = 1$, se e somente se, $x = y$.

2.4.3. Carga útil de dados

Carga útil de dados ou *payload* é compreendida como a quantidade de informação transmitida através da *watermark* ou a repetição da informação dentro do arquivo (Woo, 2007), de forma oculta (Katariya, 2012) ou não. A quantidade de informação dependerá do tamanho da *watermark* a ser introduzida no objeto, uma vez que seu tamanho é influenciado por sua finalidade, considerando que este elemento poderá ter diferentes finalidades.

Podemos ser introduzidas mensagens de *N* bits em um arquivo, o que nos permite criar 2^N diferentes *watermarks* possíveis. *Watermark* pequenas podem ser utilizadas para controles de cópias, facilitando o processo de detecção (Cox, 2008), ou pode-se utilizar ainda *watermarks* grandes o suficiente para transmitir uma segunda mensagem dentro do arquivo original. Uma das vantagens de *watermarks* pequenas é a repetição de uma mesma informação dentro do material, assim um pequeno trecho do material é capaz de conter a mensagem oculta completa.

Para Alotaibi (2015), a propriedade (ou atributo) carga útil pode ser expressa através de uma taxa de bits, que define a taxa de capacidade de uma *watermarking* (Alotaibi, 2015). A taxa de capacidade é expressa por meio das equações 4 e 5.

$$Taxa\ de\ Capacidade\ (bits/KB) = \frac{Dados\ da\ watermark\ (bits)}{Dados\ do\ arquivo\ (KB)}, \text{ ou} \qquad (4)$$

$$Taxa\ de\ Capacidade\ (\%) = \frac{Tamanho\ ocultado\ (Bytes)}{Tamanho\ do\ arquivo\ (Bytes)}\ x\ 100 \qquad (5)$$

Portanto, quanto maior a taxa de capacidade de uma *watermark* maior a quantidade de informação inserida em um arquivo.

2.4.4. Robustez

É a capacidade de recuperar a *watermark* mesmo após a realização de operações sobre o objeto, por exemplo, aplicação de filtros, compressão, impressão, digitalização, rotações, dentre outras operações realizadas sobre o arquivo. Uma *watermark* robusta é aquela que ainda permanece no objeto mesmo após ser submetida a diferentes ações, a *watermark* ainda permanece no objeto, sendo passíveis de recuperação e compreensão de seu conteúdo (Cox, 2008).

A robustez deste elemento a esses diferentes processos está ligada ao tipo de arquivo em que a marcação está depositada e ao procedimento que será submetida. *Watermarks* em arquivos de vídeo e áudio se comportam diferente quando submetidos a filtros e algoritmos de compressão. Portanto, encontrar uma *watermark* que seja robusta a qualquer operação é uma tarefa de difícil solução. São aplicadas técnicas sobre as *watermarks* que as tornam robustas a determinados procedimentos de manipulação, mas não a outros (Cox, 2008). Por exemplo, uma *watermark* em imagens é dita robusta contra-ataques de compressão de JPEG, quando ela ainda

é passível de detecção após a compressão, mas não é um indicativo que seja robusta contra uma operação de rotação.

A *watermark* precisa ser robusta a determinadas operações que existem dentro do contexto da aplicação em que está inserida. Em alguns casos a propriedade de robustez pode ser irrelevante para a aplicação da *watermark*. *Watermarking* para proteção de direitos autorais em uma cópia precisam ser robustas a ataques maliciosos de remoção de *watermark*, mas para uma aplicação de verificação de integridade do material, uma *watermark* frágil pode ser utilizada (Katariya, 2012). Embora seja desejada uma marcação que seja robusta a qualquer tipo de operação, em aplicações reais ela precisa ser robusta a apenas um subconjunto de operações (Woo, 2007).

Existem três classificações possíveis em relação a esta propriedade: robusta, frágil ou semi-frágil (Woo, 2007). O rótulo de robusta se deve a capacidade de suportar ações comuns que podem ocorrer no processamento do arquivo. No outro extremo estão as *watermarks* frágeis, as quais são facilmente destruídas ou removidas. Entre os dois extremos estão as semi-frágeis que possuem características das anteriores, sendo robustas a determinados tipos de operações, no entanto é frágil a outros. Para Cox (2008), a presença da propriedade de robustez torna impossível desassociar a *watermark* do objeto sem comprometer a utilidade deste, portanto a extração indevida da mensagem comprometeria a legibilidade da informação.

2.4.5. Segurança

É descrita como a capacidade de resistir a diferentes tipos de ataques e manter seu conteúdo protegido contra adulteração. Três categorias de ataques podem ser enumeradas. A violação da *watermark* por um desses ataques comprometeria a propriedade de segurança do mecanismo (Cox, 2008):

- Remoção não autorizada
- Inserção não autorizada
- Detecção não autorizada

As duas primeiras categorias são classificadas como ataques ativos, devido ao fato de modificarem o conteúdo dos arquivos em que as *watermarks* estão inseridas. Como o ataque de detecção não autorizada não realiza alterações, ele é chamado de ataque passivo.

O objetivo do ataque de remoção não autorizada é tornar a *watermark* indetectável. Desta maneira o ataque pode apresentar dois resultados diferentes: eliminação ou mascaramento. No primeiro resultado a marcação é removida do arquivo, tornando-a não detectável por uma ferramenta. O arquivo final não será necessariamente igual ao arquivo original sem *watermark*, mas apresenta grau de semelhança elevado com o arquivo original (Cox, 2008).

O segundo resultado, o mascaramento, não há a remoção da *watermark* do arquivo, apenas é aumentada a dificuldade de realizar sua detecção por ferramentas. Um exemplo conhecido dessa técnica é aplica em *watermarks* em imagens, nas quais a rotação da *watermark* dificulta o reconhecimento do mecanismo, apesar da marcação ainda estar presente no material.

O ataque de inserção não autorizada consiste na introdução de uma *watermark* ilegítima. A detecção não autorizada pode ser decomposta em três níveis de segurança. Primeiramente, e o nível mais grave de ataque, é a detecção e decifração de uma mensagem. A segunda detecção seria conseguir distinguir *watermarks*, mas não conseguir decifrá-las. E por fim, o nível menos grave de ataque é a capacidade de reconhecer a existência de uma marcação, mas não ser capaz de distingui-las ou decifrá-las.

Os ataques passivos são mais frequentes em aplicações que utilizam esteganografia, enquanto ataques ativos são mais frequentes em *watermarking* (Cox, 2008).

Um outro mecanismo de segurança é o de utilização de chaves criptográficas aplicadas como forma de proteção da *watermark* contra-ataques de remoção ou modificação. Sua aplicação se baseia no princípio de Kerckhoffs, o qual se baseia na obscuridade da chave em vez do algoritmo de *watermarking*. Portanto, o algoritmo pode ser conhecido por todos, desde que a chave continue em segredo (Woo, 2007).

2.5. AVALIAÇÃO DE UM SISTEMA DE *WATERMARKING*

A avaliação de um método de *watermarking* deve considerar as aplicações que farão uso da técnica (Cox, 2008). Por exemplo, uma *watermark* de um arquivo de vídeo pode ser adequada para controle de cópias, entretanto pode não ser robusta contra ataques de rotação. Os parâmetros para avaliação de um sistema de *watermarking* devem considerar o contexto em que o mecanismo está inserido, os tipos de materiais utilizados, critérios de qualidade e as características das *watermarks* utilizadas. Uma *watermark* com *payload* de 20 bits é

considerada inferior a uma *watermark* com *payload* de 30 bits, desde que não afete outras propriedades, quando o objetivo é transportar informação.

Após definir o contexto de aplicação da *watermarking* e o tipo de documento material a ser utilizado, é preciso definir propriedades relevantes que um sistema de *watermarking* precisa possuir, desta forma é possível criar um *benchmarking* com testes desenvolvidos para mensurar as propriedades da *watermark*. Os testes devem ser executados utilizando os mesmos parâmetros tanto para inclusão como para detecção (Cox, 2008).

Cox (2008) cita diferentes critérios que podem mensurar a qualidade de uma *watermark*. Entre os mais conhecidos estão: quantidade de ruído produzido após a introdução da mensagem; quantidade de informação transportada pela mensagem ocultada, também conhecida como payload; nível de robustez apresentada pela *watermarking*; sua imperceptibilidade; entre outros critérios dependendo da aplicação do algoritmo.

Segundo Woo (2007), outro aspecto a ser considerado durante a avaliação, é o *trade-off* entre as propriedades presentes em algoritmos de *watermarking*. Os algoritmos de *watermarking* podem explorar a redundância para introduzir informação. Entretanto, a repetição pode diminuir a imperceptibilidade, o que pode tornar a *watermark* vulnerável. Entretanto, a redundância pode aumentar a robustez e a eficácia.

Algumas propriedades descritas anteriormente podem ser conflitantes. Por exemplo, com o aumento da robustez a propriedade de imperceptibilidade pode ser comprometida, assim como uma *watermark* com grande carga útil pode afetar a imperceptibilidade e a robustez. O projeto de um algoritmo de *watermarking* deve avaliar as propriedades de acordo com a real aplicação deste mecanismo (Woo, 2007).

2.6. RESILIÊNCIA A ATAQUES

O ataque ao esquema de *watermarking*, normalmente, busca impossibilitar a detecção da *watermark* ou manipular as informações transportada por ela. A propriedade mais relevante ao se avaliar ataques contra *watermarking* é a robustez, a qual pode ser avaliada de acordo com o grau de degradação da informação causado pelo ataque e pela capacidade de detecção de dados recuperados pelo atacante para extrair a *watermark* (Ahmadi, 2014). As principais categorias de ataque são: ataque de remoção; ataque geométrico; ataque criptográfico e ataque de protocolo.

O ataque de remoção tem como objetivo remover completamente a *watermark* ou torná-la irrecuperável. O ataque geométrico é comum em arquivos de vídeo e imagens, os quais podem sofrer operações de rotação, translação, recorte, entre outras. O objetivo não é destruir a marcação, mas comprometer o mecanismo que possibilite sua detecção, impossibilitando sua recuperação. O ataque criptográfico procurar substituir a *watermark* original por uma falsa, introduzindo informações ilegítimas. Por fim, o ataque de protocolo procurar introduzir uma nova *watermark* sobre a original, de modo que se torna impossível distinguir qual *watermark* foi a primeira a ser introduzida no arquivo (Ahmadi, 2014).

3. *WATERMARK* APLICADA A DOCUMENTOS TEXTUAIS ELETRÔNICOS

O processo de introduzir uma *watermark* digital dentro de um documento textual contendo informações que possam identificar o proprietário do documento ou seu criador é conhecido como *Digital Text Watermark* (JALIL, 2009). Desta forma, a aplicação desta técnica pode dificultar a distribuição e reprodução ilegal de informação.

Em arquivos multimídia como áudio, vídeo e imagem são possíveis explorar limitações humanas ou redundância de informações para introduzir mensagens ocultas que não destruam ou impossibilitem a utilização do conteúdo original do arquivo. Portanto, a utilização de *watermarking* em documentos textuais pode explorar esses aspectos para permitir a ocultação da informação. Padrões de linhas e palavras, marcações no plano de fundo, estruturas e regras linguísticas são algumas das características presentes em textos que podem ser utilizadas em algoritmos de *watermarking* (JALIL, 2009). Os algoritmos podem depender do tamanho do texto, da língua predominante no documento, das regras gramaticais e dos estilos de escrita e de formatação.

Alguns trabalhos correlatos, como Varna (2009), Kim (2007) e Shirali-Shahreza (2006), utilizam aspectos estruturais do texto ou dos caracteres para criarem as *watermarks*. Diferentes abordagens para criação de *watermark* relacionados às características do texto foram analisadas durante a pesquisa, e algumas características do método proposto neste trabalho foram baseadas em alguns comportamentos desses trabalhos correlatos.

A literatura classifica as *watermarkings* em documentos textuais em três categorias: Baseadas em imagem; Abordagem Sintática; e Abordagem Semântica. Tais conceitos serão melhores explicados nas próximas subseções.

3.1. TÉCNICAS BASEADAS EM IMAGEM

Brassil (1995) descreve *watermarkings* baseadas em imagens como as técnicas que consideram o texto como uma imagem, fazendo uso das estruturas presentes (linhas, palavras, margens, entre outros) para construção da *watermark*. Algumas das técnicas mais comuns de *watermarking* baseadas em imagens utilizam movimentação de linhas e palavras para embutir a mensagem sob o texto. As técnicas comumente encontradas na literatura são: *Line-Shift*

Coding; *Word Shift Coding*; e *Character Coding* (Brassil, 1995). O autor chama a atenção ao fato de que a percepção humana não é capaz de reconhecer facilmente variações de espaçamento no texto em uma linha, se a movimentação for menor que 1/150 polegadas (0,0169 cm).

O algoritmo *Line-Shift Coding* (Figura 3.1) realiza a movimentação de linhas no sentido vertical, a depender do sinal binário da *watermark* que se deseja inserir. Caso o próximo sinal do *watermark* seja "0" então a linha não é alterada, entretanto se o sinal for "1" a linha será deslocada conforme a lógica do algoritmo implementada. A inserção da marcação é realizada apenas com base na *watermark* e no deslocamento das linhas, entretanto, a detecção precisa realizar a comparação entre as linhas adjacentes para avaliar se houve variação. Como no texto original as variações entre linhas são constantes, esse comportamento não é verdadeiro para um texto modificado, o que dificulta a comparação entre linhas. Por isso, a técnica necessita do documento original para realizar a detecção da *watermark* no texto modificado, com a finalidade de calcular as variações de distância entre linhas (Popa, 1998).

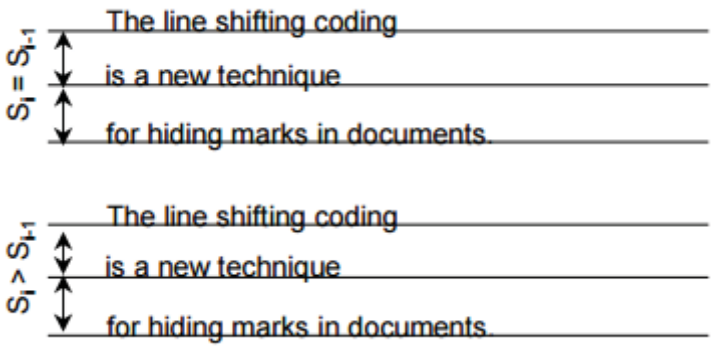


Figura 3.1 - Exemplo da técnica de *Line-Shift Coding* (Popa, 1998).

A técnica *Word Shift Coding* se comporta de forma semelhante ao algoritmo anterior, entretanto o deslocamento realizado será sobre as palavras de uma linha, além de ser um deslocamento no sentido horizontal. A técnica, primeiramente, verifica a existência de uma quantidade suficiente de palavras na linha, caso contrário esta linha será ignorada durante a execução da técnica, conforme ilustrado pela Figura 3.1 **- Exemplo da técnica de *Line-Shift Coding* (Popa, 1998).** que ilustra a diferença de espaçamento entre a linha inferior e superior. Existem variações na escolha das palavras que sofreram o deslocamento. Comumente são selecionadas as palavras nas posições pares da linha com a ressalva de permanecer inalteradas a primeira e a última palavra das linhas, afim de que seja mantido um parágrafo com

alinhamento justificado. Como existem variações naturais de espaçamento entre diferentes caracteres, a técnica precisa utilizar o documento original ou conhecer os detalhes sobre os espaçamentos entre palavras para conseguir recuperar a *watermark* inserida. Na Figura 3.2 é realizada a comparação de um texto original com sua versão modificada através dos deslocamentos (Popa, 1998).

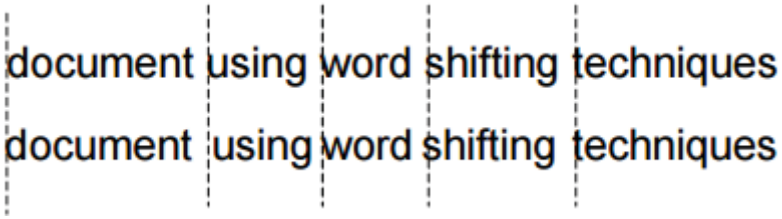


Figura 3.2 - Exemplo da técnica de *Word-Shift Coding* (Popa, 1998).

A técnica proposta no trabalho de Chen (2011) tem como objetivos a proteção dos direitos autorais de uma cópia do documento e a possibilidade de ser utilizada como ferramenta de autenticação. O autor relata que o método é robusto contra manipulações de formatação, por exemplo: alteração na fonte do texto (tipo, tamanho e cor) e alterações de conteúdo (substituição, remoção e acréscimo de palavras no texto). Além disso, o autor descreve um método que pode ser empregado na identificação de adulterações e possui alta capacidade de embutir informações de forma oculta.

O princípio da técnica é esconder a *watermark* por meio de variações de espaçamento entre os caracteres. A ocultação ocorre em um arquivo do tipo .DOC do software Microsoft Office Word[1]. Assim, uma mensagem escolhida é convertida para código binário, que posteriormente é submetido a uma função criptográfica e ao código de verificação de erro *Hamming*[2]. O texto é digitalizado e cada linha e dividida em grupos de caracteres. O texto é percorrido linha por linha e de acordo com o valor do bit da *watermark* o caractere sofre um deslocamento. O procedimento é repetido até o término do texto (Figura 3.3).

O algoritmo utiliza os princípios do *Character-shift Coding*, o qual realiza deslocamentos de caracteres horizontalmente de acordo com a *watermark*. Os deslocamentos devem respeitar as margens do documento e cada deslocamento deve ser menor que 1/150 polegadas. Em adição à imperceptibilidade proporcionada pelo *Character-shift Coding*, o

[1] Software para produção de texto desenvolvido pela empresa Microsoft. Atualmente utiliza arquivos com extensão .docx como padrão.
[2] Codificação utilizada no processamento de sinais capaz de detectar erros de bits durante sua transmissão.

algoritmo utiliza criptografia para manter a mensagem em segredo e o código de Hamming (7,4) para recuperação de um bit errado.

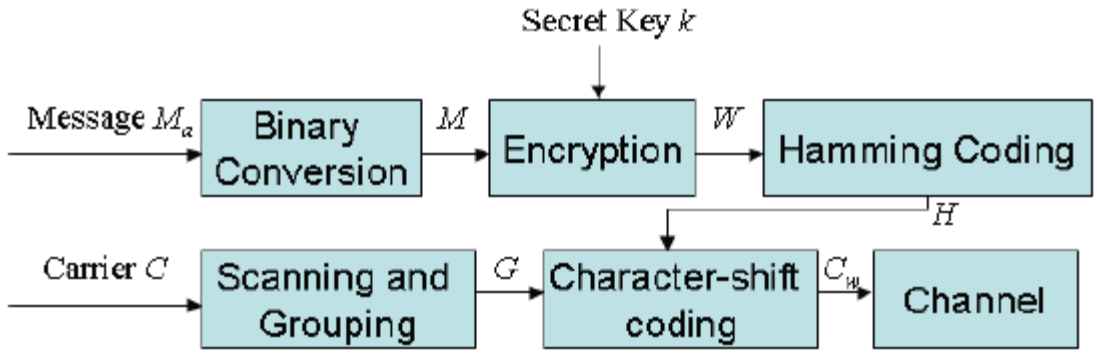


Figura 3.3 - Diagrama de inclusão de ***watermark*** com *Character-shift coding*, após criptografia e *Hamming Coding* (Chen, 2011).

A extração é a reversão do processo de inclusão, podendo fazer uso, ou não, do documento original. Chen (2011) relata que a técnica é robusta contra ataques de formatação de texto, como por exemplo, alterações de cores, tamanho e fontes. Além disso, é possível recuperar a *watermark* após alterações de conteúdo do texto. Entretanto, não foi avaliada a eficácia da técnica em texto impressos, e também é preciso conhecer valores de espaçamento para diferentes situações de variações de formatação de texto ou possuir o documento original para fins de comparação, assim como nas técnicas *Line-Shift Coding* e *Word Shift Coding*.

Em experimentos realizados por Chen (2011) a utilização de texto nas línguas chinesa e inglesa apresenta capacidade de armazenar informações diferentes. A técnica foi desenvolvida para documentos digitais, portanto as alterações de formatação e alteração de conteúdo nestes documentos podem ser detectadas pela técnica.

Assim como no método *Line-Shift Coding* e *Word-Shift Coding*, a técnica proposta por Huang (2001) também faz uso de deslocamentos no texto. Entretanto, a técnica do autor utiliza deslocamento entre palavras, e realiza uma análise estatística dos espaçamentos criados, a fim de identificar as marcações criadas.

O método não utiliza o documento original, nem faz uso de linhas ou blocos de controle para decodificação da *watermark* como os métodos em que é baseado. O autor atribui o nome

de *Space Coding* a sua técnica devido à codificação das *watermarks* através dos espaçamentos entre palavras.

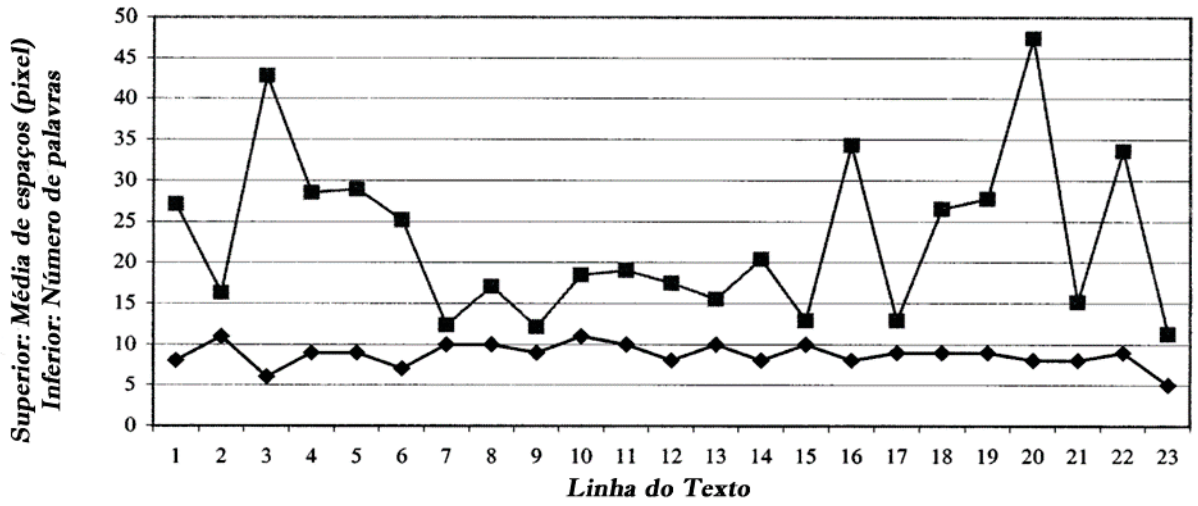


Figura 3.4 - Média do número de espaços entre palavras a cada linha do texto (Huang, 2001).

O trabalho proposto por Brassil (1995) é conhecido como *Character Coding*, o qual utiliza características presentes no texto, como as dimensões de uma letra ou a posição do caractere em relação aos demais. A Figura 3.5 apresenta um exemplo de análise realizada pelo método *Character Coding*. Utilizando essas características é possível ocultar uma mensagem realizando alterações nessas dimensões de acordo com as informações a serem embutidas. Durante a escolha do caractere que será alterado é necessário cuidado com a letra escolhida, a fim de evitar que o leitor possa realizar uma comparação e descobrir a alteração, como o caso de duas letras adjacentes (Brassil, 1999). Na língua portuguesa essa construção é conhecida como dígrafo. A técnica proposta neste trabalho é baseada em características presentes em fontes textuais e na similaridade entre diferentes fontes presentes em editores de texto. Desta forma, introduzindo *watermarks* através de variações de fontes textuais.

Figura 3.5 - Exemplo da técnica de *Character Coding* (Brassil, 1999). A letra "r" da palavra "Internet" foi deslocada para baixo em relação às demais letras.

O trabalho de Lu (2009) também utiliza documentos .DOC para implementar sua técnica. Seus experimentos são feitos utilizando variações de espaçamento e tamanhos de caracteres. O método *Inter-Character Space Coding* é utilizado para variações de espaçamento entre caracteres de acordo com o bit da *watermark* e *Font Coding* para as variações dos tamanhos dos caracteres. Quando o bit da *watermark* for '1' o caractere é modificado, caso contrário não há alterações. Através da mensuração da distribuição de *pixels* no texto após as alterações, a técnica de espaçamento entre caracteres introduz mais ruído no documento, o que aumenta a proteção contra-ataques de OCR[3] (Figura 3.6).

São utilizadas propriedades de caracteres presentes em documentos do formato .DOC, como a propriedade *Font.Spacing*. Os algoritmos de inserção e extração fazem uso dessa propriedade para executar a técnica.

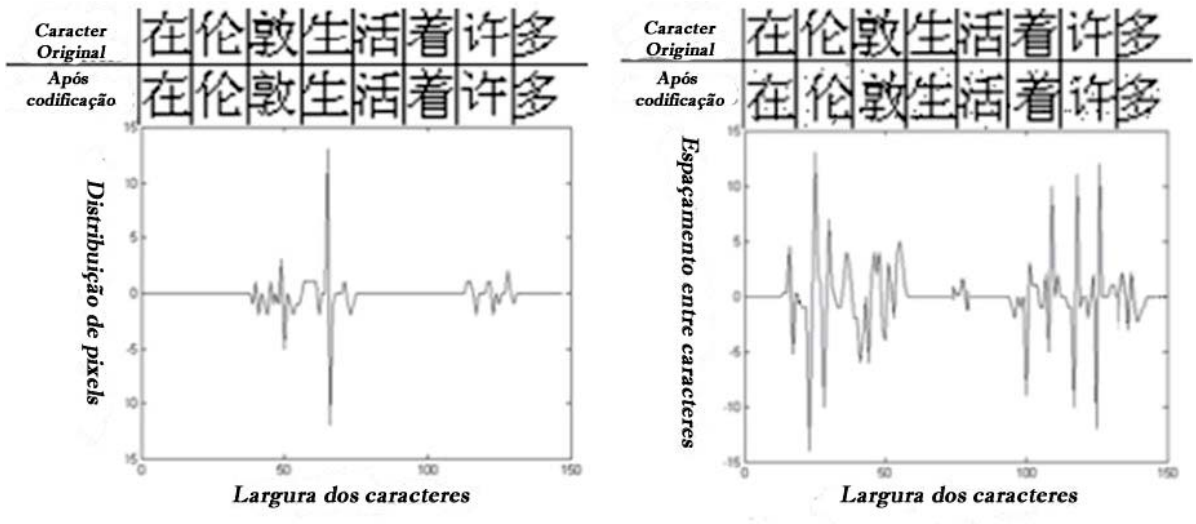


Figura 3.6 - Gráficos de ruídos introduzidos no texto após alterações de espaçamento e tamanho da fonte. À esquerda é ilustrada a técnica *Font Coding* e à direita *Inter-Character Space Coding* (Lu, 2009).

O método proposto por Varna (2009) procura recuperar *watermarks* em documentos impressos ou digitalizados. Portanto, a *watermark* é inserida antes de tais processos e recuperada através do método. A ideia da técnica é realizar pequenas modificações em caracteres do texto, e através de detectores de correlação e um código de correção de erro seria possível identificar esses caracteres. Além disso, com o uso de um algoritmo de OCR a

[3] Significa Reconhecimento Óptico de Caracteres (Optical Character Recognition) que permite o recolhecimento de caracteres a partir de uma imagem de texto.

watermark seria identificada mesmo após múltiplos ciclos de cópias. A técnica seria pouco perceptível para um leitor leigo, conforme ilustrado pela Figura 3.7 **- Exemplos de caracteres modificados pela manipulação de *pixels* que compõem os caracteres (Varna, 2009).** que apresenta caracteres que sofrem introdução de ruídos em suas formas.

O algoritmo insere pequenas alterações em *pixels* dos caracteres, entretanto em alguns caracteres essas alterações sofrem degradações durante o processo de cópia, o que pode comprometer a robustez do algoritmo. Para corrigir o problema é utilizado um código de correção de erro.

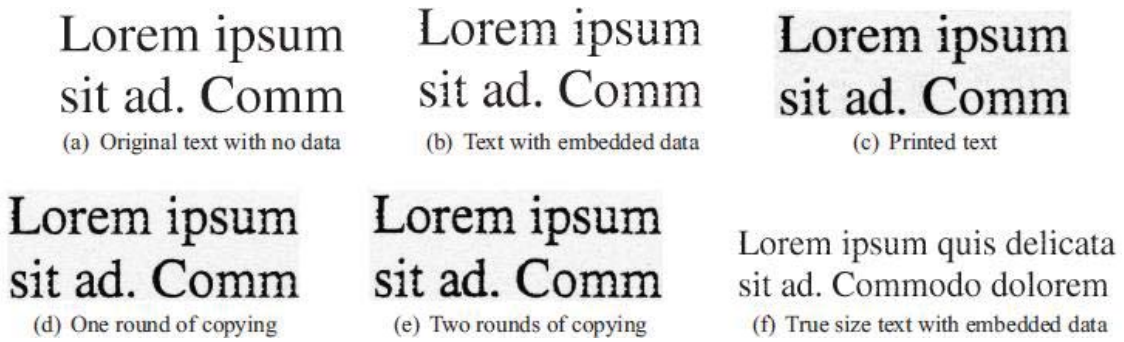


Figura 3.7 - Exemplos de caracteres modificados pela manipulação de *pixels* que compõem os caracteres (Varna, 2009).

Uma abordagem diferente, mas também relacionado às técnicas baseadas em imagens, é o trabalho proposto por Kim (2007) relacionado com *watermarks* em documentos impressos. O autor introduz pequenos pontos imperceptíveis ao longo do texto para embutir a mensagem oculta. Para recuperar a mensagem são implementadas autocorrelações e pontos adicionais para corrigir distorções geométricas. Entretanto, diferente do primeiro método que suporta múltiplos processos de cópia (Varna, 2009), a técnica descrita por Kim (2007) não apresenta a mesma robustez. O método foi desenvolvido para documentos bicolores, sendo robusta a processos únicos de impressão e digitalização. Com a introdução de algoritmos de *Hash* e criptografia pode ser utilizada como autenticação.

A técnica é nomeada de DHDD ou Ocultação de Dados em Documentos Baseado em Pontos (*Data Hiding for Documents based on Dots*), a qual impressoras a laser ou jato de tinta são capazes de imprimir pequenos pontos em documentos que são imperceptíveis para um leitor. Através da disposição desses pontos, que podem ser pseudoaleatórios, é inserida a

mensagem oculta. A implementação desta ténica é capaz de inserir 1370 bits de informação em uma página de tamanho A4 e impressão de 600 dpi.

Neste caso, para recuperação da mensagem o texto é digitalizado, e caso não haja distorções geométricas (rotações, translações, alterações de escala, etc.) a recuperação seria trivial. Entretanto, estas distorções são comuns em processos de impressão e digitalização. Para tratar o problema, os autores dividiram o documento em quatro quadrantes, e em cada quadrante existe uma *watermark*. Entretanto, o método continua frágil a distorções provocadas por processos de translações e rotações da imagem. Para compensar essas distorções, foram inseridos pontos adicionais chamados de pontos de registro, conforme pode ser observado na Figura 3.8 **- Sequência de pontos inseridos antes da impressão ou digitalização do documento (Kim, 2007).**.

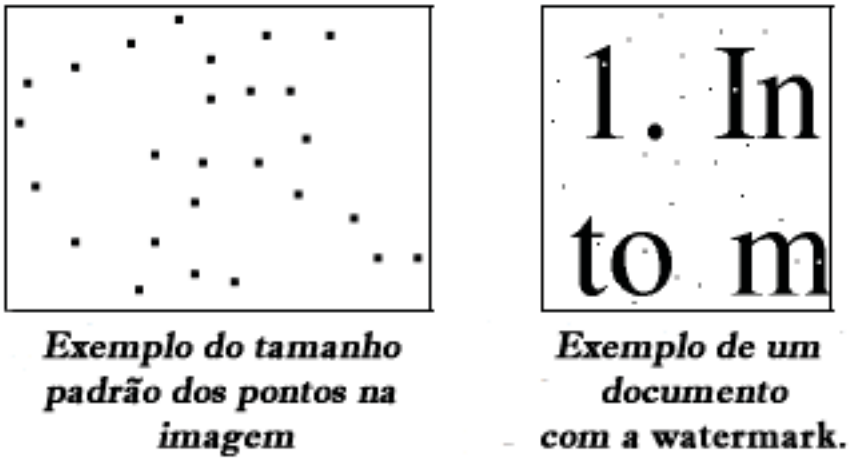


Figura 3.8 - Sequência de pontos inseridos antes da impressão ou digitalização do documento (Kim, 2007).

Todas as técnicas apresentadas nesta seção são baseadas em imagens de documentos nos quais são inseridas *watermarks* binárias. Porém, é importante destacar que os arquivos devem ser tratados quanto ao seu conteúdo textual e não apenas como um conjunto de imagens. Estes algoritmos não são robustos a ataques de *re-typing*, uma vez que ao serem novamente digitados, a *watermark* inserida nos textos é perdida, e quando submetidos a mecanismos de OCR (*Optical Character Recognition*) mudanças de deslocamentos de linhas são ignorados durante o processamento do documento (JALIL, 2009).

Um resumo comparativo das três técnicas descritas anteriormente é apresentado por Brassil (1999). Na visão do autor, a técnica *Line-Shift Coding* é a melhor opção quando aplicada

sobre texto impressos por apresentar maior resistência às degradações introduzidas no processo de foto cópia. O *Word Shift Coding* é menos perceptível ao leitor, entretanto também é menos robusto a presença de ruídos no documento. O *Character Coding* aumenta a densidade de codificação, permitindo a inserção de mais alterações que os dois métodos anteriores. Essa propriedade permite introduzir informações maiores e adicionar redundância à *watermark*.

Segundo Kim (2007), a ocultação de informação em arquivos de imagens pode ser classificada em três classes:

- *Component-wise*: Alteração de características de conjunto de *pixels*, por exemplo: espessura dos traços; posição de caracteres; características de brilho e iluminação. O trabalho de Huang (2001) pode ser classificado nessa categoria.
- *Pixel-wise*: Alteração de valores de *pixels* individualmente, podendo o *pixel* escolhido ser aleatório ou de acordo com o grau de impacto visual causado pela alteração. Os trabalhos de Varna (2009) e Kim (2007) fazem parte desta classificação.
- *Block-wise*: Divide a imagem em blocos, modificando cada bloco para ocultar a informação. Alguns autores sugerem realizar modificações nestes blocos de acordo com a quantidade de *pixels* pretos existentes na região.

3.2. ABORDAGEM SINTÁTICA

Diferente da abordagem Baseada em Imagem, na qual são utilizados aspectos visuais do texto final, a abordagem sintática utiliza a estrutura sintática do texto para introduzir a *watermark*. Como o texto é formado de sentenças, que por sua vez são formadas por palavras (substantivos, verbos, artigos, preposições, entre outros), a organização desses elementos sintáticos no texto é utilizada para criação da *watermark*. Como existe uma relação com as classes de palavras existentes, esta abordagem também será influenciada pelo idioma do texto (Jalil, 2009).

Atallah (2001) propôs um dos primeiros métodos de abordagem sintática utilizando linguagem natural, seu método faz uso de uma árvore sintática baseada no texto, aplicando sobre ela transformações para embutir a *watermark*. A primeira etapa do método é realizar o *parsing* das sentenças do texto (Figura 3.9), separando as classes gramaticais das palavras, posteriormente, são aplicadas transformações para introduzir a *watermark*.

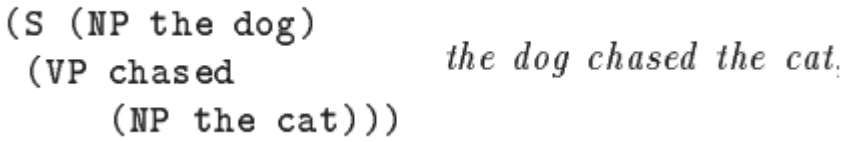


Figura 3.9 - *Parsing* da frase "*the dog chased the cat*" (Atallah, 2001).

Entre os trabalhos correlatos que se enquadram nessa abordagem, estão o algoritmo classificado por Kaur (2013) como abordagem zero *watermarking*, o qual faz uso da frequência das letras em sentenças escolhidas. Para cada sentença é criada um código de letras que será concatenado com outros códigos para criação da *watermark*. No exemplo apresentado na Figura 3.10 foram selecionadas as primeiras letras de substantivos e verbos de sentenças para formar parte do código. Para revelar o identificador é necessário comparar o *watermark* recebido com o *watermark* obtido durante uma nova execução do algoritmo sobre o texto. A técnica auxilia a verificação de possíveis alterações no texto (Kaur, 2013).

Sentences	Pattern
Many *resources* are *available* to help you use your *device*	RAD
You can *look* for *answers* in help *application*	LAA
Features such as an *internal* GPS *receiver*	FIR

Figura 3.10 - Exemplo de texto em que foi aplicado algoritmo *zero watermarking*. O código gerado a partir das três sentenças é RAD.LAA.FIR (Kaur, 2013). A técnica utiliza a primeira letra de cada substantivo encontrado nas sentenças.

O algoritmo zero *watermarking* suporta ataques de reescrita e reordenamento de sentenças, desde que as alterações sejam realizadas em poucas sentenças. Caso ocorra excessivas alterações o algoritmo não é capaz de recuperar a *watermark*.

Uma outra abordagem proposta por Mir (2014) defende a utilização de *watermarking* em páginas da Internet. A *watermark*, após ser criada de acordo com suas regras de formação, será submetida a um processo criptográfico e o resultado convertido em espaços em branco de acordo com o código binário da *watermark*. Através da estrutura do HTML é possível ocultar essa informação utilizando caracteres que não são exibidos nos navegadores. As codificações

ASCII e Unicode possuem conjunto de caracteres que não possuem representação gráfica nos documentos. Esses caracteres são conhecidos como invisíveis ou sem face.

Na metodologia proposta por Mir (2014) uma função Hash realiza o papel de função criptográfica e a *tag* <meta> da linguagem HTML é utilizada para inserir a *watermark*. A geração da *watermark* consiste de quatro etapas: submeter a mensagem a ser inserida a uma função de Hash; converter o resultado da função Hash em valores de 8 dígitos; criar uma sequência de caracteres invisíveis de acordo com a sequência de bits da etapa anterior; e ao final inserir a sequência de caracteres invisíveis na página web.

Com base no processo descrito na Figura 3.11 **- Processo de geração, de acordo com regras de formação, e inserção da *watermark* em páginas web (Mir, 2014).**, a mensagem utilizada no início do processo é obtida a partir de caracteres ou palavras presentes no texto. As frequências desses caracteres ou palavras são concatenadas para a criação da *watermark*. Os caracteres invisíveis utilizados no método são ignorados pelos navegadores, portanto não são removidos durante a exibição de uma página. Para validar as páginas é realiza a extração da *watermark* e comparada com a *watermark* do texto original.

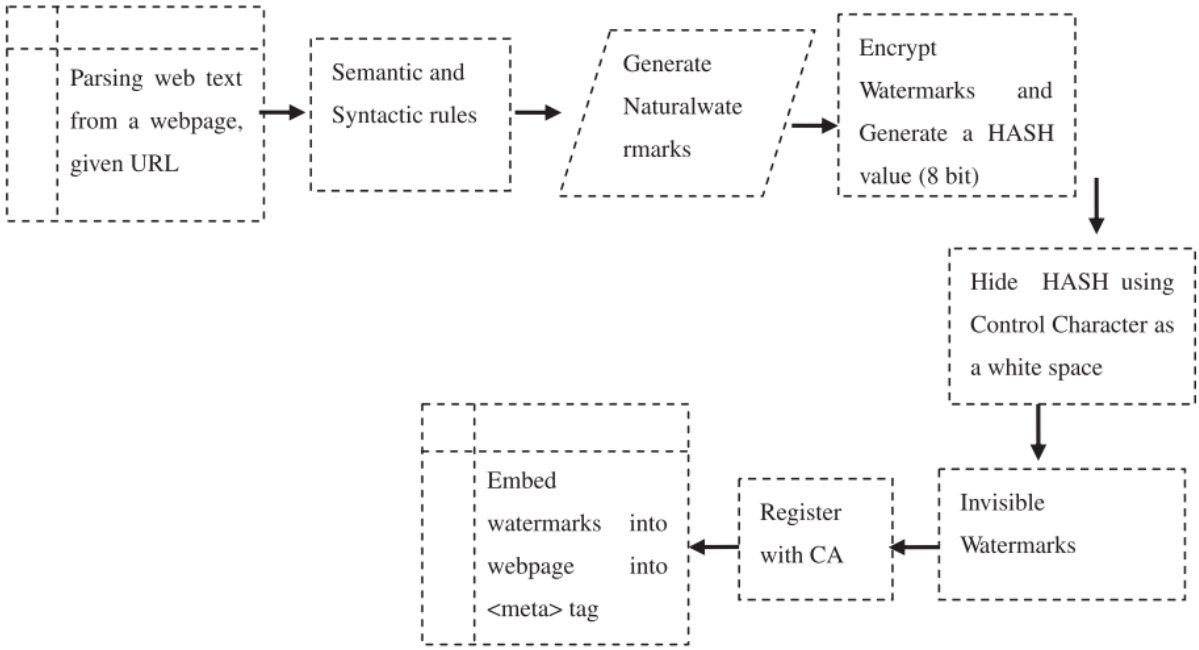


Figura 3.11 - Processo de geração, de acordo com regras de formação, e inserção da *watermark* em páginas web (Mir, 2014).

Por fim, Khan (2015) discorre sobre a utilização de palavras do alfabeto polonês para introduzir mensagens ocultas. Seu trabalho é baseado na técnica proposta por Shirali-Shahreza

(2006) que utiliza letras do alfabeto Arábico que possuem pontos, assim introduzindo mensagens binárias nos textos.

Uma das principais diferenças entre os dois métodos é que o trabalho de Khan (2015) utiliza letras com pontos (‘i’ e ‘j’) para simbolizar o dígito ‘1’, e as demais podendo simbolizar o dígito ‘0’. No trabalho de Shirali-Shahreza (2006) são utilizadas 15 letras com pontos do alfabeto árabe, no qual são realizados deslocamentos dos pontos dos caracteres para introdução de mensagens, como ilustra a Figura 3.12.

Figura 3.12 - À esquerda método proposto por (Shirali-Shahreza, 2006) para deslocamento de pontos em letras do alfabeto Arábico. À direita método proposto por (Khan, 2015) para utilização de letras com ou sem pontos.

O trabalho de Sun (2005) utiliza a relação entre substantivos e verbos presentes nas sentenças para ocultar uma mensagem através dessa relação. As sentenças são submetidas ao *parsing*, gerando uma árvore com os termos presentes Figura 3.13.

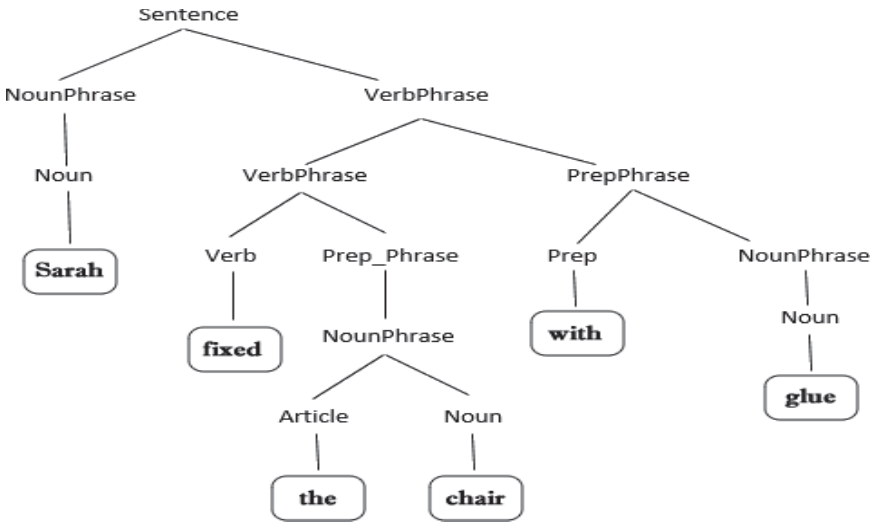


Figura 3.13 - Árvore de *parsing* da sentença “*Sarah fixed the chair with glue*”, em que os substantivos e verbos são utilizados para construir a *watermark* (Sun, 2005).

3.3. ABORDAGEM SEMÂNTICA

O foco da abordagem é utilizar a estrutura semântica do texto para embutir a *watermark*. Assim como a abordagem sintática que realiza a separação das palavras em classes gramaticais, essa metodologia também faz uso de separação e classificação dos léxicos. Entretanto, realiza a substituição de palavras em um texto por sinônimos, conforme propõem Topkara (2006) em seu trabalho.

Um dos desafios dessa solução é o tratamento de palavras homógrafas, em que há escrita igual das palavras e sons diferentes, ou homônimos perfeitos, grafia e pronúncias iguais. A técnica seleciona os sinônimos que tem maior relevância para o contexto e que podem estar associados a outras palavras, como ilustra a Figura 3.14.

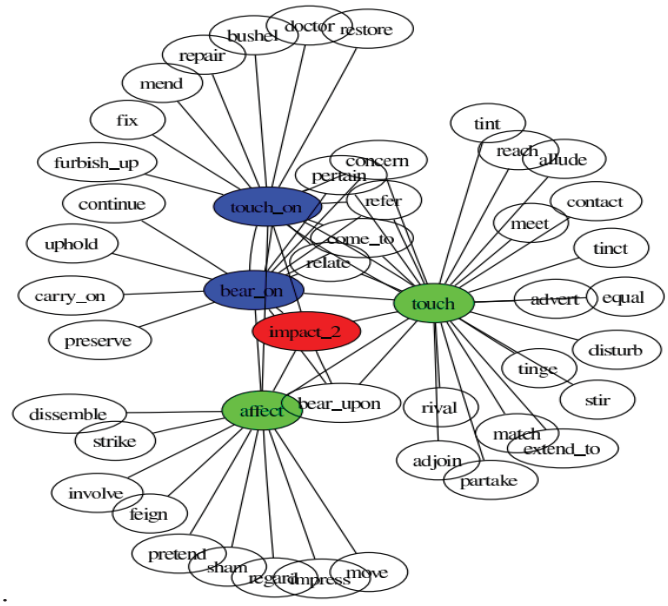


Figura 3.14 - Busca por palavras sinônimas ao termo "*impact*". Os termos coloridos foram selecionados como de maior relevância para o contexto (Topkara, 2006).

4. CRITÉRIOS DE AVALIAÇÃO DE ALGORITMOS DE *WATERMARKING*

Apesar de utilizarem tipos de arquivos e objetivos diferentes, algumas propriedades presentes em uma *watermark* são repetidas em diversos trabalhos, como Cox (2008), Katariya (2012) e Woo (2007).

Entre as propriedades citadas na literatura, Panah (2016) enumera algumas de maior relevância: capacidade de transportar informação ou *payload*; perceptibilidade da *watermark* no material; robustez do algoritmo contra-ataques; segurança contra acesso não autorizado à mensagem oculta; e grau de similaridade entre o material antes e após a inserção da *watermark*, também chamado de fidelidade (Subhedar, 2013).

O método proposto neste trabalho será submetido à avaliação de acordo com as propriedades citadas no parágrafo anterior. Alguns testes serão realizados em materiais que foram submetidos ao método, a fim de aferir seu desempenho em relação a outros métodos da literatura correlata. As seções seguintes descrevem comportamentos esperados do método proposto para cada uma das propriedades.

4.1. CAPACIDADE DE TRANSPORTAR INFORMAÇÃO

Também chamada de *payload* ou carga útil, essa propriedade implica em adicionar dados ao documento original, de modo que os dados estejam sempre presentes no documento, podendo ser extraídos posteriormente. As técnicas citadas apresentam capacidades diferentes de transportar informações.

A quantidade de dados/bits que podem ser ocultados em um arquivo é chamada de *embedding capacity*/*embedding rate* ou taxa de capacidade, conforme apresentado na seção 2.4.3. A eficiência de inserção de dados/bits é defino como a quantidade de bits da mensagem a ser ocultada pela quantidade de bits do documento original modificado. A relação ideal seria uma alta quantidade de bits ocultados provocando poucas modificações (ruídos) no documento original (Subhedar, 2013).

Entretanto, a quantidade crescente de carga útil, apesar de proporcionar um maior volume de informações enviadas, pode comprometer o sigilo da mensagem ou sua perceptibilidade quando inserida no arquivo que irá transportá-la. Relação citada anteriormente

e conhecida como *trade-off*. Sobre outra perspectiva, uma taxa de *embedding capacity* pequena e redundante poderia facilitar a recuperação de *wateramark* em trechos menores do documento.

4.2. ROBUSTEZ

Entre os tipos de ataques que o algoritmo proposto foi submetido estão: ataque geométrico e ataque de modificação intencional ou não (Voloshynovskiy, 2001).

O primeiro tipo de ataque consiste em realizar manipulações com o documento, de modo que comprometa a recuperação da *watermark* inserida. Diferente de ataques de remoção, este ataque tem como objetivo distorcer a informação da *watermark*, tornando-a de difícil recuperação. Entre as manipulações possíveis de documento, Voloshynovskiy (2010) cita as seguintes possibilidades: rotação do texto; corte do texto original; inversão de imagem; entre outros.

Em relação ao ataque de modificação intencional ou não, Voloshynovskiy (2010) descreve que o objetivo é recuperar a *watermark* inserida no documento, mesmo que uma pequena parte seja perdida ou alterada. Portanto, caso ocorra alguma modificação decorrente de ação direta humana e intencional ou modificação decorrente de um processo de conversão, será possível recuperar a *watermark* original e ainda identificar a região que sofreu alteração. Para realizar essa detecção e permitir sua correção, um dos algoritmos utilizados em transmissão de sinais é o Código de *Hamming*, conforme descrito por Chen (2011), o qual possui diversas variações a depender do tamanho da mensagem e números de bits de paridades utilizados no algoritmo.

4.3. FIDELIDADE/PERCEPÇÃO

Os aspectos visuais dos documentos devem ser semelhantes, de modo que o leitor não perceba as alterações causadas pela introdução de *watermark*. São necessários critérios para avaliação do grau de semelhança entre os documentos produzidos. Dois critérios podem ser aplicados para essa avaliação: critérios de fidelidade objetivos e critérios de fidelidade subjetivos (Gonzalez, 2010).

Quando a avalição é feita em termos de funções matemáticas de entrada e saída, são utilizados critérios de fidelidade objetivo. Para exemplificar a utilização de funções matemáticas serão utilizadas algumas métricas, por exemplo: PSNR e RMSE (Subhedar, 2013).

PSNR, conforme descrito na seção 2.4.2 sobre as propriedades de *watermarkings*, é um método comumente utilizado para verificar o percentual de qualidade de imagens utilizadas em conjunto com esteganografia. Também pode ser escrita em termos do RMSE para o caso de imagens com 8 bits.

$$\text{PSNR} = 20 \log_{10} \frac{255}{RMSE} \text{ dB} \tag{6}$$

O método RMSE (Root Mean Square Error) também é uma forma utilizada para quantificar as diferenças entre imagens que sofrem manipulação, e pode ser expressa em termos do MSE, onde N x M é o tamanho da imagem, Cij é a imagem original e Sij é a imagem após ser inserida a mensagem escondida.

$$\text{RMSE} = \sqrt{MSE} = \sqrt{\frac{1}{MN} \sum_{i=1}^{N} \sum_{j=1}^{M} (Cij - Sij)^2} \tag{7}$$

O objetivo da utilização dessas equações é comparar dois sinais, no caso *pixels*, produzindo um resultado quantitativo que descreverá o grau de similaridade ou diferença entre os dois (Wang, 2009).

Segundo Gonzalez (2010), apesar de critérios objetivos oferecerem uma maneira simples, de menor custo e prática de avaliar a perda de informação, as imagens serão analisadas ao final das etapas por seres humanos. Portanto, avaliar de forma subjetiva pode ser mais apropriado. O autor sugere duas formas de quantificar a similaridade através da opinião de um grupo de indivíduos que avaliaram as imagens. Primeiramente, sugere a utilização de escalas de classificação com valores absolutos, que pode ser ilustrada pela Tabela 4.1, na qual a imagem resultante será classificada. Ou pode ser avaliada por meio de comparações entre as duas imagens atribuindo avaliações como: muito pior, pior, ligeiramente pior, igual, ligeiramente melhor, melhor e muito melhor. Neste último cenário é interessante que os resultados estejam próximos da opção “igual”.

Tabela 4.1 - Escala de classificação da *Television Allocations Study Organization* (Gonzalez, 2010).

Valor	Classificação	Descrição
1	Excelente	Uma imagem de qualidade extremamente alta, o melhor que se pode desejar.
2	Boa	Uma imagem de alta qualidade, proporcionando uma experiência visual agradável. A interferência não chega a incomodar.
3	Razoável	Uma imagem de qualidade aceitável. A interferência não chega a incomodar.
4	No limite	Uma imagem de baixa qualidade, você gostaria que ela fosse melhor. A interferência incomoda um pouco.
5	Inferior	Uma imagem muito ruim, mas é possível assistir. A interferência definitivamente incomoda.
6	Inutilizável	Uma imagem tão ruim que você não assistiria.

4.4. SEGURANÇA

Em relação à propriedade de segurança, não podemos restringir a *watermark* apenas quanto ao sigilo da mensagem, mas também deve estar relacionada à possibilidade de detecção de alterações e garantia da autenticidade do documento.

A utilização de criptografia em *watermarking* em textos, além de garantir sigilo da mensagem, pode ser utilizada como mecanismo de detecção de alterações. Criando-se uma chave de criptografia a partir de aspectos sintáticos ou semânticos do texto podemos identificar adulterações no texto original (Cheema, 2014). Portanto, a formação da chave criptográfica utilizando informações provenientes do texto pode ser eficaz para detectar ataques de modificação do texto.

Algoritmos de criptografia simétricos, como AES e OTP, ou de criptografia assimétrica, como RSA ou ElGamal, poderiam ser utilizados durante as etapas de encriptação e decriptação. E propriedades acessórias da utilização de criptografia como integridade, autenticidade e não-repúdio da mensagem também estariam presentes quando utilizado criptografia simétrica ou assimétrica (Stallings, 2005).

5. MÉTODO PROPOSTO

O objetivo do trabalho é realizar um estudo sobre algoritmos de *watermarking* baseados em documentos textuais e propor um algoritmo que se enquadre dentro deste contexto. Analisando as características de diferentes métodos de autores, como Kaur (2013), Chen (2011), Lu (2009), Khan (2015), entre outros, e avaliando aspectos do ambiente no qual o método será utilizado, foram elencadas características que devem estar presentes no algoritmo de *watermarking* proposto, como: robutez, capacidade de transportar informação, imperceptibilidade e segurança.

O procedimento para elaboração do algoritmo atende ao descrito por Mohanty (1999), sendo divido em três partes:

Criação da *Watermark* – elaboração da mensagem que será inserida em um objeto, no caso deste trabalho um documento textual. Nesta etapa estão inclusos aspectos como a utilização de funções criptográficas na mensagem ou criação de mensagens diferentes para destinatários diferentes.

Procedimento de inserção – Após a criação de uma *watermark*, é preciso introduzi-la em um documento. Para isto foi utilizada uma função que recebe como parâmetros a *watermark* e o documento original, mostrado na Equação 8, produzindo ao fim do procedimento um documento marcado, conforme ilustra a Figura 5.1. A equação 8 descreve esta etapa,

$$E(I, S) = I' \tag{8}$$

Onde E é a função de inserção, que recebe os parâmetros I e S, os quais são o documento original e a *watermark* utilizada, respectivamente. Produzindo ao final I', representando o documento final.

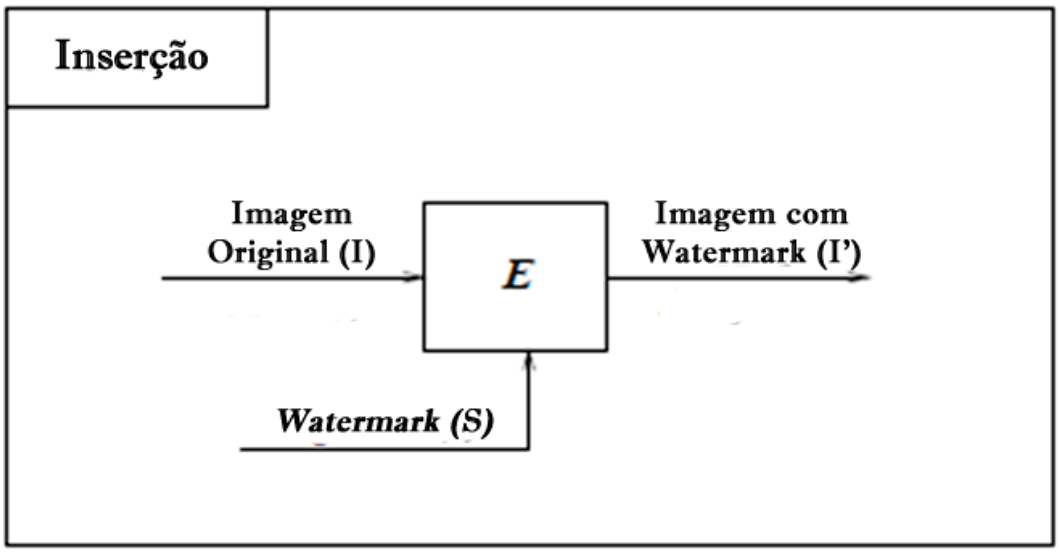


Figura 5.1 - Procedimento de inclusão de *watermarks* em um documento, produzindo um documento marcado (Mohanty, 1999).

Procedimento de Recuperação – Como última etapa do algoritmo de *watermarking*, a *watermark* inserida no documento deve ser passível de recuperação para fins de verificação da legitimidade do documento. Matematicamente, segundo Mohanty (1999), a equação dessa etapa seria descrita como:

$$D(J, I) = S' \tag{9}$$

Onde D representa a função de recuperação da *watermark* e os parâmetros J e I seriam o documento marcado e sua versão original, respectivamente. Desta forma recuperando a *watermark* S'. Para Mohanty (1999), utilizar o documento original no processo de recuperação pode ser uma alternativa do algoritmo, mas não a regra desta etapa. De posse da *watermark* S', ela ainda precisa ser submetida a uma função de comparação para verificar a semelhança com a *watermark* S do processo de inclusão, comprovando que são idênticas, conforme ilustrado na Figura 5.2.

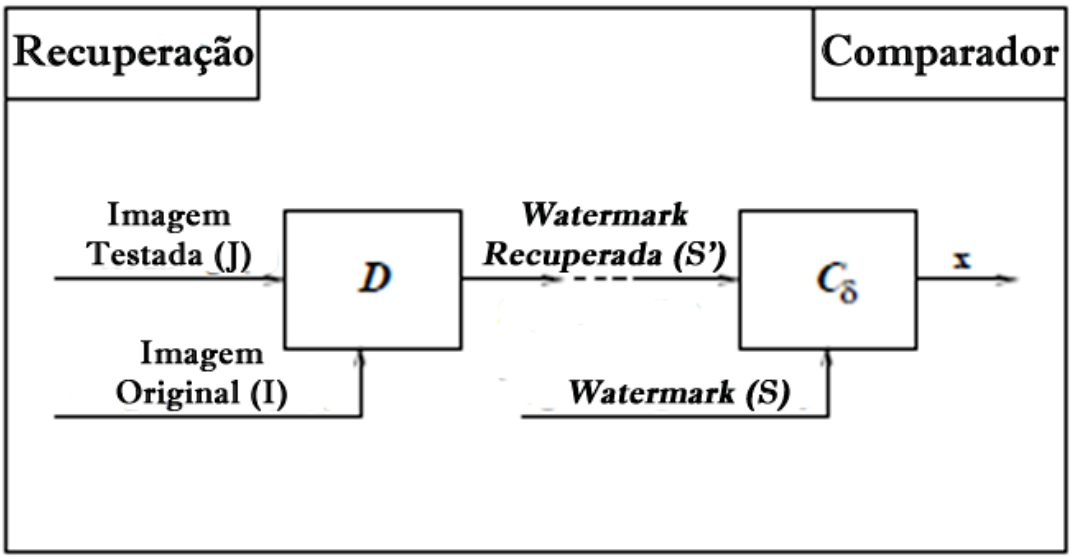


Figura 5.2 - Procedimento de recuperação de watermarks em um documento e a função de comparação das watermarks (Mohanty, 1999).

A função de comparação recebeu como parâmetros a *watermark* S da etapa de inclusão e a *watermark* S' da etapa de recuperação. Caso fossem idênticos os bits comparados retornaria 1, caso contrário 0, conforme a equação a seguir:

$$C_\partial\,(S, S') = \begin{cases} 1, \ para\ todo\ S_i = S'_j, onde\ i\ e\ j > 0 \\ 0, caso\ contrário \end{cases} \quad (10)$$

O método proposto neste trabalho sugere o estabelecimento de etapas prévias à criação da *watermark*, de modo que algumas condições existam para permitir a utilização do algoritmo. O contexto de utilização da técnica são os documentos produzidos para inquéritos policiais e processos judiciais. Portanto, são documentos que podem ser sigilosos e possuem relevância no âmbito dos respectivos procedimentos. Entretanto, tais documentos podem ser acessados por diferentes atores, como advogados, funcionários públicos do órgão e até mesmo por terceirizados. Atores com acesso a tais documentos poderiam realizar cópias ou digitalizações dos documentos, e posteriormente, realizar sua divulgação não autorizada em veículos de comunicação ou utilizá-los para interesses particulares.

A técnica apresentada neste trabalho tem a preocupação de realizar um mapeamento entre as cópias eletrônicas digitais criadas e seus destinatários, além de manter a *watermark* nos documentos impressos, mesmo após fotocópias e digitalizações. Entretanto, algumas condições precisam ser adotadas para garantir essas características.

Primeiramente, no procedimento de geração de cópias digitais propõe-se a introdução da etapa de incorporação da *watermark*, o que engloba sua geração e inserção no documento digital, o que alterará o rito de criação das cópias. Posteriormente, a relação entre a *watermark* criada, a cópia do documento que receberá a marcação e o destinatário da cópia deverão ser registradas, a fim de que seja possível realizar a rastreabilidade de um documento. Logo, para cada cópia de documento é gerado uma *watermark* que também estará associado a seu destinatário, desta maneira criando um algoritmo de *watermarking* com a função de *fingerprinting*. Uma alternativa para realizar esse registro seria a utilização de uma base de dados para armazenamento da rastreabilidade das cópias ou a *watermark* incluída no documento seja por si só identificadora do destinatário.

O que o algoritmo apresentado propõe é realizar a inserção de mensagens ocultas dentro de documentos eletrônicos, de modo que a mensagem permaneça no documento mesmo após sua impressão. A mensagem seria transformada em código binário e sua inserção seria realizada em caracteres pré-definidos do texto. Esses caracteres sofreriam alterações em sua forma de acordo com os valores dos bits da *watermark*. As alterações apresentadas nos caracteres seriam sutis, de modo que quando inseridos em um contexto com inúmeras palavras seriam imperceptível a um leitor.

Entretanto, algumas restrições foram adotadas para realizar a escolha dos caracteres, as quais serão apresentadas na subseção 5.2, diminuindo, assim, o grau de perceptibilidade do leitor a mudanças, e, além disso, garantindo que tais mudanças permaneçam no documento após ser impresso.

Após a escolha do documento, três ações precisam ser realizadas para inserir a *watermark* sob o documento:

1. Criação do código identificador ou *watermark*;
2. Definição de um subconjunto de letras do mesmo alfabeto do texto a ser marcado;
3. E escolha de mecanismos de segurança adicionais para compor a *watermark*.

5.1. CRIAÇÃO DO CÓDIGO IDENTIFICADOR

Como um dos objetivos desse método é realizar a vinculação entre a cópia de um documento e seu destinatário, o código identificador deve manter relação com estes elementos.

A mensagem poderá ser a composição de diferentes códigos que ao final serão convertidos para bits. Para fins de teste, foram utilizados dois tamanhos de mensagens durante as pesquisas, a fim de ilustrar características distintas.

Como descrito na seção anterior, esse código deverá ser armazenado para que eventuais procedimentos de rastreamento de documentos sejam possíveis ou então a mensagem inserida contenha dados identificadores do destinatário.

5.2. DEFINIÇÃO DO SUBCONJUNTO DE CARACTERES

Por utilizar caracteres para inserir a *watermark*, é necessário definir quais caracteres serão utilizados neste processo. Os caracteres escolhidos sofreram alterações em suas formas originais, o que indicará a presença de um bit da mensagem oculta. Entretanto, a alteração e a escolha dos caracteres precisam manter a imperceptibilidade da *watermark* ao leitor.

Como o método é executado em documentos eletrônicos que permitem sua edição, as alterações no formato dos caracteres podem ser introduzidas por variações na diferença entre estilos de fontes, como a fonte *Arial* e a fonte *Calibri*. A letra 'a' nestas fontes apresentam aspectos semelhantes, mas existem detalhes em cada caractere que permite sua diferenciação. Outra abordagem seria a criação de fontes personalizadas com alterações de formatos, tendo como referência uma fonte textual conhecida.

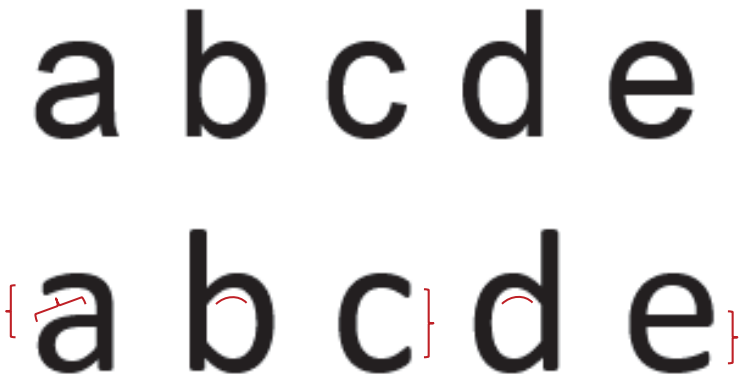


Figura 5.3 - Na linha superior são apresentados caracteres formatados com a fonte textual *Arial*, enquanto na linha inferior é utilizada a fonte *Calibri*. As marcações em vermelho ilustram as divergências de formato presente nos dois estilos, apesar de apresentarem contornos semelhantes.

Entretanto, nem todos os caracteres do texto são passíveis de alterações sutis, imperceptíveis ao leitor e que possam ser recuperadas posteriormente. A análise do caractere a ser alterado está diretamente relacionada à perceptibilidade desta alteração pelo leitor e a capacidade de manter essa alteração após um processo de fotocópia. Portanto, a escolha do subconjunto segue algumas regras e recomendações:

a) A escolha dos caracteres está relacionada ao idioma em que é escrito o documento. Por exemplo, segundo Zim (1948), no idioma inglês a sequência de caracteres mais utilizados é, de forma decrescente, "etaoin shrdlu cmfwyp vbgkqj xz". O assunto do texto e o estilo do autor também podem influenciar na frequência dos caracteres do texto. Para que uma *watermark* seja repetida o maior número de vezes durante o texto, é preferível a escolha de caracteres mais frequentes nas palavras do idioma do documento. A Tabela 5.1 **- Distribuição de frequência de letras em palavras de cinco diferentes idiomas.** descreve a frequência de ocorrência de letras em um alfabeto de cinco idiomas diferentes.

Tabela 5.1 - Distribuição de frequência de letras em palavras de cinco diferentes idiomas.

Letra	Português (Vicki, 2009)	Inglês (Zim, 1948)	Espanhol (Pratt, 1942)	Francês (Georges, 1976)	Alemão (Pacher, 2005)
a	14,634	8,167	11,525	7,636	6,516
b	1,043	1,492	2,215	0,901	1,886
c	3,882	2,782	4,019	3,260	2,732
d	4,992	4,253	5,010	3,669	5,076
e	12,57	12,702	12,181	14,715	16,396
f	1,023	2,228	0,692	1,066	1,656
g	1,303	2,015	1,768	0,866	3,009
h	0,781	6,094	0,703	0,737	4,577
i	6,186	6,966	6,247	7,529	6,550
j	0,397	0,153	0,493	0,613	0,268
k	0,015	0,772	0,011	0,049	1,417
l	2,779	4,025	4,967	5,456	3,437
m	4,738	2,406	3,157	2,968	2,534
n	4,446	6,749	6,712	7,095	9,776
o	9,735	7,507	8,683	5,796	2,594
p	2,523	1,929	2,510	2,521	0,670
q	1,204	0,095	0,877	1,362	0,018
r	6,530	5,987	6,871	6,693	7,003
s	6,805	6,327	7,977	7,948	7,270
t	4,336	9,056	4,632	7,244	6,154

u	3,639	2,758	2,927	6,311	4,166
v	1,575	0,978	1,138	1,838	0,846
w	0,037	2,361	0,017	0,074	1,921
x	0,253	0,150	0,215	0,427	0,034
y	0,006	1,974	1,008	0,128	0,039
z	0,470	0.074	0,467	0,326	1,134

b) Como o objetivo é serem imperceptíveis ao leitor, pequenas alterações em caracteres quando inseridos em agrupamentos de caracteres tornam essas alterações discretas. Entretanto, ao contrastar um caractere alterado com um caractere em sua forma original lado a lado, aumenta-se a chance do reconhecimento de tais alterações. Portanto, construções específicas de idiomas, como dígrafos na língua português (“rr”, “ss”, “ee” ou “oo”) ou na língua inglesa (“ll”, “tt”, “ff”, entre outras) podem comprometer a propriedade da imperceptibilidade. A possibilidade de haver um caractere com alterações, enquanto o outro permanece sem alterações pode aumentar as chances de o leitor perceber as mudanças.

Portanto, este tipo de construção linguística é ignorado durante a execução do algoritmo. Logo, seus caracteres nunca sofrerão mudanças ao longo do texto.

c) A quantidade de elementos do subconjunto de caracteres também tem implicações no desempenho e na eficácia da técnica. A escolha de um subconjunto A com muitos caracteres aumenta a possibilidade de que uma *watermark* possa ser inserida em um pequeno fragmento de texto, uma vez que a probabilidade de um caractere estar presente no subconjunto A é maior que a probabilidade de um caractere estar presente em um subconjunto menor A’. Portanto, dado que count(A) >= count(A’), onde *count* é uma função que contabiliza o número de caracteres em um subconjunto, temos que P(A) >= P(A’).

A vantagem de um subconjunto grande é a possibilidade de escrever a *watermark* repetidamente em trechos de texto menores, quando comparado ao subconjunto com poucos caracteres. Entretanto, outro impacto é o tempo de processamento que é afetado pelo maior número de alterações realizadas pelo algoritmo.

d) O tamanho da fonte textual pode afetar dois fatores no algoritmo: a perceptibilidade e a reprodutibilidade da *watermark*. O primeiro fator está relacionado à possibilidade do

leitor ser capaz de distinguir caracteres iguais, mas com formas diferentes. Aumentando-se o tamanho da fonte as alterações tornam-se mais evidentes, obtendo-se o efeito contrário com sua diminuição. Entretanto, a diminuição do tamanho do caractere pode afetar sua reprodutibilidade em processos de fotocópias e digitalizações. Como são introduzidos ruídos durantes estas etapas, as alterações nos caracteres podem ser perdidas nestes processos utilizando-se fontes textuais pequenas (Varna, 2009). Portanto, é necessário conciliar os dois aspectos para determinação de um tamanho ideal de fonte.

Como ilustrado na Figura 5.4, características dos caracteres são perdidas ao longo de sucessivos processos de impressão e digitalização, o que podem tornar irreconhecíveis letras após diversas iterações dessas etapas. A Figura 5.5 ilustra exemplos de ruídos inseridos em um processo de cópia de um documento impresso.

Figura 5.4 - Diferentes reproduções da letra ‘A’ através do processo de digitalização/impressão. A primeira letra representa a fonte original encontrada em um documento eletrônico, antes do processo de impressão. As demais representam resultados do processo de impressão seguido do processo de digitalização. Elas representam, respectivamente, a terceira, sexta e nona iterações do processo de impressão/digitalização do documento.

Figura 5.5 - A introdução de etapas de impressão e digitalização de documentos introduz ruídos no texto do documento. Na letra à direita, é possível observar *pixels* de cor cinza ao redor do caractere.

5.3. MECANISMOS DE SEGURANÇA ADICIONAIS

Para a formação do identificador foi acrescentado diferentes mecanismos de segurança com finalidades distintas. A *watermark* pode vir acompanhada de, por exemplo, um código preâmbulo; ser submetida a uma função criptográfica; ou um código de verificação de erro. No caso da utilização de um preâmbulo, é definido seu tamanho e se será inserido no início e/ou fim do código identificador, desta forma auxiliando na identificação da *watermark* no texto.

No segundo caso, uma função criptográfica é aplicada com a finalidade de ocultação da mensagem proposta, entretanto pode gerar uma *watermark* de tamanho maior ao inicial. O terceiro mecanismo proposto consiste na inclusão de um código de verificação de erros associado ao código identificador, a fim de detectar e recuperar bits errados na *watermark*.

Uma abordagem a ser utilizada com códigos identificadores pequenos é o código de *Hamming*(7,4) (Chen, 2011), o qual possibilita a detecção de até dois bits e a recuperação de até um bit da mensagem. A aplicação de um código de verificação contribui para solução de dois problemas (detecção e recuperação de bits) desse contexto de *watermarks* em documentos impressos ou digitalizados. Como existe a possibilidade de ruídos, é possível que alguma informação seja perdida durante o processo de recuperação da *watermark*; e no caso do código de *Hamming*, permite a detecção da letra que sofreu interferência ou foi alterada propositalmente, além de permitir sua correção.

5.3.1. Pseudocódigo do método

De posse do subconjunto de caracteres selecionados e da *watermark* a ser inserida, inicia-se a fase de inserção da *watermark* no documento escolhido, conforme ilustrado pela Figura 5.6. De acordo com o subconjunto de caracteres e a *watermark* convertida em bits, os caracteres do texto são alterados, a fim de que a *watermark* seja inserida, preservando a formatação do texto e gerando o menor impacto visual possível ao leitor. Os retângulos vermelhos na Figura 5.6 ilustram os caracteres que tiveram suas formas alteradas no texto, de acordo com os bits da *watermark*.

À medida que os caracteres do texto são lidos, a sequência de bits da *watermark* também são percorridos. Visto que a quantidade de caracteres do texto é superior à *watermark*, ao término da sequência de bits uma nova iteração deve ser iniciada. Entretanto, para o caso da quantidade de caracteres do documento ser inferior à sequência de bits, isto impossibilitará a execução do algoritmo, uma vez que não será possível inserir todos os bits da *watermark* no documento.

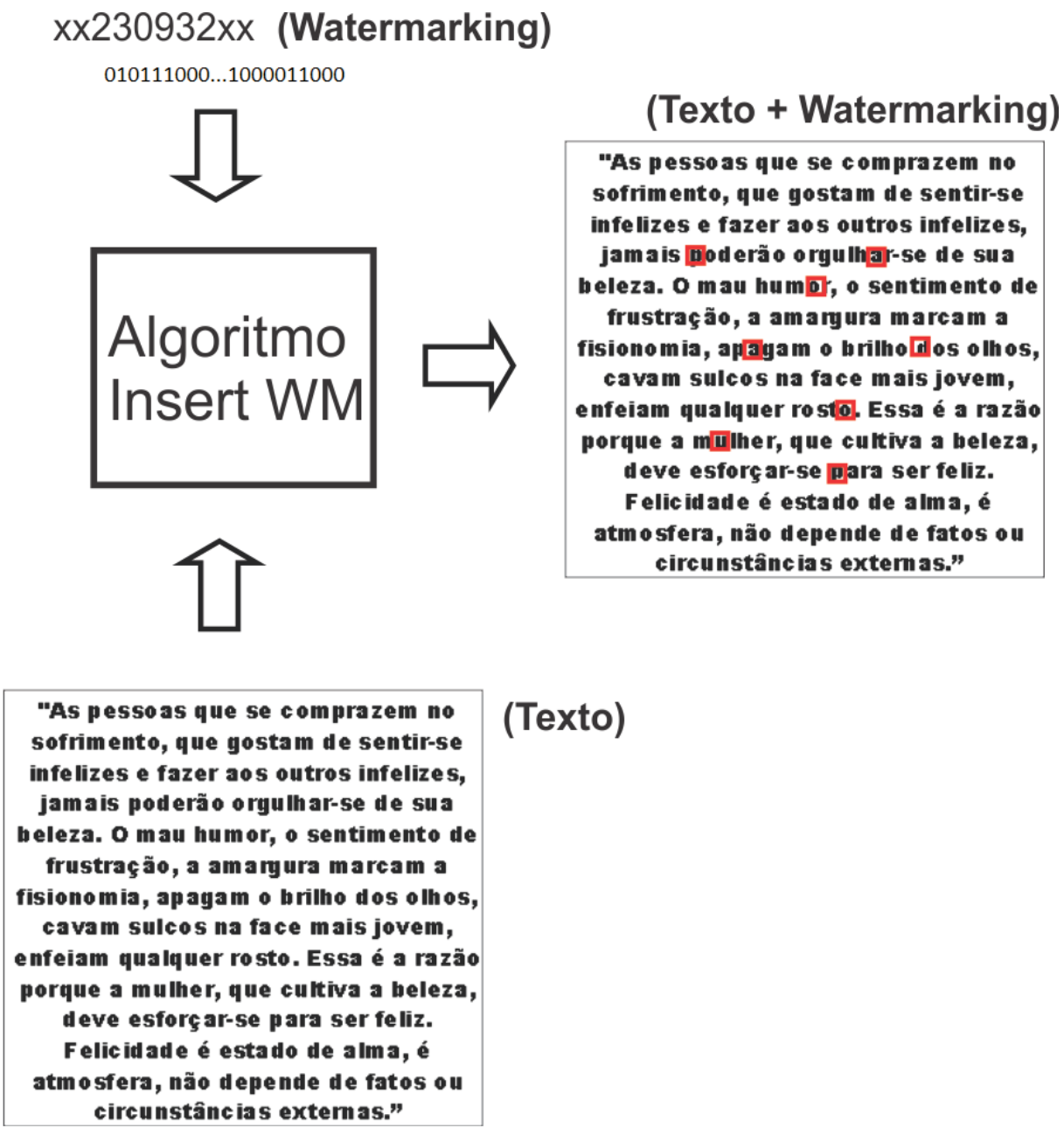


Figura 5.6 - A mensagem convertida em bits é introduzida no texto através do algoritmo proposto, produzindo um texto com a mesma semântica e sintática, entretanto com alterações visuais em alguns caracteres.

Os parâmetros de entrada do algoritmo são o código binário da *watermark*, o texto a ser alterado e o subconjunto de caracteres, nomeado como subconjunto C no código das Tabela 5.2 e Tabela 5.3 nomeado como subconjunto C. Cada caractere do texto é verificado, e caso seja um caractere pertencente ao subconjunto C, respeite as regras citadas anteriormente, como a presença de dígrafos, e o próximo bit da *watermark* tenha o valor '1', então o caractere terá sua forma alterada. Caso alguma dessas condições não seja atendida, o caractere não é alterado e o

algoritmo segue para o próximo caractere do texto. O algoritmo se encerra após analisar a última letra presente no texto. O pseudocódigo do algoritmo é detalhado na Tabela 5.2. Como o algoritmo é repetido até a última letra do texto, diversas *watermarks* podem ser inseridas até o término do texto, uma vez que geralmente o tamanho do texto é superior ao tamanho da sequência de bits.

Tabela 5.2 - Algoritmo para inserção da ***watermark*** em textos.

```
1. Obter Watermark;
2. Obter Subconjunto C; //Caracteres de forma variável
3. ENQUANTO texto não terminar FAÇA
4.      Próximo caractere do texto;
5.      SE letra pertence ao subconjunto C ENTÃO
6.          SE letra é um caractere válido ENTÃO //Regras
7.              SE próxima_letra_Watermark() == 1 ENTÃO
8.                  Alterar forma da letra no texto;
9.              Fim_Se
10.         Fim_Se
11.     Fim_Se
12. Fim_Loop
```

Para a recuperação da *watermark* o algoritmo de recuperação recebe como parâmetro o texto que possui a *watermark*, retornando o código binário referente à *watermark*. Para isto, o algoritmo percorre os caracteres do texto em busca dos caracteres presentes no subconjunto C e que obedeçam às regras citadas anteriormente. Caso a letra esteja alterada, então é retornado o valor ‘1’, caso contrário é retornado o valor ‘0’. Ao final do algoritmo é retornando uma sequencias de zeros e uns que representam a *watermark* inserida, conforme ilustra o pseudocódigo descrito na Tabela 5.3 e ilustrado na Figura 5.7.

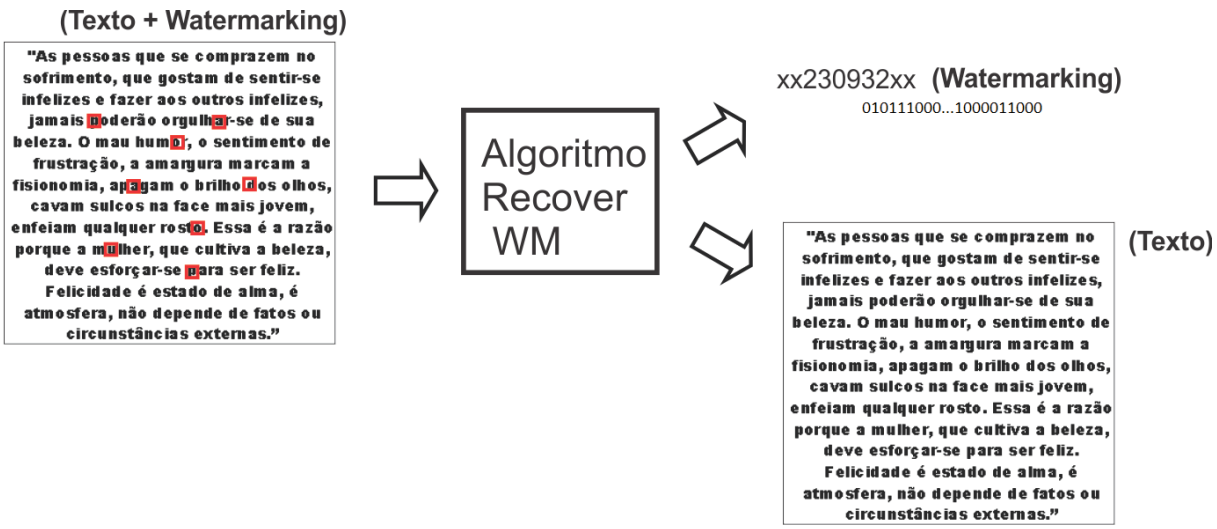


Figura 5.7 - O texto com a *watermark* é processado pelo algoritmo de recuperação, extraindo a partir do texto analisado a codificação binária inserida, e posteriormente transformando-a na mensagem oculta correspondente.

Tabela 5.3 - Algoritmo para recuperação da *watermark* em textos.

```
1. Obter Subconjunto C;
2. ENQUANTO Texto não acabar FAÇA
3.     Próximo caractere do texto;
4.         SE letra pertence ao subconjunto C ENTÃO
5.             SE letra é um caractere válido ENTÃO //Regras
6.                 SE letra tem a forma alterada ENTÃO
7.                     Watermark = Watermark + '1';
8.                 SENÃO
9.                     Watermark = Watermark + '0';
10.                Fim_Se
11.            Fim_Se
12.        Fim_se
13. Fim_Loop
```

Diante das considerações para execução do algoritmo e seus parâmetros de entrada e saída, a análise dos resultados obtidos de diversos experimentos nos permitirá mensurar se o método proposto possui as propriedades elencadas na seção 4 e se é possível de ser aplicável em ambientes reais com documentos reais.

6. RESULTADOS E DISCUSSÃO

Este capítulo será dedicado a apresentar dos resultados dos diferentes cenários no qual o método foi aplicado, tendo como principal objetivo a validação da solução proposta O método foi submetido a um trecho selecionado de texto, apresentado na Figura 6.1, e os resultados dos diferentes testes estão descritos ao longo desta seção.

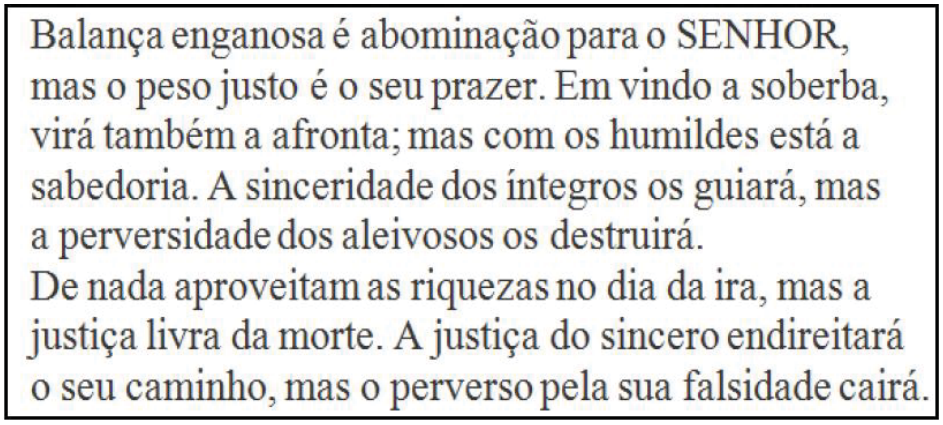

Balança enganosa é abominação para o SENHOR,
mas o peso justo é o seu prazer. Em vindo a soberba,
virá também a afronta; mas com os humildes está a
sabedoria. A sinceridade dos íntegros os guiará, mas
a perversidade dos aleivosos os destruirá.
De nada aproveitam as riquezas no dia da ira, mas a
justiça livra da morte. A justiça do sincero endireitará
o seu caminho, mas o perverso pela sua falsidade cairá.

Figura 6.1 - Texto original antes da inserção das *watermarks*.

Em um dos testes realizados foram definidas duas *watermarks* a serem inseridas no texto selecionado para, posteriormente, comparar os resultados obtidos. A primeira possui o tamanho de 16 bits, com preâmbulos de 4 bits e o código identificador de 8 bits. A segunda *watermark* era composta de uma palavra chave de 6 caracteres e será submetida ao algoritmo base64 (Linn, 1987), criando uma palavra de 64 bits no padrão ASCII. A função base64 é utilizada para demonstrar a possibilidade de emprego de uma função criptográfica sobre a *watermark*.

A *watermark* selecionada para o primeiro teste foi **1111100000101111**, enquanto a segunda *watermark* é **xx28xx**, que quando submetida à função base64 retornou **eHgyOHh4** em ASCII. Convertendo o texto para código binário, assumindo que cada letra é composta por oito bits, teremos **01100101 01001000 01100111 01111001 01001111 01001000 01101000 00110100**. O subconjunto de caracteres escolhido é: C = {a, d, e, i, r}, portanto esses caracteres poderão ser alterados no documento de acordo com as regras do algoritmo e da *watermark* escolhida. O tamanho e o estilo da fonte utilizada no texto selecionado são 12 e *Times New Roman*, respectivamente. As escolhas das *watermarks* foram aleatórias e utilizadas apenas para exemplificar a técnica.

Para alterar a forma dos caracteres selecionados foi escolhido um estilo de fonte que apresentava semelhanças com a fonte *Times New Roman*. O estilo de fonte *Caladea* apresenta semelhanças conforme ilustrado na Figura 6.2.

Figura 6.2 - Subconjunto de caracteres selecionados para teste. Na linha superior, os caracteres utilizam fonte *Times New Roman*, enquanto que na linha inferior utilizam fonte *Caladea*.

Três diferentes testes foram realizados sobre o texto. Primeiramente, duas *watermarks* de tamanhos diferentes foram aplicadas a duas cópias do texto. Posteriormente, o texto com a *watermark* será exibido após ser impresso e digitalizado, exemplificando quatro resoluções diferentes no equipamento de digitalização. Por fim, o material será exibido através de duas fotografias de *Smartphones* com câmeras de 5 e 8 *megapixels*. Os diferentes cenários têm como propósito ilustrar situações de utilização da técnica com parâmetros diferentes, desde modo ilustrando o comportamento do método em cada cenário.

6.1. *WATERMARKS* DE TAMANHOS DIFERENTES

Foram selecionadas *watermarks* de tamanhos distintos, uma de 16 bits e outra de 64 bits, para demonstrar as características que cada uma possui e seus reflexos sobre o texto. O mesmo texto foi utilizado para as duas *watermarks*, e como descrito no algoritmo da seção 5.3, a iteração do algoritmo é realizada sob todos os caracteres do texto do texto, de forma sequencialmente, finalizando sua execução após o último caractere. Como a *watermark* possui tamanho inferior ao número de caracteres encontrados no texto, então a mesma *watermark* é repetida inumeradas vezes dentro do documento até que o algoritmo seja encerrado.

Para facilitar a visualização da aplicação das *watermarks*, a cada iteração da *watermark* no texto seu início e término serão demarcados com retângulos, e as letras que foram selecionadas pelo algoritmo serão representadas pelos valores binários '0' ou '1' de acordo com a correspondência da *watermark,* conforme as Figura 6.4 e Figura 6.6.

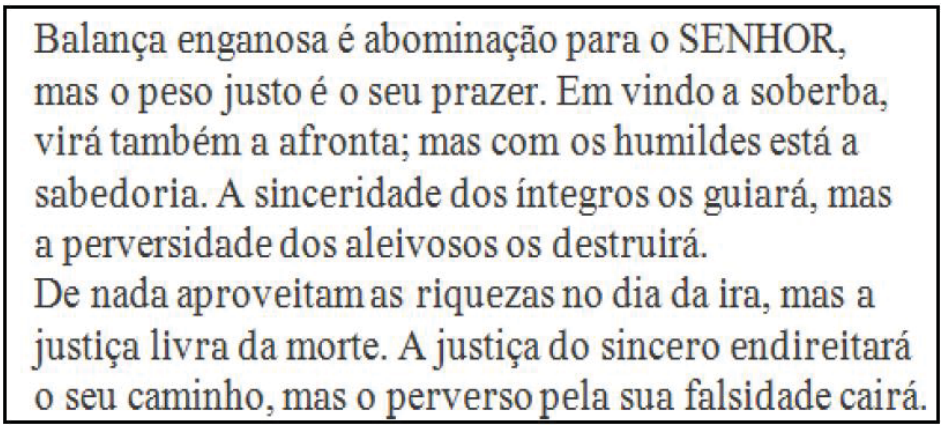

Balança enganosa é abominação para o SENHOR,
mas o peso justo é o seu prazer. Em vindo a soberba,
virá também a afronta; mas com os humildes está a
sabedoria. A sinceridade dos íntegros os guiará, mas
a perversidade dos aleivosos os destruirá.
De nada aproveitam as riquezas no dia da ira, mas a
justiça livra da morte. A justiça do sincero endireitará
o seu caminho, mas o perverso pela sua falsidade cairá.

Figura 6.3 - Texto após a inclusão da *watermark* de 16 bits '1111100000101111'.

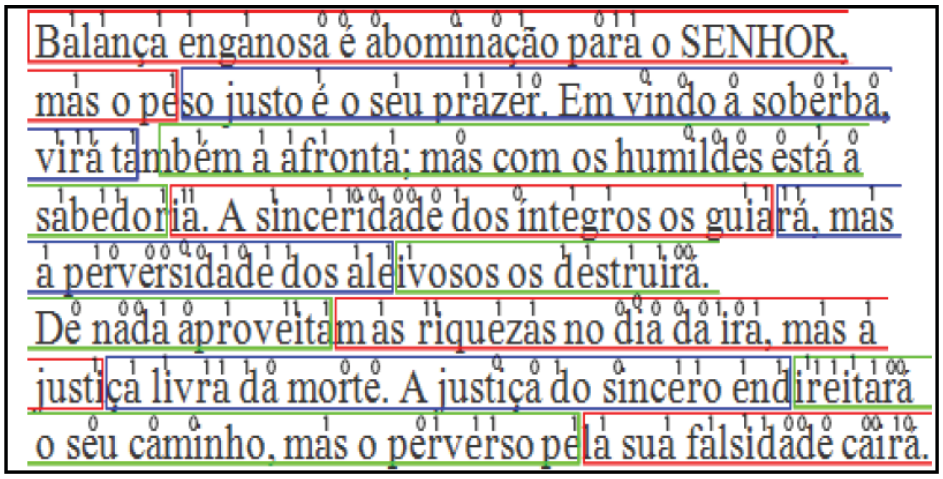

Balança enganosa é abominação para o SENHOR,
mas o peso justo é o seu prazer. Em vindo a soberba,
virá também a afronta; mas com os humildes está a
sabedoria. A sinceridade dos íntegros os guiará, mas
a perversidade dos aleivosos os destruirá.
De nada aproveitam as riquezas no dia da ira, mas a
justiça livra da morte. A justiça do sincero endireitará
o seu caminho, mas o perverso pela sua falsidade cairá.

Figura 6.4 - Texto com as marcações para *watermark* de 16 bits.

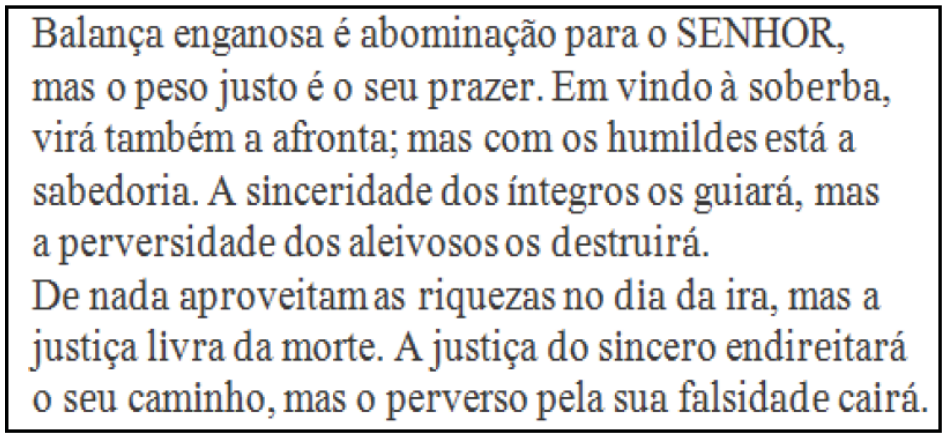


Figura 6.5 - Texto após a inclusão da *watermark* de 64 bits '01100101 01001000 01100111 01111001 01001111 01001000 01101000 00110100'.

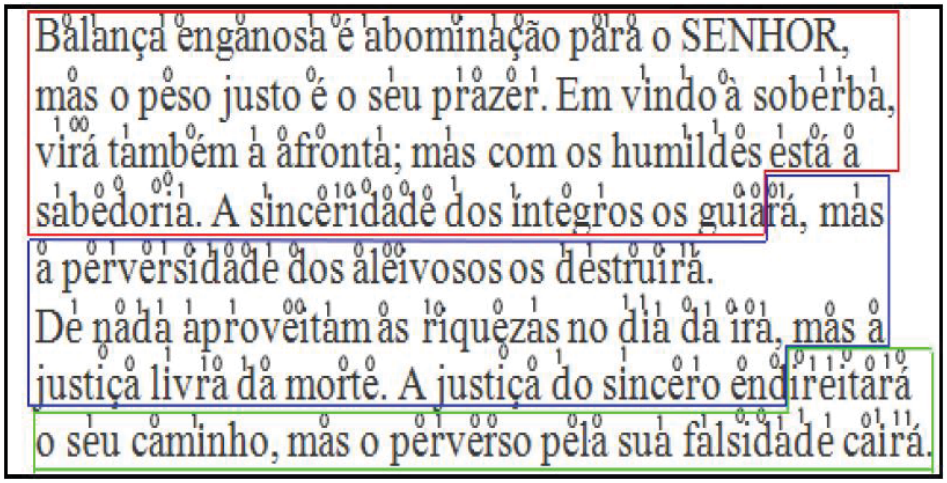


Figura 6.6 - Texto com as marcações para *watermark* de 64 bits.

Enquanto a *watermark* de 16 bits (Figura 6.4) utiliza pouco mais de uma linha para ser expressa, a segunda de 64 bits (Figura 6.6) utiliza quatro linhas para concluir sua primeira representação. A primeira *watermark* foi repetida nove vezes no trecho apresentado, enquanto a segunda apenas concluiu duas repetições no mesmo trecho de texto.

Em relação à primeira *watermark*, podemos destacar os seguintes aspectos:

- Capacidade de repetição maior, o que proporcionar maior robustez, uma vez que a *watermark* estará presente diversas vezes no documento. Enquanto a *watermark* de 16 bits foi repetida 9 nove vezes, a segunda *watermark* foi repetida apenas 2 vezes para o mesmo trecho de texto;

- Possiblidade de recuperação da *watermark* em pequenos fragmentos de texto, visto que uma cópia da *watermark* era inserida na proporção de uma *watermark* por linha, aproximadamente;
- Com a utilização de preâmbulos, no pior caso de busca da *watermark* no texto, no qual a *watermark* é desconhecida, serão verificados [2 * (tamanho em bits da *watermark*) - 1] caracteres pertencentes ao subconjunto C para encontrar a *watermark*, e no melhor caso a quantidade de bits da *watermark*.

Acerca dos aspectos destacados sobre a segunda *watermark* temos:

- Por ser uma sequência longa de bits, a utilização de uma função criptográfica, cujo retorno possua tamanho semelhante à *watermark*, antes da aplicação da técnica não influenciaria o comprimento da mensagem e ainda protegeria o conteúdo presente na *watermark*;
- Apesar de ter um número de bits maior, isto aumenta a complexidade de recuperação da sequência binária, uma vez que a aplicação da função criptográfica pode retornar sequências de bits de tamanhos variados;
- A mensagem transmitida contém mais informações que uma mensagem menor.

6.2. DIGITALIZAÇÕES COM DIFERENTES DPI (*DOTS PER INCH*)

O segundo teste teve por objetivo realçar as diferenças de qualidade existentes em documentos digitalizados com diferentes DPIs. Foram selecionados quatro modos de digitalização disponíveis em uma impressora multifuncional[4]. As opções selecionadas foram: digitalização em escala de cinza; resolução de 75 dpi, que é a menor resolução do equipamento; resolução de 200 dpi, que é a configuração padrão do dispositivo; e 600 dpi, que é a maior resolução do equipamento. Os resultados são apresentados em sequência nas figuras seguintes.

[4] Marca OKI Data Corporation, modelo MB491+

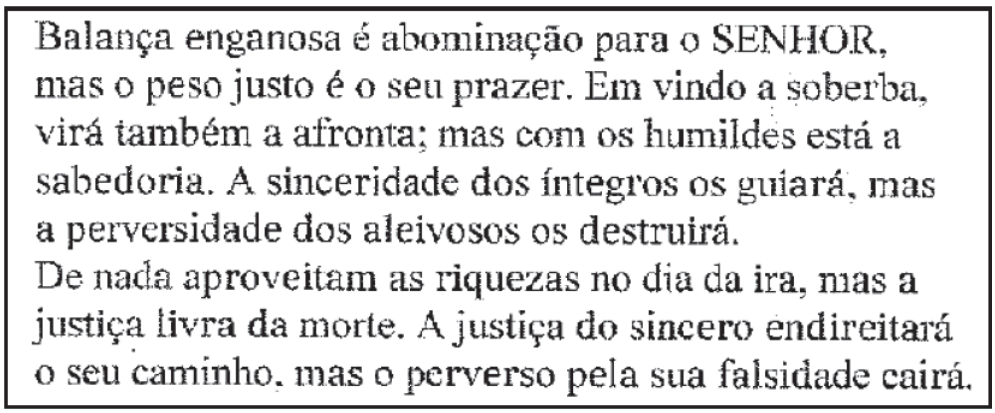


Figura 6.7 – Digitalização de texto em escala de cinza.

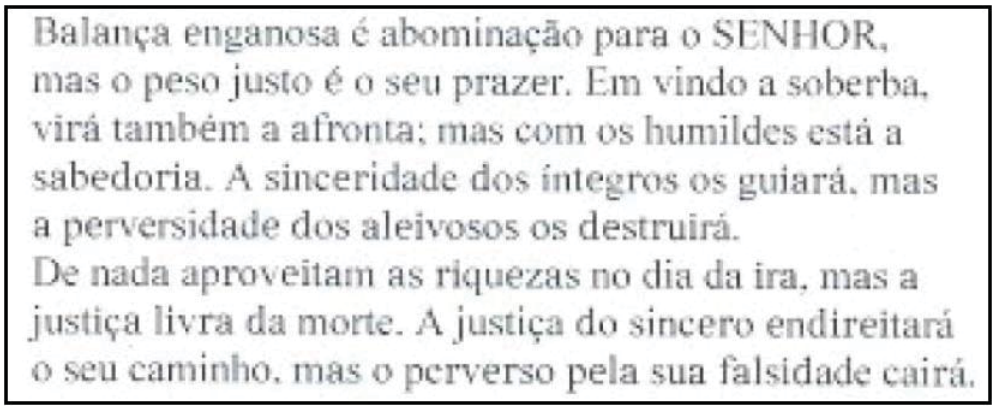


Figura 6.8 - Texto com resolução de 75 dpi.

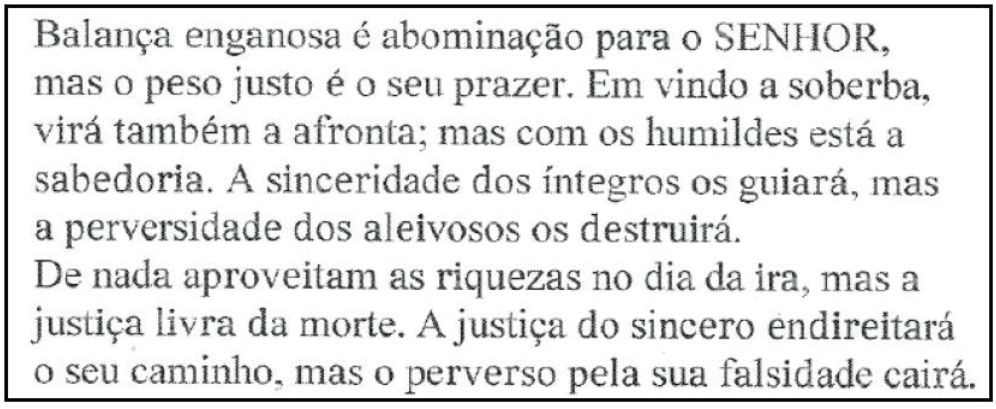


Figura 6.9 - Texto com resolução de 200 dpi.

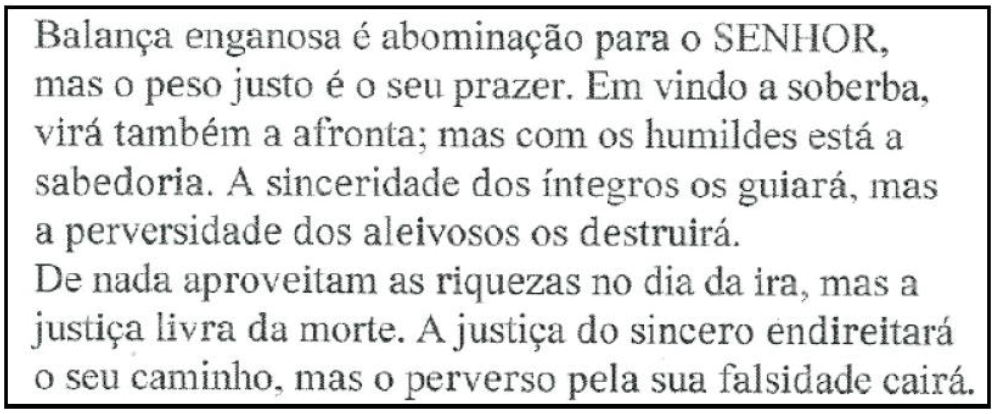


Figura 6.10 - Texto com resolução de 600 dpi.

As Figuras 6.7, 6.8, 6.9 e 6.10 permitem concluir que a qualidade da digitalização de um documento pode trazer dificuldades para recuperação da *watermark*. Uma imagem muito degradada pode interferir na interpretação dos caracteres analisados. Entretanto, nos quatro cenários analisados, através da ampliação das imagens, ainda é possível verificar as diferenças entre os caracteres, como ilustra a Figura 6.11. É perceptível que a degradação da imagem é mais acentuada com a resolução de 75 dpi, mas ainda existe a variação da silhueta da letra 'a' nos quatro cenários, o que a torna um caractere indicado para compor o subconjunto C, por manter sua forma mesmo após um processo de digitalização de baixa resolução. Propriedade que não é verdadeira para todos os caracteres de um alfabeto.

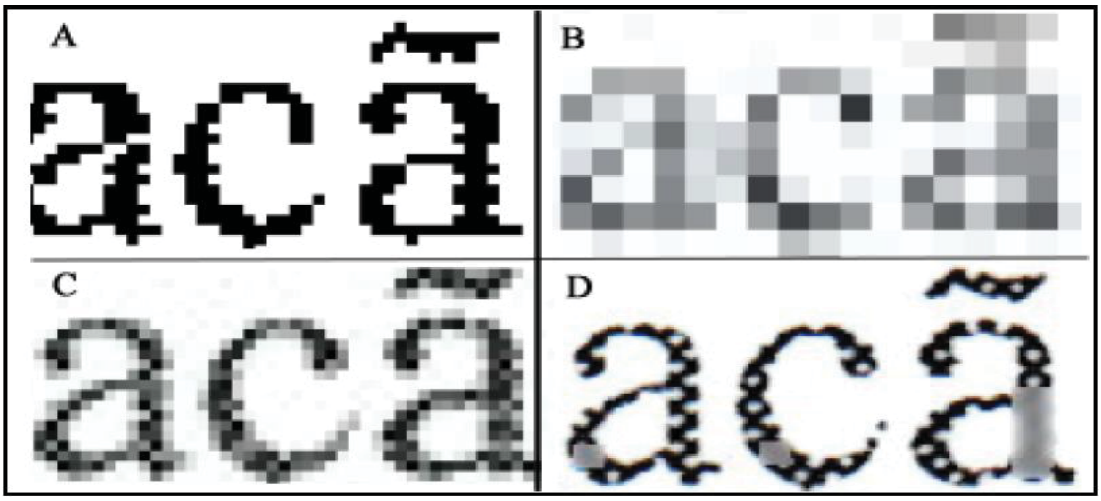


Figura 6.11 - Comparativo entre digitalizações do caractere 'a'. A) Digitalização em escala de cinza; B) Digitalização em resolução de 75 dpi; C) Digitalização em resolução de 200 dpi; D) Digitalização em resolução de 600 dpi.

Outro ponto a ser destacado é a distorção que algumas letras sofrem no processo de digitalização. Portanto, as variações dos caracteres selecionados para o subconjunto C devem ser avaliadas, para que não sejam ofuscadas pelo processo de digitalização.

Como a técnica de recuperação poderá ser empregada sobre imagens de baixa qualidade, o tratamento da imagem pode ser uma etapa anterior à aplicação do algoritmo. A manipulação de brilho e contraste de imagens podem acentuar as características das letras, como ilustra a Figura 6.12, que foram submetidas a tratamento. Como é uma imagem em escala de cinza, através da equalização do histograma da imagem obtemos uma melhor distribuição de cores ao longo do histograma (Gonzalez, 2010). Assim, realçando as características das imagens e destacando as formas dos caracteres.

Na Figura 6.12, também é possível observar a presença de ruídos ao redor dos caracteres. Com o aumento do valor da resolução do equipamento de digitalização o ruído diminui, estando mais concentrado próximo aos contornos dos caracteres. Como mencionado anteriormente e ilustrado pelas Figura 5.4 e Figura 5.5, a presença desses ruídos durante processos de digitalização podem afetar a identificação de caracteres ou distorcer a representação de traços destas letras.

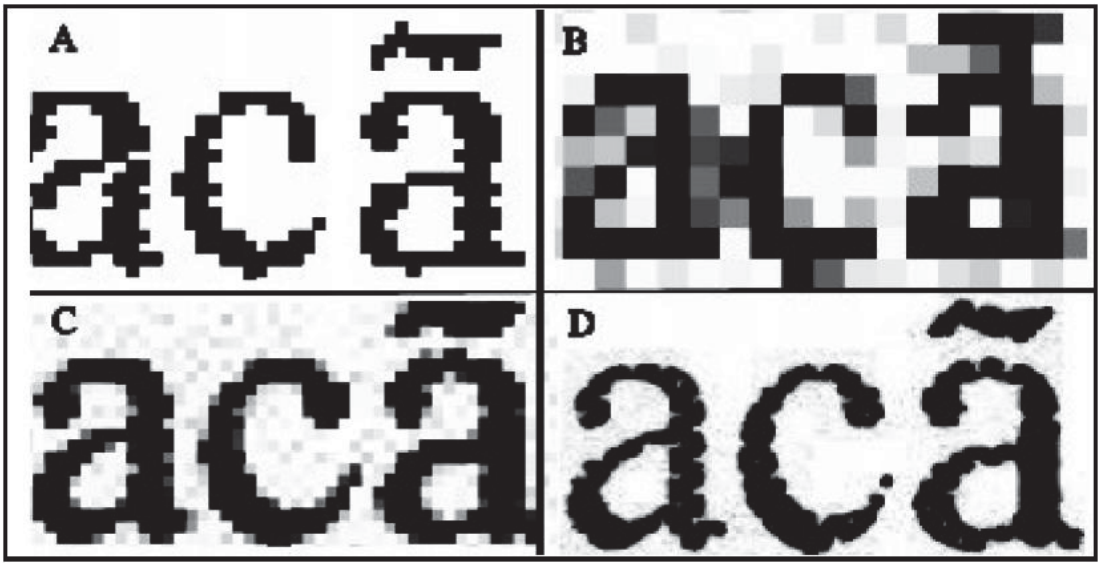


Figura 6.12 - Digitalizações do texto após o tratamento de brilho e contraste.

6.3. IMAGENS DE TEXTO ATRAVÉS DE FOTOGRAFIAS

Para o teste com fotografias foram utilizados dois Smartphones com câmeras acopladas. Os aparelhos possuíam câmeras com resolução de 5 e 8 *megapixels*, respectivamente, conforme ilustrado pela Figura 6.13 **- Fotografias do texto após a inserção da *watermark*. A) Câmera de 8 megapixels. B) Câmera de 5 *megapixels*.**. O objetivo desse cenário é mostrar uma comparação entre equipamentos com capacidades diferentes e menor impacto do ruído, quando comparado aos textos digitalizados.

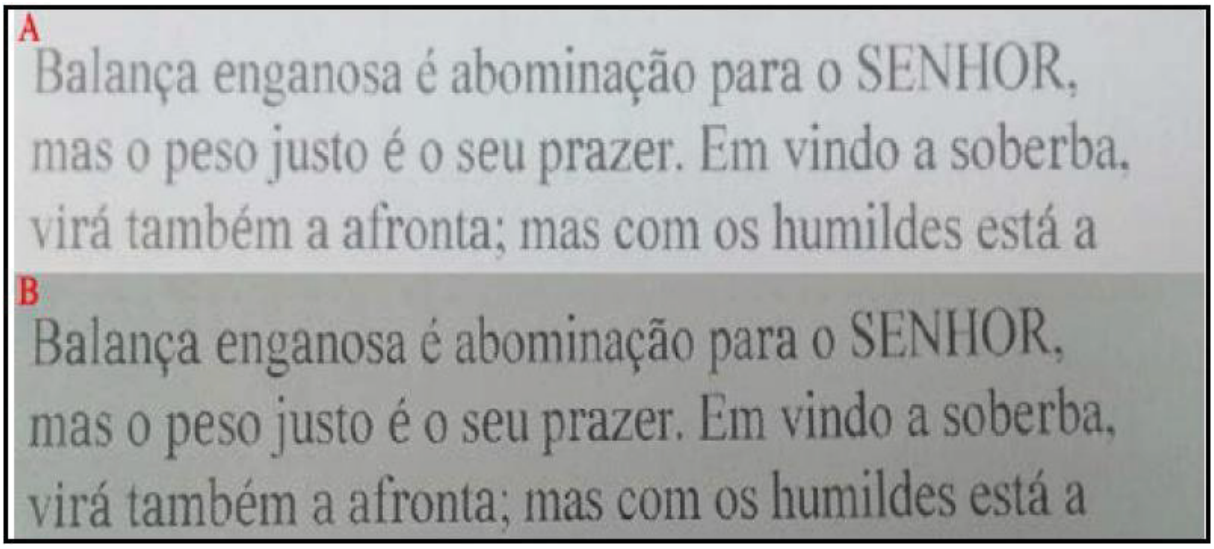


Figura 6.13 - Fotografias do texto após a inserção da *watermark*. A) Câmera de 8 megapixels. B) Câmera de 5 *megapixels*.

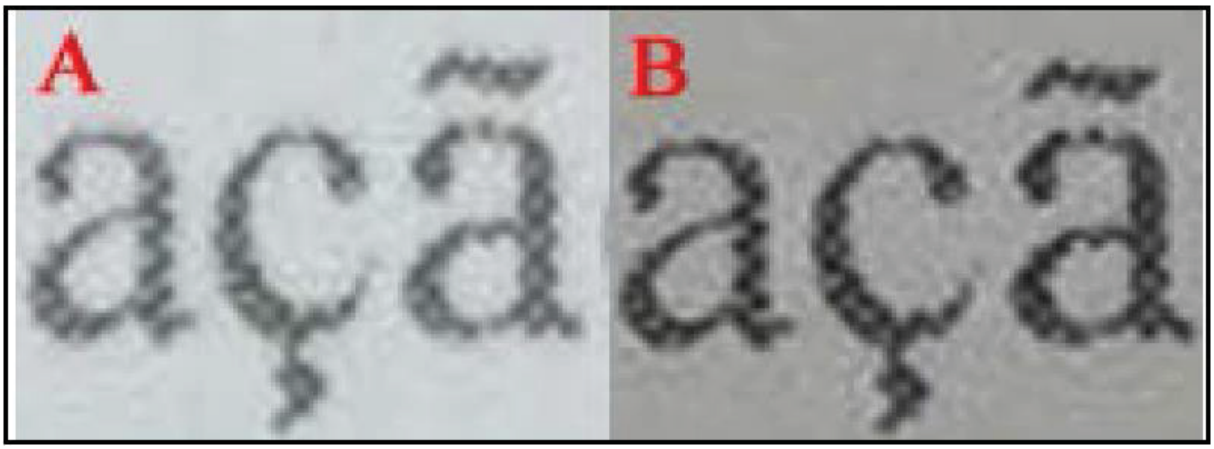


Figura 6.14 - Ampliação do texto fotografado após aplicação da *watermark*. A) Câmera de 8 megapixels. B) Câmera de 5 *megapixels*.

A análise da *watermark* através da fotografia permite concluir que as características identificadoras da *watermark* foram preservadas, permitindo a ampliação das imagens, mantendo os elementos identificadores dos caracteres, e obtendo resultados melhores que os textos digitalizados. Mesmo com o aumento da imagem (Figura 6.14), gerando distorções e ruído, ainda é possível identificar as letras que compõem a *watermark*.

Neste cenário não foram considerados parâmetros de fotografia como luminosidade, abertura do obturador e diafragma, ISO ou outra configuração de máquinas fotográficas.

6.4. ANÁLISES QUALITATIVA E QUANTITATIVA ENTRE A TÉCNICA PROPOSTA E OUTROS MÉTODOS

Alguns critérios foram considerados, a fim de se comparar o método proposto com as técnicas encontradas na literatura. Os testes verificaram: a quantidade de informação introduzida no texto (Davarzani, 2009); robustez contra-ataques de alteração intencional de texto, deleção de sentença/linha e modificação de formatação do texto (Chen, 2011); e detecção da *watermark* através de OCR. Foram selecionados os métodos *Line Shifting* e *Word-Shift Coding*.

Os algoritmos *Line Shifting* e *Word-Shift Coding* foram utilizados no texto da Figura 6.1. A Tabela 6.1 descreve a quantidade de bits inseridos no documento com oito linhas, setenta e três palavras e trezentos e trinta e seis caracteres. Os espaços em branco foram desconsiderados.

Tabela 6.1 - Relação entre quantidade de bits inserida no texto e método utilizado.

Método	**Nº de bits**
Line Shifting	4
Word-Shift Coding	30
Método Proposto (Subconjunto com 5 caracteres)	156

O método que possibilitou a menor quantidade de inserção de informação foi o método *Line Shifting*, uma vez que sua capacidade de introduzir informação está diretamente associada à quantidade de linhas presentes no texto. Apesar do método proposto, utilizando um subconjunto de 5 caracteres, inserir 156 bits neste documento, um aumento ou diminuição do número de caracteres desse subconjunto reflete diretamente na quantidade de informação que poderá ser inserida em um texto.

A análise quanto à robustez das técnicas, apenas o método proposto com a utilização de função criptográfica ou código de verificação de erros é capaz de detectar um ataque de alteração intencional do texto, entretanto somente utilizando o código de verificação de erros é possível recuperar o caractere alterado. Em relação à deleção de sentença/linha, os métodos *Line Shifting* e *Word-Shift Coding* não são robustos, porque essa remoção compromete a estrutura da *watermark*. O método proposto será robusto dependendo do tamanho da *watermark* escolhida e dos caracteres do subconjunto C, visto que para *watermarks* com sequências longas de bits a deleção poderá danificar parte da marcação.

Para o ataque de alteração de formatação, mudanças de alinhamento não comprometem a robustez do método proposto, o que não é verdade para os outros métodos testados. Entretanto, para mudanças no tamanho da fonte, a propriedade da imperceptibilidade pode ser afetada no método proposto, prejudicando também os outros métodos, como *Line Shifting* e *Word-Shift Coding*.

Quanto à utilização de OCR para detecção das *watermarks*, foi utilizada a biblioteca Tessaract OCR (Github, 2016), que quando executado nos documentos não detectou *watermarks* nas três técnicas.

6.5. AVALIAÇÃO DO MÉTODO PROPOSTO COM AS TÉCNICAS DE MENSURAÇÃO OBJETIVAS PSNR, MSE, RMSE E SSIM INDEX

Como citado na seção 2, acerca das propriedades de algoritmos de *watermarking*, uma das características das *watermarks* é a fidelidade. Após o processo de inserção da *watermarking*, o algoritmo tem como objetivo manter a semelhança entre o documento original e o novo documento. Quanto maior a semelhança, maior o nível de fidelidade do método.

Uma das maneiras de avaliar a fidelidade de duas imagens é através de métodos objetivos, os quais apresentam resultados estáticos que tem por objetivo mostrar o grau de

similaridade entre duas imagens. Por apresentar resultados rapidamente e ter uma relação custo-benefício melhor que métodos subjetivos, os quais precisam de avaliadores, são utilizados para avaliação de imagens (Almohammad, 2010). Como exemplos, existem os métodos PSNR, MSE, RMSE e SSIM index.

Para verificação dos valores relacionados ao PSNR, MSE e RMSE foi implementado um software para automatizar seu cálculo (Figura 6.15), e para o cálculo do SSIM index foi utilizado um *plugin* do software ImageJ. As imagens utilizadas são as mesmas apresentadas nos cenários anteriores, além de um novo conjunto de imagens do mesmo texto, mas com caracteres formatados com uma fonte desenvolvida especificamente para o propósito do experimento. Essa nova fonte é baseada na fonte *Times New Roman*, entretanto com modificações estruturais em alguns caracteres, conforme ilustrado na Figura 6.16.

O objetivo desse comparativo é verificar o grau de semelhança entre as imagens antes e após a introdução de um *watermark*. Desta forma, comparando a utilização do método proposto com fontes textuais usuais presentes nos editores de textos e fontes textuais personalizadas, as quais foram criadas especificamente para o método. Com a análise de imagens realizada pelo software ImageJ e os cálculos dos métodos PSNR, MSE, RMSE e SSIM index nestes dois cenários, é possível estimar qual abordagem introduz menor quantidade de ruído no documento final.

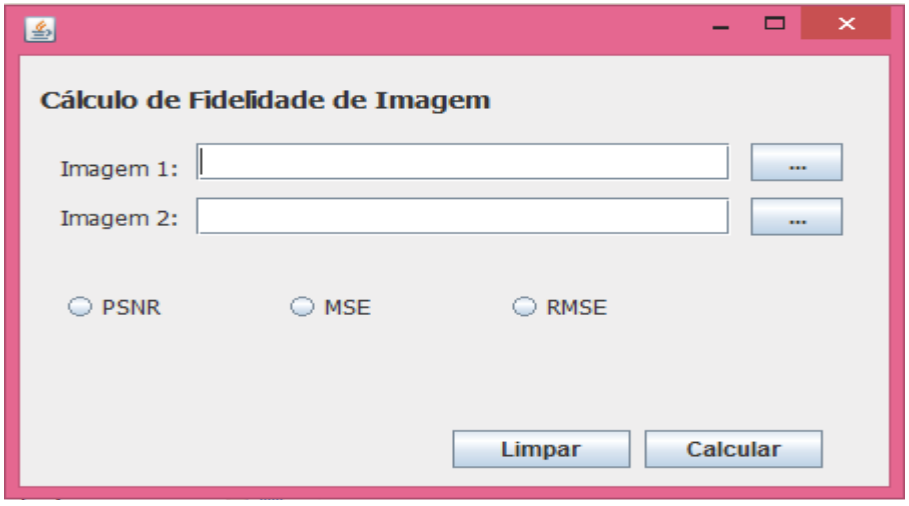


Figura 6.15 - Software utilizado para cálculo do grau de fidelidade a partir dos métodos PSNR, MSE e RMSE.

Figura 6.16 - Fontes criadas para o teste de fidelidade das imagens. Na coluna da esquerda a fonte criada para o teste e na coluna da direita a fonte *Times New Roman*.

A Figura 6.1 foi utilizada como imagem original (Imagem 1), enquanto as Figura 6.3 e Figura 6.5 Foram utilizadas para validação do método (Imagem 2). Como foram usados dois tipos de *watermark* (16 bits e 64 bits) são realizados cálculos distintos, um para cada *watermark*. Os resultados estão nas Tabela 6.2 e Tabela 6.3.

Tabela 6.2 - Resultado da análise sobre *watermark* de 16 bits e 64 bits utilizando PSNR, MSE, RMSE e SSIM index em imagens gerada a partir de alterações de fonte *Times New Roman* por fonte *Caladea*.

Método	**16 bits**	**64 bits**
PSNR	14.8070	12.8228
MSE	3394.7037	2149.7357
RMSE	58.264085	46.365242
SSIM index	0.2414	0.3984

Tabela 6.3 - Resultado da análise sobre *watermark* de 16 bits e 64 bits utilizando PSNR, MSE, RMSE e SSIM index em imagens gerada a partir da criação de uma nova fonte textual derivada da fonte *Times New Roman*.

Método	**16 bits**	**64 bits**
PSNR	10.8538	10.0558

MSE	6419.5006	5341.9496
RMSE	80.121786	73.088642
SSIM index	0.7287	0.6568

Os valores do método PSNR de imagens idênticas tende ao infinito, portanto quanto mais próximo de zero, maior o nível de similaridade dos pixels na região. Assim como os métodos MSE e RMSE, os quais também tende a zero. Enquanto o PSNR mensura o grau de similaridade entre as imagens, os métodos MSE e RMSE mensuram a diferença entre elas (Almohammad, 2010). Para o método SSIM index duas imagens são consideradas idênticas quando o valor de seu coeficiente tende a um.

Dois aspectos devem ser considerados nos resultados das Tabela 6.2 e Tabela 6.3: composição da *watermark* e o tipo de fonte textual utilizada. O primeiro aspecto não deve se restringir apenas ao tamanho da cadeia de bits que compõem a *watermark*. É preciso considerar quantos bits, efetivamente, são responsáveis por realizar as variações dos caracteres do texto, no caso a quantidade de bits '1' presentes na *watermark*. As sequências de bits utilizados são as mesmas apresentadas no início desta seção (1111100000101111 e 01100101 01001000 01100111 01111001 01001111 01001000 01101000 00110100), entretanto é possível observar que apesar da primeira sequência ter um total de 16 bits, ela possui 10 bits número '1'. Enquanto a segunda sequência de 64 bits possui 29 bits número '1'. Logo, para um mesmo fragmento de texto o número de alterações de caracteres é maior quando utilizado o *watermark* de 16 bits. Enquanto em um trecho de 64 caracteres eu poderia realizar no máximo 29 alterações de caracteres com a *watermark* de 64 bits, com a *watermark* de 16 bits eu poderia realizar até 40 alterações, uma diferença de 27% em relação à quantidade de caracteres alterados.

Quanto ao segundo aspecto, ao serem analisadas as imagens geradas pelos dois tipos de fontes são perceptíveis os diferentes níveis de ruídos gerados nas imagens, conforme ilustra a Figura 6.17. Na Tabela 6.2 é utilizada a fonte textual *Caladea* para substituir caracteres formatados com a fonte textual *Times New Roman*. Por apresentar formatos diferenciados, os caracteres possuem contornos que diferem as duas fontes, o que pode produzir *pixels* com tonalidades distintas, conforme ilustra a **Figura 6.17 - Diferentes exemplos da letra 'a'. No primeiro quadro a letra 'a' formatada com a fonte textual *Times New Roman*. No segundo quadro a letra 'a' com a fonte textual *Caladea*. No terceiro quadro a mesma letra com uma variação da fonte *Times New Roman*.**.

Enquanto na Tabela 6.3, a fonte *Times New Roman* é alterada, removendo alguns detalhes dos caracteres, mas preservando grande parte de seus contornos. Desta forma, graduação de cores e contornos são semelhantes, reduzindo o nível de ruído gerado.

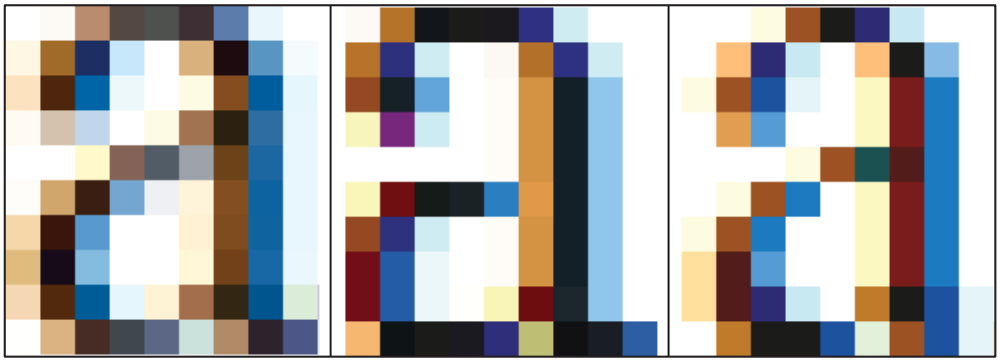


Figura 6.17 - Diferentes exemplos da letra ‘a’. No primeiro quadro a letra ‘a’ formatada com a fonte textual *Times New Roman*. No segundo quadro a letra ‘a’ com a fonte textual *Caladea*. No terceiro quadro a mesma letra com uma variação da fonte *Times New Roman*.

A diferença de quantidade de caracteres alterados refletiu sobre os resultados apresentados na Tabela 6.2 e Tabela 6.3. Na primeira tabela os valores da *watermark* de 16 bits são piores que os valores da *watermark* de 64 bits, com exceção do método SSIM index, comportamento que ocorreu em quase toda a segunda tabela, mas com valores melhores que a primeira tabela. Esse comportamento na Tabela 6.3 tem relação, principalmente, com o segundo aspecto, que introduz menos ruídos através da fonte personalizada.

Os métodos PSNR, MSE e RMSE utilizaram a diferença das cores dos pixels para estimar um valor, motivo pelo qual as *watermarks* de 16 bits apresentavam maiores ruídos, visto que apresentavam uma maior quantidade de caracteres alterados. Quando utilizado a fonte *Caladea* é perceptível que o nível de ruído é maior quando comparado à fonte *Times New Roman* customizada. Entretanto, quando mensurado o grau de semelhança através do método SSIM index o resultado foi diferente. A fonte *Caladea* inseriu maior quantidade de ruído, tendo seu resultado pior para *watermark* de 16 bits, o que não aconteceu para a fonte textual customizada. Diferente dos outros três métodos, o SSIM index utiliza três diferentes parâmetros (luminosidade, contraste e estrutura dos *pixels*) para construir seu indicador, e não apenas a coloração dos *pixels* da imagem.

Após a análise quantitativa das imagens, foi utilizado o software ImageJ para destacar as diferenças entre as imagens. O software conta com uma função (SUB) que permite verificar regiões de duas imagens que apresentam divergências. Essas áreas aparecem com tonalidade cinza, caso contrário, apresentam coloração preta. As imagens utilizando fonte *Caladea* e *Times New Roman* personalizada foram avaliadas, conforme ilustram as Figura 6.18 e Figura 6.19.

Os resultados apresentados mostram uma maior quantidade de divergências na imagem gerada a partir da fonte textual *Caladea*, porque existe uma quantidade maior de ruído introduzido com a troca de fontes. As distorções criadas acontecem porque a fonte *Caladea* introduz letras semelhantes, mas com diferenças em seus contornos, conforme ilustra a Figura 6.17.

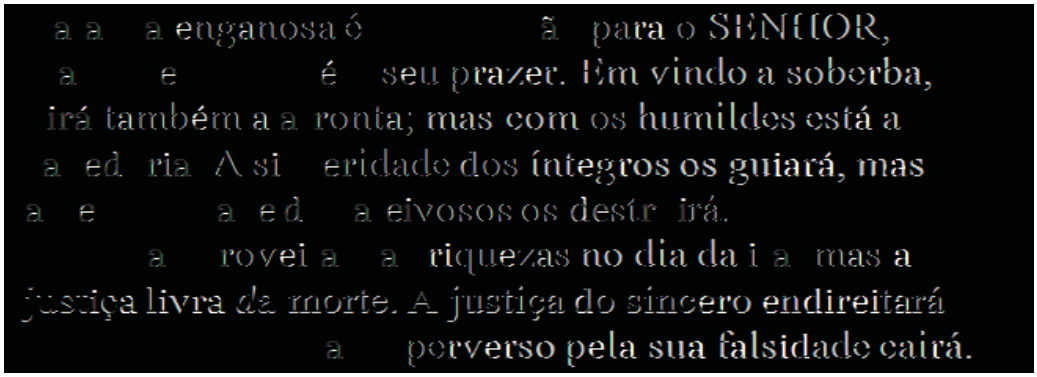


Figura 6.18 - Resultado da função SUB do software ImageJ em um texto modificado com a fonte textual *Caladea*. As áreas cinzas revelam as diferenças entre a imagem original e a alterada.

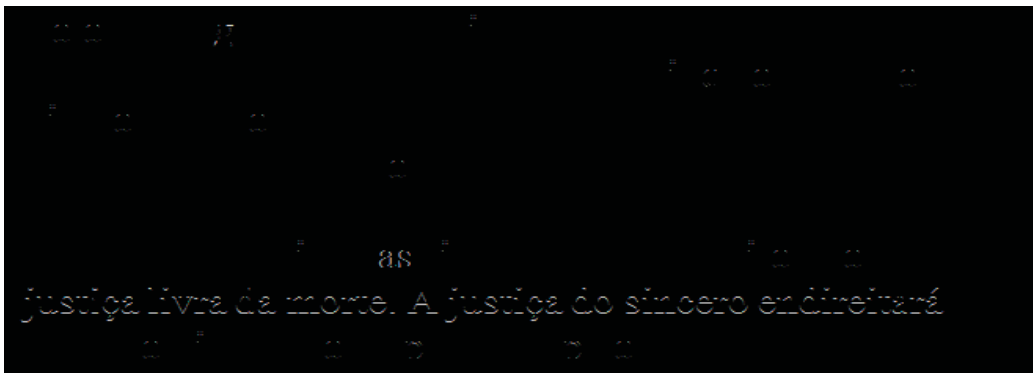


Figura 6.19 - Resultado da função SUB do software ImageJ em um texto modificado com a fonte textual **Times New Roman** personalizada. As áreas cinzas revelam as diferenças entre a imagem original e a alterada.

6.6. AVALIAÇÃO DO MÉTODO PROPOSTO COM MÉTODO SUBJETIVO

Conforme argumentado por Gonzalez (2010), apesar de automatizar e tornar mais célere o processo de comparação entre imagens utilizando abordagens objetivas, esses métodos não apresentam a sensibilidade visual que humanos possuem.

A forma de cálculo do método PSNR, por exemplo, consegue encontrar variações de cores de pixels, o que pode ser difícil para a percepção humana, entretanto, as variações de dois tipos de cores podem apresentar valores iguais. Essas variações são tratadas de forma semelhante pelo método, porém, se analisada por um ser humano, essas variações serão consideradas diferentes. Da mesma forma, o método SSIM index apresenta problema com imagens borradas, as quais seriam percebidas facilmente por um indivíduo.

Segundo Almohammad (2010), além de serem mais confiáveis que os métodos objetivos, principalmente devido ao fato do destinatário dos documentos serem pessoas, a utilização de uma metodologia subjetiva também é coerente para validação do método proposto. Como citado por Gonzalez (2010), a adoção de formulários é uma maneira de avaliação do grau de semelhança entre imagens. Para executar esse teste foi criado um formulário com oito perguntas, em que cada pergunta apresenta uma comparação entre duas imagens, classificando-as por meio de uma escala de 1 a 6, conforme citado no trabalho do autor Gonzalez (2010), e também baseado no método DSCQS (*Double Stimulus Quality Scale Method*) de Whag (2003), que relaciona duas imagens lado a lado com uma escala de avaliação. A escala contém como nível mais baixo a expressão "Totalmente Diferente" e como nível mais elevado a expressão "Idêntico". O método DSCQS propõe que as perguntas sejam inseridas aleatoriamente, além de não informar qual seria a imagem de referência.

O questionário foi aplicado a um grupo de 50 Peritos Criminais, os quais já trabalharam com comparação de documento, portanto com experiência em detecção de diferenças entre documentos questionados e documentos padrões em procedimentos criminais.

Para realizar os testes foram selecionados quatro grupos de imagens: imagens produzidas por textos utilizando *watermarks* com a fonte textual *Caladea*; textos produzidos com a *watermark* com a fonte textual *Times New Roman* personalizada; conjunto de imagens sem nenhuma alteração (idênticas); e, por fim, imagens de textos com fontes diferentes. Ao todo foram criadas oito perguntas, duas delas para cada um dos grupos. Não foi definido um conjunto de características das imagens que deveriam ser avaliadas, apenas foi solicitado que

realizassem comparações e aferissem o grau de similaridade entre as imagens apresentadas em cada pergunta.

Conforme sugerido por Gonzalez (2010), foi utilizada uma escala para graduar o nível de semelhança entres as imagens, como ilustra a Figura 6.20.

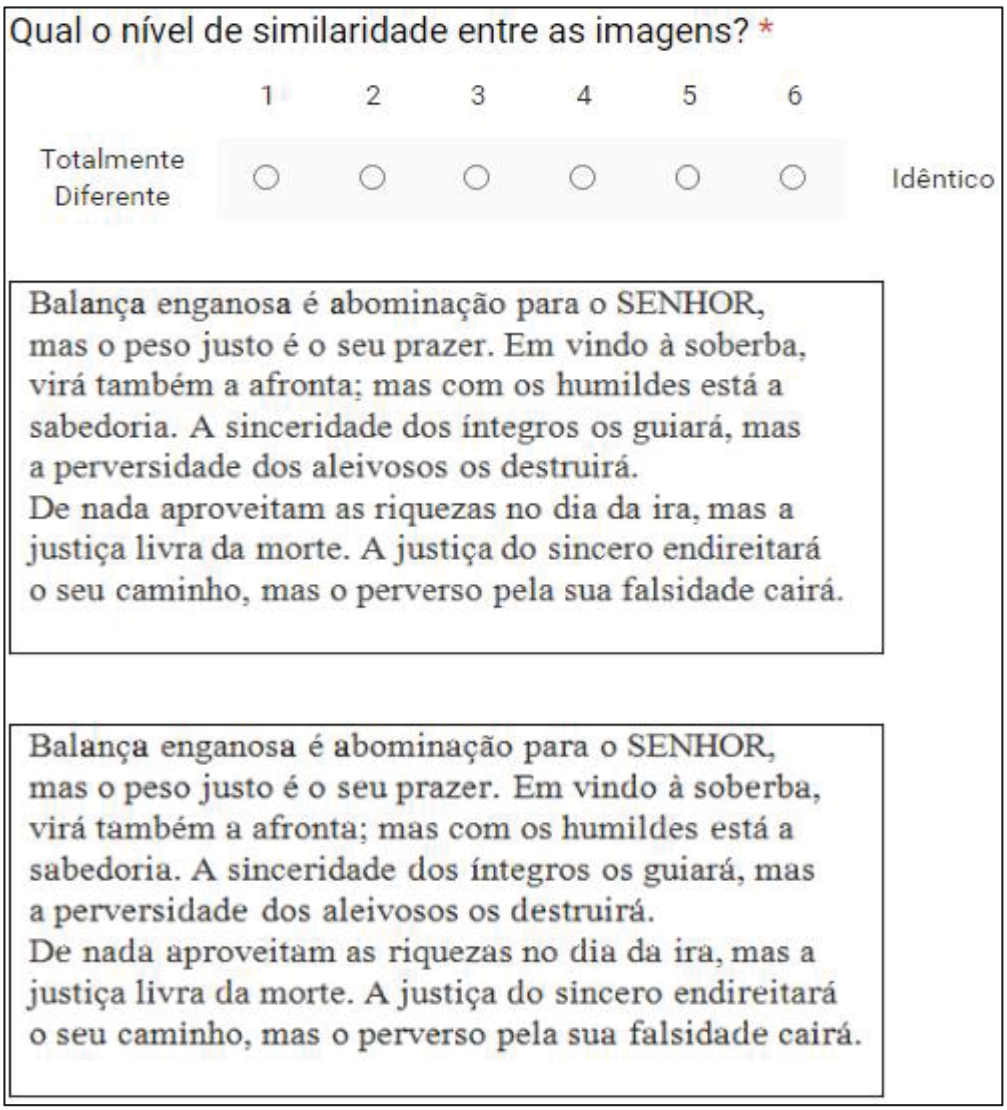


Figura 6.20 - Exemplo de pergunta realizada no teste subjetivo de comparação de imagens textuais. O entrevistado poderia escolher valores de 1 a 6, no qual a opção 6 significaria que as imagens são idênticas e a opção 1 representaria o oposto.

Os resultados obtidos foram representados através de quatro gráficos, um para cada grupo de perguntas. Os grupos de imagens idênticas e com fontes divergentes foram utilizados como controle do experimento. O resultado obtido no grupo de imagens de textos formatados

com a *watermark Times New Roman* personalizada teve resultado inferior apenas ao grupo de imagens idênticas. Mais da metade dos entrevistados assinalou que a qualidade das imagens deste grupo estava entre os níveis 5 e 6, conforme ilustra a Figura 6.22.

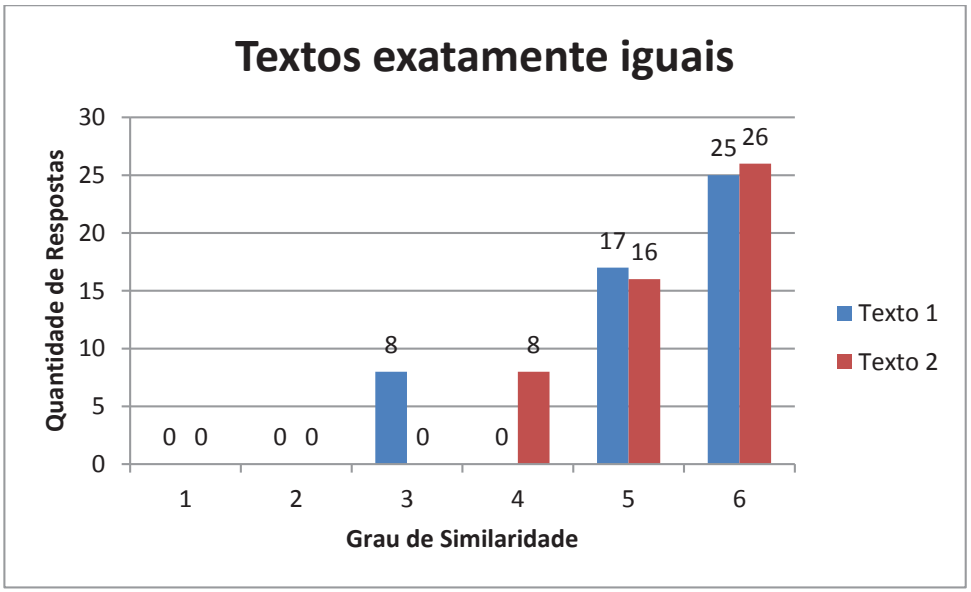


Figura 6.21 - Avaliação dos entrevistados acerca das perguntas com imagens idênticas.

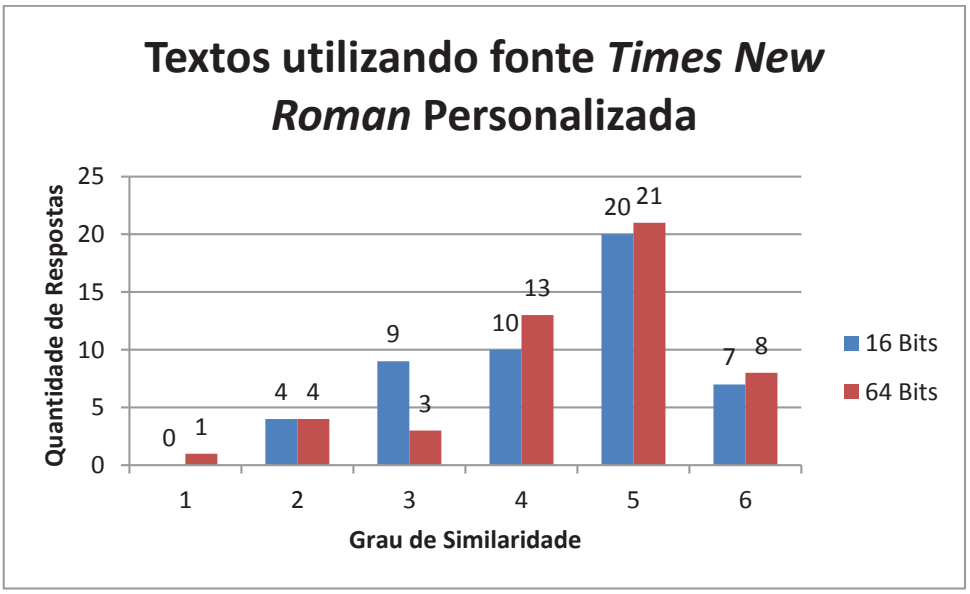


Figura 6.22 - Avaliação dos entrevistados acerca das perguntas com imagens textuais produzidas com a utilização de uma fonte textual *Times New Roman* personalizada.

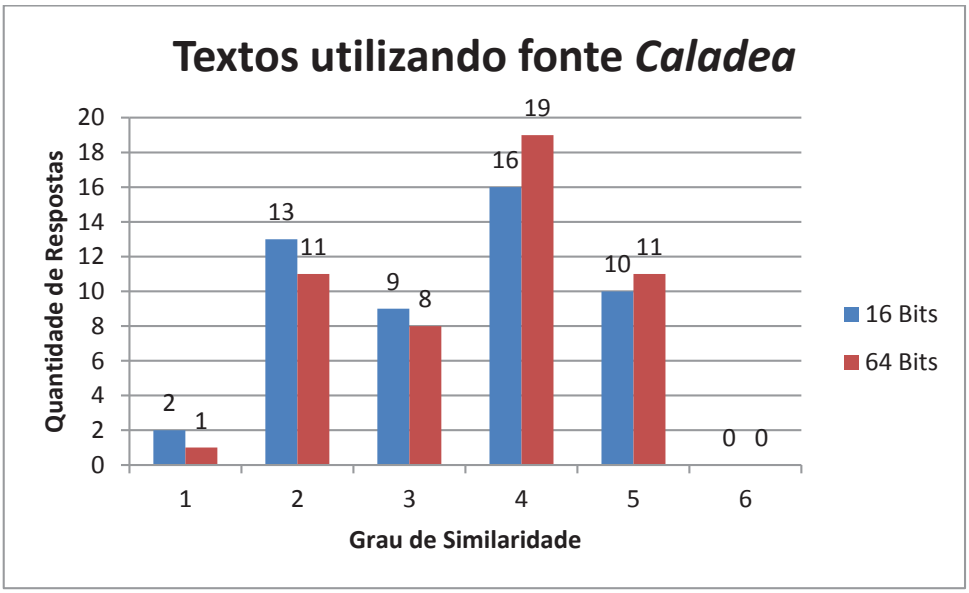


Figura 6.23 - Respostas dos entrevistados quando comparada imagens textuais produzidas com a utilização da fonte textual *Caladea*.

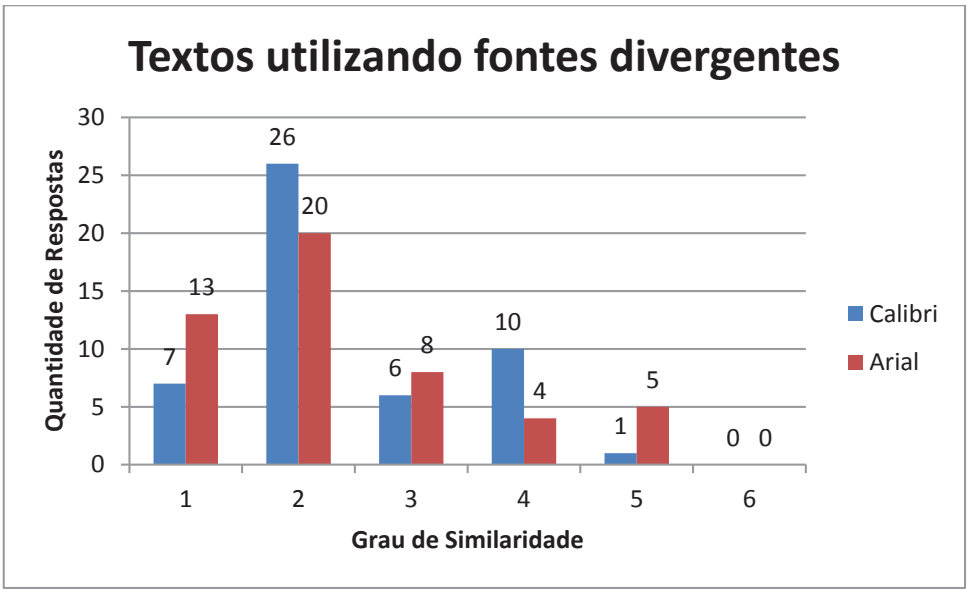


Figura 6.24 - Respostas dos entrevistados quando comparada duas imagens de textos produzidos por fontes textuais diferentes.

Para ilustrar o desempenho dos entrevistados os resultados foram agrupados nos quatro grupos de perguntas através das médias das respostas em cada grupo para cada grau de similaridade presente no questionário, produzindo o gráfico da Figura 6.25.

Como esperado, o maior grau de similaridade ocorreu para as imagens idênticas, representado pela barra de cor verde. Nota-se que nenhum dos entrevistados selecionou a opção 1 (Totalmente Diferente) para as imagens idênticas. Comparativamente, as imagens de textos com fontes *Times New Roman* personalizada obtiveram desempenho superior às imagens de texto com fonte *Caladea*, que por sua vez foi melhor que as imagens de texto com fontes diferentes.

Não foram estipulados critérios de avaliação durante a pesquisa, a fim de que os entrevistados percebessem as distorções presentes nas imagens, não sendo direcionados pelo entrevistador. Não houve delimitação de características ou ponderação de quais seriam mais importantes durante a análise.

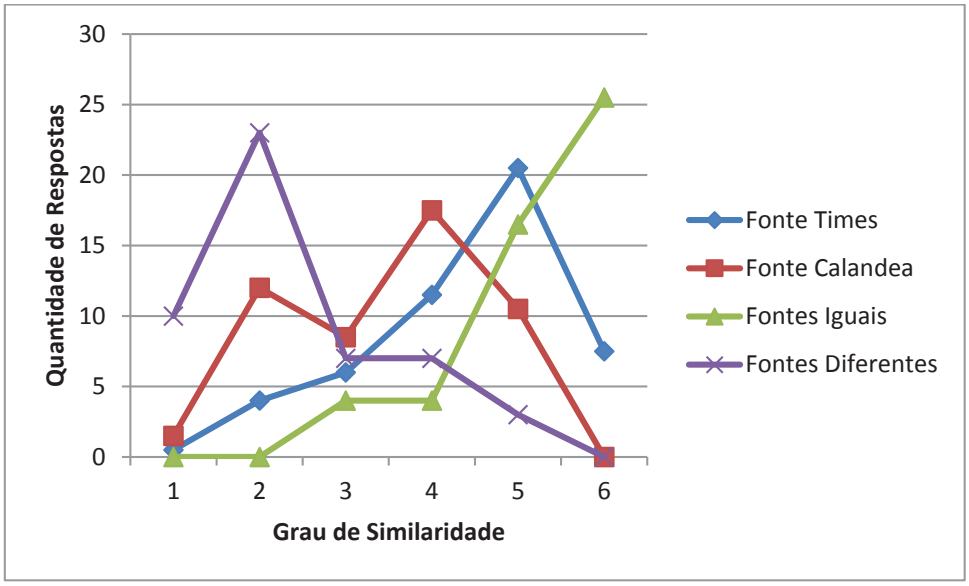


Figura 6.25 - Comparativo do desempenho dos entrevistados nos quatro grupos de perguntas presentes no questionário.

O cálculo para construção do gráfico da Figura 6.25 foi baseado no número MOS (Mean Opinion Score), proposto por Simone (2009). Ele propõe que sejam realizados somatórios de todas as respostas para cada pergunta e seus resultados sejam divididos pelo número de entrevistados, conforme ilustra a Equação 11. Onde m_{nk} é o valor atribuído à imagem pelo entrevistado n para a pergunta k, e N é o número de entrevistados.

O gráfico da Figura 6.25 mostra as fontes iguais tendo um crescimento, o que representa a tendência dos entrevistados em concluírem se tratarem da mesma imagem. O gráfico da fonte

Times New Roman personalizada, também revela a tendência a concluírem pela similaridade, mas alguma característica dos textos realçou alguma divergência, tornado a reta decrescente ao final. A fonte *Caladea* apresentou oscilações durante o experimento, e a linha das fontes diferentes apresentou um comportamento descente esperado.

$$MOS_k = \frac{\sum_{n=1}^{N} m_{nk}}{N} \tag{11}$$

Alguns aspectos podem ser destacados a partir da análise desse capítulo. Podemos destacar três principais variáveis que estão relacionadas diretamente com o método proposto. A primeira seria a qualidade do documento que influência a capacidade de identificar as formas dos caracteres. Outro aspecto é a escolha dos caracteres que serão alterados durante o algoritmo, uma vez que a escolha de caracteres com poucos traços identificadores ou muito sutis pode influenciar a propagação desses traços para outras cópias e digitalizações, e portanto a eficácia do método. E por fim, o tipo de avaliação que deve ser realizada sobre o resultado final do processo de *watermarking*. As avaliações objetivas e subjetivas possuem suas vantagens e desvantagens, portanto é preciso decidir quais são os objetivos e custos a serem alcançados com a mensuração.

7. ESTUDO DE CASO

Para verificar a aplicação do método proposto em um cenário prático, o algoritmo desenvolvido foi submetido a um ambiente real de produção de documentos. Para executar os testes de desempenho da técnica foi selecionado o órgão público Ministério Público do Estado do Mato Grosso.

O órgão produz diferentes tipos de documentos com graus distintos de sigilo, podendo ter como destinatários variadas partes pertencentes a processos e procedimentos administrativos e judiciais. Portanto, uma das atividades inerentes ao órgão é a tramitação de documentos, tanto em seus setores e departamentos, como para outras entidades. Entre os documentos que podem estar em trânsito estão arquivos classificados como sigilosos, os quais devem ser acessados somente por pessoas com autorização, não podendo ser divulgados.

Como forma de identificar possíveis divulgações não autorizadas de documentos sigilosos, o Ministério Público do Mato Grosso - MPMT, em sua unidade denominada GAECO (Grupo de Atuação Especial de Combate ao Crime Organizado), passou a testar a utilização de *watermarks* em documentos produzidos por esta unidade. Na estrutura do GAECO existe a Coordenadoria de Inteligência, a qual é responsável por produzir Relatórios de Informações, Relatórios Técnicos e Auto Circunstanciado de Interceptação Telefônica ou Telemática. Documentos os quais foram submetidos ao método proposto neste trabalho.

Antes da adoção de *watermarks* em documentos, o setor utilizava apenas o algoritmo MD5 (*Message-Digest algorithm 5*) em arquivos presentes em CDs e DVDs, com a finalidade de garantir a integridade das informações presentes nas mídias, as quais eram encaminhadas ao Juiz responsável por autorizar as medidas de interceptação telefônica ou telemática.

Para composição das *watermarks* são utilizadas informações relacionadas ao documento e ao destinatário do documento, portanto são geradas *watermarks* diferentes para destinatários diferentes em um mesmo documento. Para garantir a preservação e o controle das *watermarks* utilizadas, é utilizado um banco de dados SQLite[5] para armazená-las, permitindo consultas que possam relacionar as marcações com seus respectivos destinatários.

[5] É uma biblioteca que implementa um banco de dados embutido que utiliza os comandos padrões dos principais bancos de dados.

A ferramenta foi desenvolvida em linguagem JAVA[6], utilizando a versão 7 de sua *engine*, além de bibliotecas *open-source* para manipulação de arquivos Microsoft Office Word com extensão .docx.

Para o ambiente do MPMT foi definido um formulário eletrônico relacionado aos dados identificadores dos documentos do órgão. A Figura 7.1 **- Tela do software desenvolvido para inserir *watermarks* em documentos .docx.** ilustra os principais dados que um documento pode conter, por exemplo, número do documento, ano de emissão, tipo de documento, origem e setor. Além dos campos informados o formulário solicita que seja informado um destinatário ou setor a que o documento será encaminhado, objetivando manter um controle de cópias do material. Por fim, também é solicitado que se informe sobre quais caracteres se pretende aplicar o algoritmo de *watermarking*. Como resultado temos uma sequência de bits que representaria nossa *watermark*. Ela contém informações relacionadas ao documento e seu destinatário.

A Figura 7.2 **- Tela do software para recuperação de uma *watermark* a partir de um documento .docx.** ilustra o processo de recuperação da *watermark* a partir de um documento eletrônico .docx ou uma sequência de bits. O que mostra se esse documento ou sequencial está relacionado à alguma *watermark* existe, permitindo que se faça um controle de rastreabilidade das cópias de documentos.

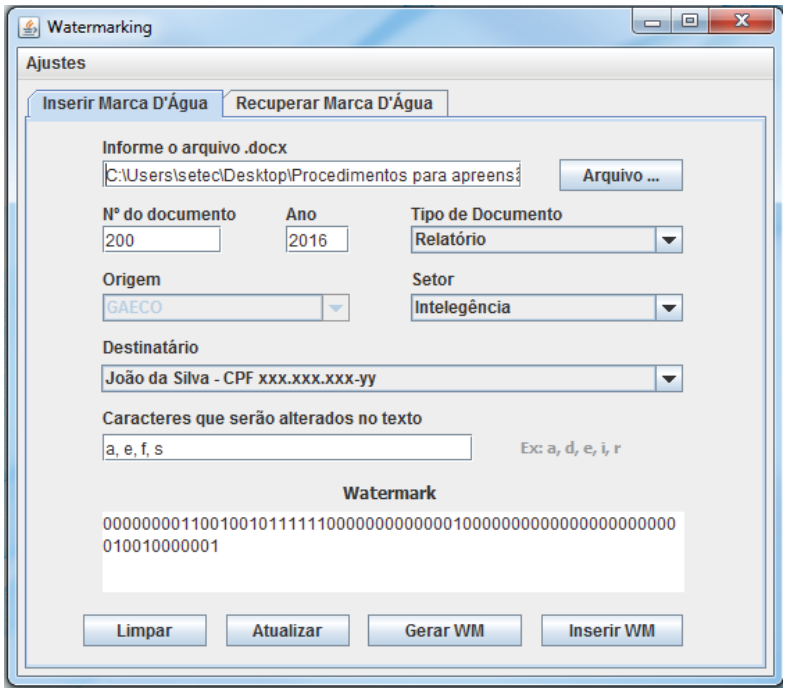


Figura 7.1 - Tela do software desenvolvido para inserir *watermarks* em documentos .docx.

[6] Linguagem de programação interpretada e orientada a objetos criada pela empresa Sun Microsystems.

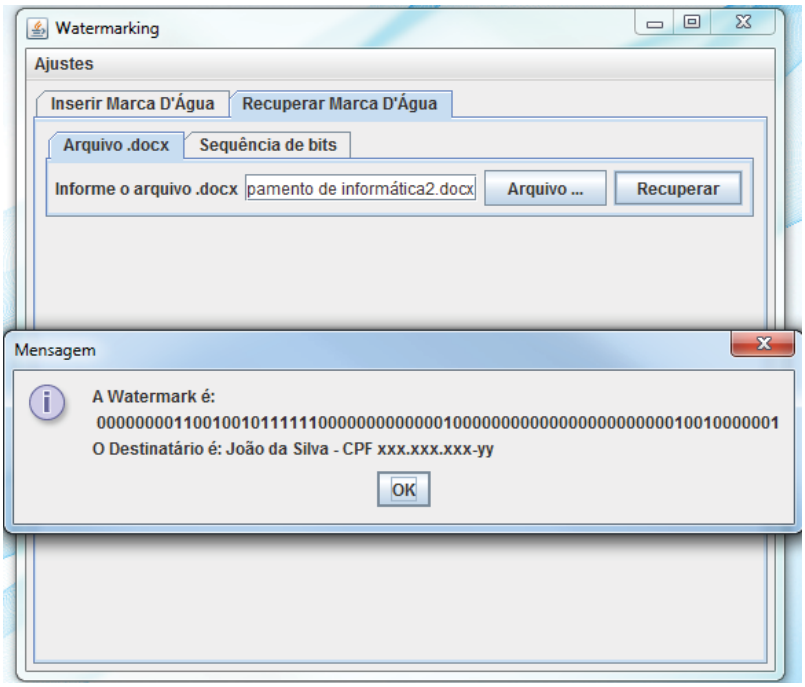
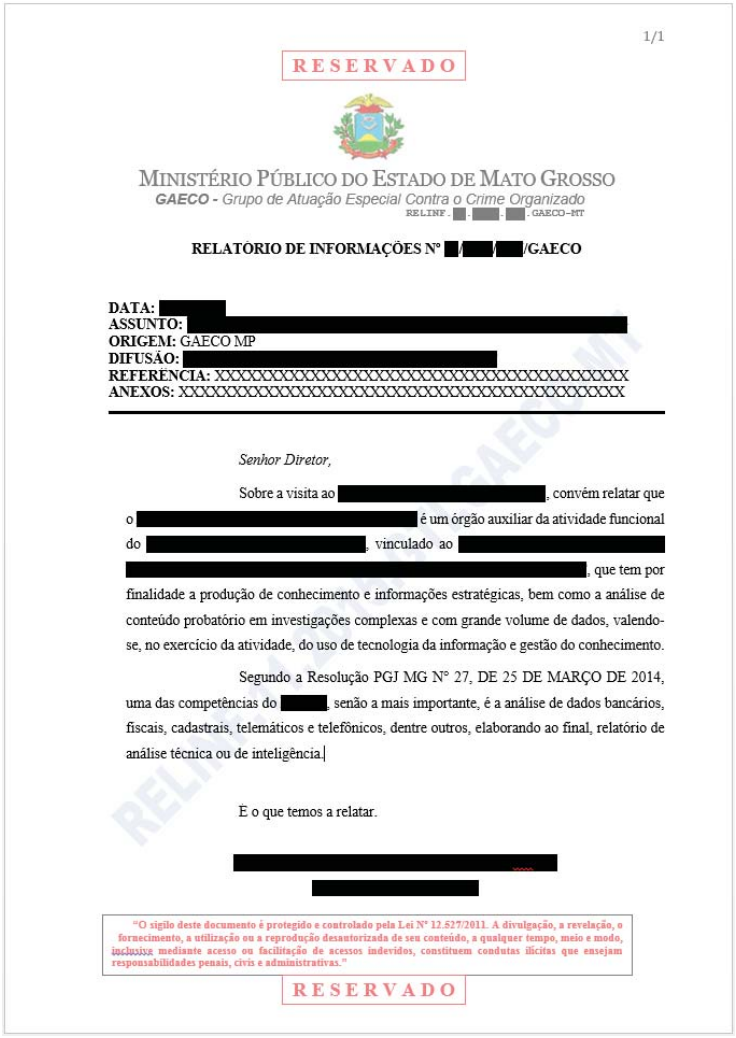


Figura 7.2 - Tela do software para recuperação de uma ***watermark*** a partir de um documento .docx.

As Figura 7.3 e Figura 7.4 ilustram o documento produzido pelo Ministério Público do Mato Grosso, na unidade GAECO, antes da inserção da *watermark* e após a introdução de uma *watermark*, respectivamente, a qual se repete ao longo do texto do documento. Os retângulos pretos foram inseridos na documento a fim de ocultar lugares e nome de indivíduos, não fazendo parte do processo de inclusão da *watermark*.

A maior parte da estrutura do documento foi mantida, sofrendo alterações apenas nos caracteres escolhidos para compor o vetor de caracteres do algoritmo (a, e, f, s).

Os mesmos documentos, antes e após o procedimento de *watermarking*, foram comparados através do software ImageJ, a fim de encontrar as divergências entre as imagens dos dois documentos. A Figura 7.5 é o resultado de uma comparação do software por meio de uma função de diferença (SUB) entre imagens. Quanto mais escuro a região, mais similares são as imagens comparadas. Portanto, é perceptível que regiões como o cabeçalho e rodapé, os quais não são alvo de alterações pelo algoritmo, permanecem idênticos, enquanto as regiões centrais da imagem apresentam áreas acinzentadas, denotando possíveis diferenças.



1/1

RESERVADO

MINISTÉRIO PÚBLICO DO ESTADO DE MATO GROSSO

GAECO - Grupo de Atuação Especial Contra o Crime Organizado

RELINF . [redacted] . [redacted] . [redacted] . GAECO-MT

RELATÓRIO DE INFORMAÇÕES Nº [redacted]/GAECO

DATA: [redacted]
ASSUNTO: [redacted]
ORIGEM: GAECO MP
DIFUSÃO: [redacted]
REFERENCIA: XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
ANEXOS: XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

Senhor Diretor,

Sobre a visita ao [redacted], convém relatar que o [redacted] é um órgão auxiliar da atividade funcional do [redacted], vinculado ao [redacted], que tem por finalidade a produção de conhecimento e informações estratégicas, bem como a análise de conteúdo probatório em investigações complexas e com grande volume de dados, valendo-se, no exercício da atividade, do uso de tecnologia da informação e gestão do conhecimento.

Segundo a Resolução PGJ MG N° 27, DE 25 DE MARÇO DE 2014, uma das competências do [redacted], senão a mais importante, é a análise de dados bancários, fiscais, cadastrais, telemáticos e telefônicos, dentre outros, elaborando ao final, relatório de análise técnica ou de inteligência.

È o que temos a relatar.

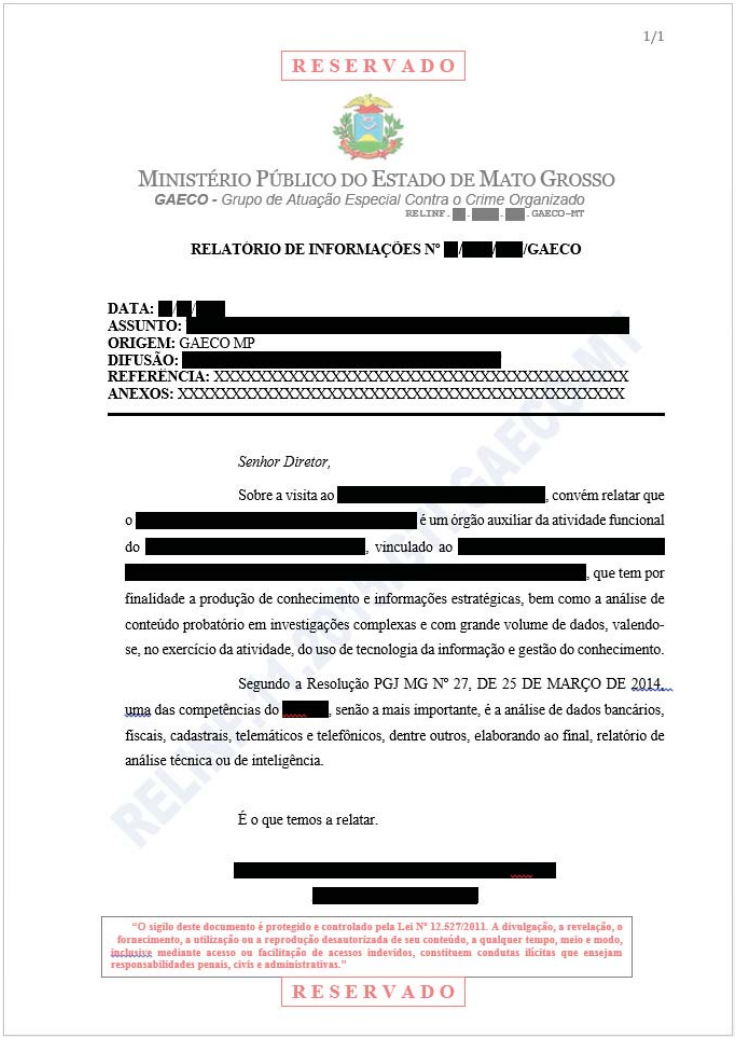
[redacted]

[redacted]

"O sigilo deste documento é protegido e controlado pela Lei Nº 12.527/2011. A divulgação, a revelação, o fornecimento, a utilização ou a reprodução desautorizada de seu conteúdo, a qualquer tempo, meio e modo, inclusive mediante acesso ou facilitação de acessos indevidos, constituem condutas ilícitas que ensejam responsabilidades penais, civis e administrativas."

RESERVADO

Figura 7.3 - Exemplo do documento original produzido pelo Ministério Público do Mato Grosso/GAECO antes da inserção de *watermarks*. Ressalta-se que os retângulos pretos foram colocados apenas para ocultar informações do documento original.



1/1

RESERVADO

MINISTÉRIO PÚBLICO DO ESTADO DE MATO GROSSO

GAECO - Grupo de Atuação Especial Contra o Crime Organizado

RELINF . [redacted] . [redacted] . [redacted] . GAECO-MT

RELATÓRIO DE INFORMAÇÕES Nº [redacted]/[redacted]/[redacted]/GAECO

DATA: [redacted]
ASSUNTO: [redacted]
ORIGEM: GAECO MP
DIFUSÃO: [redacted]
REFERÊNCIA: XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
ANEXOS: XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

Senhor Diretor,

Sobre a visita ao [redacted], convém relatar que o [redacted] é um órgão auxiliar da atividade funcional do [redacted], vinculado ao [redacted], que tem por finalidade a produção de conhecimento e informações estratégicas, bem como a análise de conteúdo probatório em investigações complexas e com grande volume de dados, valendo-se, no exercício da atividade, do uso de tecnologia da informação e gestão do conhecimento.

Segundo a Resolução PGJ MG Nº 27, DE 25 DE MARÇO DE 2014, uma das competências do [redacted], senão a mais importante, é a análise de dados bancários, fiscais, cadastrais, telemáticos e telefônicos, dentre outros, elaborando ao final, relatório de análise técnica ou de inteligência.

É o que temos a relatar.

[redacted]

"O sigilo deste documento é protegido e controlado pela Lei Nº 12.527/2011. A divulgação, a revelação, o fornecimento, a utilização ou a reprodução desautorizada de seu conteúdo, a qualquer tempo, meio e modo, inclusive mediante acesso ou facilitação de acessos indevidos, constituem condutas ilícitas que ensejam responsabilidades penais, civis e administrativas."

RESERVADO

Figura 7.4 - Exemplo de documento final produzido pelo Ministério Público do Mato Grosso/GAECO após a inserção de *watermarks*. Ressalta-se que os retângulos pretos foram colocados apenas para ocultar informações do documento original.

Os mesmos documentos, antes e após o procedimento de *watermarking*, foram comparados através do software ImageJ, a fim de encontrar as divergências entre as imagens dos dois documentos. A Figura 7.5 é o resultado de uma comparação do software por meio de uma função de diferença (SUB) entre imagens. Quanto mais escuro a região, mais similares são as imagens comparadas. Portanto, é perceptível que regiões como o cabeçalho e rodapé, os quais não são alvo de alterações pelo algoritmo, permanecem idênticos, enquanto as regiões centrais da imagem apresentam áreas acinzentadas, denotando possíveis diferenças.

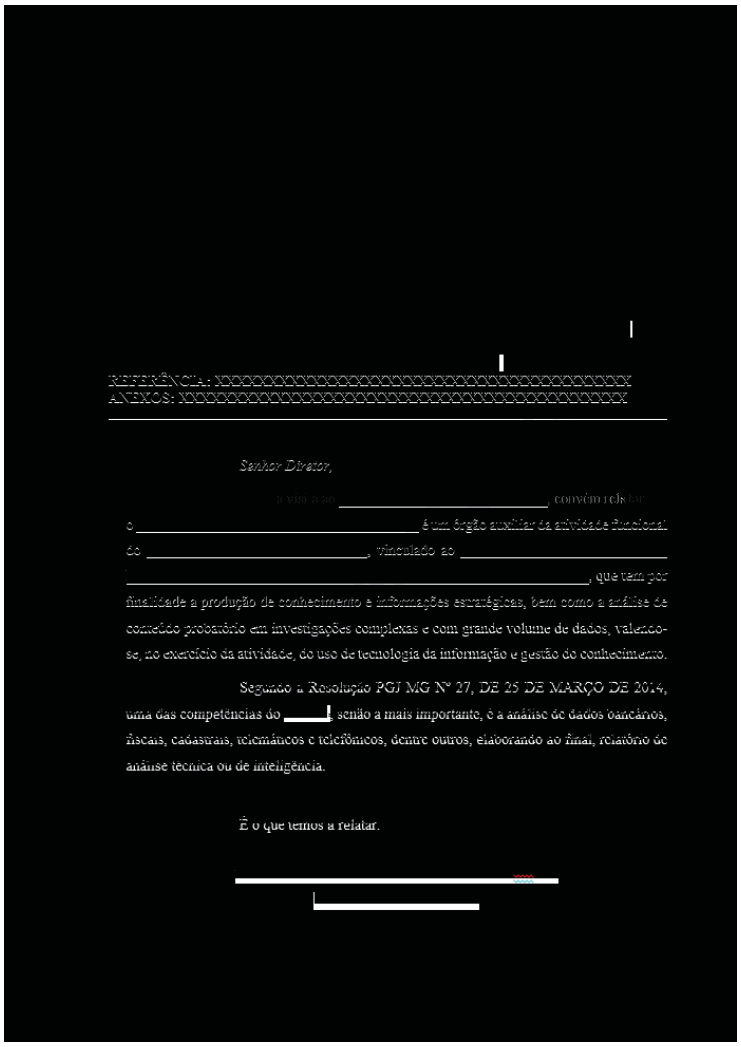


Figura 7.5 - Resultado da função SUB do software ImageJ. As áreas escuras inferem que são regiões idênticas entre as duas imagens comparadas, enquanto as áreas de cores cinza demonstram diferenças entre as imagens.

A fonte utilizada para substituir os caracteres foi a fonte textual *Calandea*. Como existem caracteres com formas diferentes nos dois textos, *pixels* próximo a esses caracteres têm suas componentes de cores RGB sutilmente alterados, o que só é possível perceber ao se aumentar a imagens. Como a função SUB verifica a diferença de valores entre cada *pixel* da imagem, essas pequenas variações são destacadas pelo software.

8. CONCLUSÕES

Neste Capítulo são apresentadas as conclusões da pesquisa. A Seção 8.1 apresenta as principais contribuições, enquanto que na Seção 8.2 são apresentadas as considerações finais. Por fim, são relacionados trabalhos futuros, que seguem na Seção 8.3.

8.1. PRINCIPAIS CONTRIBUIÇÕES

A pesquisa proporcionou a aplicação de mecanismos de *watermarking* em documentos utilizados em investigações policiais e processos judiciais, abordagem desconhecida a documentos deste contexto. Essa abordagem contribui para ótica da descoberta e do enfrentamento ao vazamento de informações. Além de apresentar opções para identificação de material com conteúdo adulterado e ocultação de informação.

Diferentes cenários de teste foram criados para validação do método proposto, o que proporcionou análise do desempenho do método em diferentes ambientes. Além de permitir a comparação com outros métodos amplamente citados na literatura.

A validação prática do método aconteceu com utilização do mecanismo em documentos produzidos pelo Ministério Público do Mato Grosso[7], o qual fez uso da técnica em alguns documentos sigilosos produzidos pelo órgão. E futuramente a disponibilização de uma ferramenta para inserção de *watermarks*.

Com base neste trabalho, um artigo científico (Ferreira, 2015) foi submetido à ICoFCS 2015 (*The Tenth International Conference on Forensic Computer Science*), tendo sido publicado nos anais dessa conferência e apresentado no X Conferência Internacional de Perícias em Crimes Cibernéticos (ICCyber 2015).

8.2. CONSIDERAÇÕES FINAIS

A aplicação de *watermarking*, essencialmente, procura vincular uma produção documental ou arquivo de mídia a um autor. A técnica apresentada neste trabalho além de permitir a vinculação entre documento e autor, também possibilita a identificação do

[7] https://www.mpmt.mp.br/

destinatário da cópia do documento. Dentro do contexto jurídico e policial, a guarda da prova documental pode afetar diretamente a condução de um processo ou inquérito. O vazamento de informações pode comprometer todo o trabalho realizado. Entretanto, a partir do controle de cópia documental e da utilização de *watermarking*, são incluídos elementos fiscalizadores dentro do cenário descrito, o que contribuiu como instrumento de auditoria e segurança para os atores vinculados aos trâmites documentais.

Diferente de algumas técnicas de *watermarking* em documentos, a técnica proposta não precisa do documento original e nem de grandes fragmentos de texto para recuperação da *watermark*. Entretanto, a técnica ainda é vulnerável ao ataque de *re-typing*, que consiste em redigitar novamente o texto. Embora os vazamentos apresentados em veículos de comunicação prefiram apresentar os documentos em sua forma original com timbres, formatação e assinaturas do órgão emissor do documento.

Como a técnica utiliza imagens de textos para recuperação da *watermark*, é importante que o texto a ser analisado tenha qualidade em sua digitalização ou impressão compatível com a técnica apresentada. O texto submetido a processos de digitalização e impressão sequenciais influenciam a qualidade da informação e pode comprometer a eficiência da técnica. Uma alternativa para a baixa qualidade das imagens de texto seria o tratamento de imagem antes da aplicação da técnica.

Com os resultados dos testes realizados, é perceptível que processos sequenciais de digitalização e impressão introduzem ruídos nas formas dos caracteres do texto, o que em grandes proporções pode ocasionar a perda de características identificadoras de tais caracteres. Fatores como a resolução empregada em equipamentos de digitalização ou os traços identificadores escolhidos nos caracteres podem afetar o resultado.

Também baseado nos resultados dos testes, a escolha da fonte também influencia a perceptibilidade da técnica. As duas maneiras de seleção de fontes foram testadas: fontes pré-definidas em editores de texto e fontes criadas especificamente para serem utilizadas com *watermarks*.

Os testes objetivos e subjetivos apontam como tendo desempenho melhor as *watermarks* que utilizam fontes criadas especificamente para esta finalidade. Quando analisadas objetivamente através dos métodos PSNR, MSE e SSIM-index, as *watermark* que utilizam fontes customizadas apresentam desempenho melhor, isto é, a quantidade de ruído introduzido no documento final é menor, quando comparadas a *watermarks* que utilizam fontes pré-

definidas. Um fator que influencia a quantidade de ruído presente em um documento não é apenas o tamanho em bits da *watermark* utilizada, mas sim a quantidade de alterações que essa *watermark* pode gerar. Portanto, *watermarks* grandes possuem um *payload* maior, entretanto não trazem necessariamente mais ruído para o documento.

Quando analisado subjetivamente, o resultado ainda permanece favorável às *watermarks* com fontes customizadas. Nos testes realizadas houve uma concentração maior de entrevistados que apontam alto grau de similaridade para fontes personalizadas. Para fontes pré-definidas há uma distribuição mais homogênea entre entrevistados que encontram similaridades e os que encontram divergências.

8.3. TRABALHOS FUTUROS

A próxima etapa do trabalho será incluir a extração automatizada da *watermark* através de reconhecimento textual, como OCR, e estudar alternativas para que a técnica suporte ataques de *re-typing*, criando *watermarks* relacionadas a aspectos sintáticos ou semânticos dos documentos. As variações de degradação dos caracteres com introdução de ruídos durante o processo de digitalização precisa ser mensurado, a fim de estipular um limite de qualidade do documento para ser submetido a um OCR ou mesmo ser passível de uma extração manual da *watermark* por meio da leitura do texto.

O estudo de caso também continuará sendo acompanhado para avaliar o grau de satisfação do usuário ou caso haja um caso de vazamento de documentos, validar a recuperação da *watermark* em um caso real, e por consequência traçar a rastreabilidade do documento "vazado" até sua guarda/destinatário. Em paralelo, será realizada a introdução da técnica em outros ambientes que possuem documentos sigilosos.

REFERÊNCIAS BIBLIOGRÁFICAS

SKODOWSKI, T. PF abre inquérito para investigar vazamento de delação de Cerveró, 2015. Disponível em:<http://oglobo.globo.com/brasil/pf-abre-inquerito-para-investigar-vazamento-de-delacao-de-cervero-18160237>. Acesso em: 20 de Set. 2016.

OLIVEIRA, M. Teori abre inquérito sobre vazamento de delação da Carioca Engenharia, 2016. Disponível em:< http:// http://g1.globo.com/politica/operacao-lava-jato/noticia/2016/03/teori-abre-inquerito-sobre-vazamento-de-delacao-da-carioca-engenharia.html>. Acesso em: 20 de Set. 2016.

AHMADI, S. B. B. (2014). Digital Image Watermarking For Intellectual Property Protection. 4th International Scientific Conference of Iranian Academics in Turkey, Ankara.

KATARIYA, S. S. (2012). Digital Watermarking: Review. International Journal of Engineering and Innovative Technology - IJEIT. Volume 1, Issue 2.

CHEN, Q. & Zhang, Y. (2010). A Novel Robust Text Watermarking For Word Document. 3º Internacional Congress on Image and Signal Processing.

COX, I. J., Miller, M. L. et al (2008). Digital Watermarking and Steganography – 2º Edição. Ed. Elsevier.

TAO, H. et al (2014). Robust Image Watermarking Theories and Techniques: A Review. Journal of Applied Research and Technology. Vol. 12(1).

WOO, C. S. (2007). Digital Image Watermarking Methods for Copyright Protection and Authentication. Thesis submitted in accordance with the regulations for Degree of Doctor of Philosophy, Queensland University of Technology.

KASHYAP, R. & MAHAJAN, K. (2014). Embedding Useful Information in Digital Watermarking: A Review. Ruchi Kashyap Int. Journal of Engineering Research and Applications. Vol. 4, Issue 6.

ALOTAIBI, R. A & ELREFAEI, L. A. (2015). Arabic Text Watermarking: A Review. International Journal of Artificial Intelligence & Applications (IJAIA), Vol. 6, No. 4.

SONG, w., Liu, X. & Ding, R. (2012). Digital Watermarking Technique for Digital Medical Images. International Symposium on Information Technology in Medicine and Education - IEEE.

BERGHEL, H. (1997). Watermarking Cyberspace. Communications of the ACM. Volume 40, No 11.

MOHANTY, S. P. (1999). Digital Watermarking: A Tutorial Review. Indian Institute of Science – Bangalore.

POPA, R. (1998). NA ANALYSIS OF STEGANOGRAPHIC TECHNIQUES. THE POLITEHNICA UNIVERSITY OF TIMISOARA.

ATALLAH, M. J. ET AL. (2001). NATURAL LANGUAGE WATERMARKING: DESIGN, ANALYSIS, AND A PROOF-OF-CONCEPT IMPLEMENTATION. PROCEEDINGS OF THE FOURTH INFORMATION HIDING WORKSHOP - PITTSBURGH.

TOPKARA, U., TOPKARA M. & ATALLAH, M. J. (2006). THE HIDING VIRTUES OF AMBIGUITY: QUANTIFIABLY RESILIENT WATERMARKING OF NATURAL LANGUAGE TEXT THROUGH SYNONYM SUBSTITUTIONS. PROCEEDINGS OF THE 8TH WORKSHOP ON MULTIMEDIA AND SECURITY. PAGES 164-174.

JALIL, Z. & MIRZA, A. M. (2009). A REVIEW OF DIGITAL WATERMARKING TECHNIQUES FOR TEXT DOCUMENTS. INTERNATIONAL CONFERENCE ON INFORMATION AND MULTIMEDIA TECHNOLOGY.

BRASSIL, S. LOW E ET AL. (1995). HIDING INFORMATION IN DOCUMENT IMAGES. PROCEEDINGS OF THE 29TH ANNUAL CONFERENCE ON INFORMATION SCIENCES AND SYSTEMS, JOHNS HOPKINS UNIVERSITY.

BRASSIL, J. T., LOW, S. & MAXEMCHUK, N. F. (1999). COPYRIGHT PROTECTION FOR THE ELECTRONIC DISTRIBUTION OF TEXT DOCUMENT. PROCEEDINGS OF THE IEEE, VOL. 87, NO. 7. DINGS OF ACM MULTIMEDIA AND SECURITY CONFERENCE, GENEVA.

SUN, X. & ASIIMWE, A. J. (2005). NOUN-VERB BASED TECHNIQUE OF TEXT WATERMARKING USING RECURSIVE DECENT SEMANTIC NET PARSERS. LECTURE NOTES IN COMPUTER SCIENCE, SPRINGER PRESS.

DEVIDAS, P. B. & NAMDEO, P. N. (2012). TEXT WATERMARKING ALGORITHM USING STRUCTURAL APPROACH. WORLD CONGRESS ON INFORMATION AND COMMUNICATION TECHNOLOGIES – IEEE.

ALMOHAMMAD, A. & GHINEA, G. (2010). STEGO IMAGE QUALITY AND THE RELIABILITY OF PSNR. IMAGE PROCESSING THEORY, TOOLS AND APPLICATIONS, 2ND INTERNATIONAL CONFERENCE ON (PP. 215-220). IEEE.

KAUR, S. (2013). A ZERO-WATERMARKING ALGORITHM ON MULTIPLE OCCURRENCES OF LETTERS FOR TEXT TAMPERING DETECTION. INTERNACIONAL JOURNAL ON COOMPUTER SCIENCE AND ENGINEERING.

CHEN, Q., ZHANG, Y. ET AL. (2011). WORD TEXT WATERMARKING FOR IP PROTECTION AND TAMPER LOCALIZATION. ARTIFICIAL INTELLIGENCE, MANAGEMENT SCIENCE AND ELECTRONIC COMMERCE - AIMSEC, IEEE.

LU, H. ET AL. (2009). A NEW CHINESE TEXT DIGITAL WATERMARKING FOR COPYRIGHT PROTECTING WORD DOCUMENT. INTERNATIONAL CONFERENCE ON COMMUNICATION AND MOBILE COMPUTING.

MIR, N. (2014). COPYRIGHT FOR WEB CONTENT USING INVISIBLE TEXT WATERMARKING. COMPUTERS IN HUMAN BEHAVIOR 30, P. 648-653.

HUANG, D. & YAN, H. (2001). INTERWORD DISTANCE CHANGES REPRESENTED BY SINE WAVES FOR WATERMARKING TEXT IMAGES. IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS FOR VIDEO TECHNOLOGY, VOL. 11, NO. 12.

VARNA, A. L., RANE, S. & VETRO, A. (2009). DATA HIDING IN HARD-COPY TEXT DOCUMENTS ROBUST TO PRINT, SCAN AND PHOTOCOPY OPERATIONS. ACOUSTICS, SPEECH AND SIGNAL PROCESSING – ICASSP, IEEE.

KIM, Y. H. & MAYER, J. (2007). DATA HIDING FOR BINARY DOCUMENTS ROBUST TO PRINT-SCAN, PHOTOCOPY AND GEOMETRIC DISTORTIONS. COMPUTER GRAPHICS AND IMAGE PROCESSING - SIBGRAPI.

KHAN, S., ET. AL. (2015). POLISH TEXT STEGANOGRAPHY METHOD USING LETTER POINTS AND EXTENSION. ELECTRICAL, COMPUTER AND COMMUNICATION TECHNOLOGIES – ICECCT, IEEE.

SHIRALI-SHAHREZA, M. H & SHIRALI-SHAHREZA, M. (2006). A NEW APPROACH TO PERSIAN/ARABIC TEXT STEGANOGRAPHY, 5TH IEEEIACIS INTERNATIONAL COTIFERENCE ON COMPUTER AND ITIFORMATION SCIENCE (ICISCOMSAR 06), PP. 310- 315.

GONZALEZ, R. C & WOODS, R. E. (2010). PROCESSAMENTO DIGITAL DE IMAGENS - 3ª EDIÇÃO, ED. PEARSON PRENTICE HALL, SÃO PAULO.

PANAH, A. S. ET AL. (2016). ON THE PROPERTIES OF NON-MEDIA DIGITAL WATERMARKING: A REVIEW OF STATE OF THE ART TECHNIQUES. SPECIAL SECTION ON LATEST ADVANCES AND EMERGING APPLICATIONS OF DATA HIDING – IEEE ACCESS.

SUBHEDAR, M. S. & MANKAR, V. H. (2013). PERFORMANCE EVALUATION OF IMAGE STEGANOGRAPHY BASED ON COVER SELECTION AND CONTOURLET TRANSFORM. INTERNATIONAL CONFERENCE ON CLOUD AND UBIQUITOUS COMPUTING AND EMERGING TECHNOLOGIES – IEEE.

VOLOSHYNOVSKIY, S. ET. AL. (2001). ATTACKS ON DIGITAL WATERMARKS: CLASSIFICATION, ESTIMATION-BASED ATTACKS AND BENCHMARKS. IEEE COMMUNICATIONS MAGAZINE.

WANG, Z. & BOVIK, A. C. (2009). MEAN SQUARED ERROR: LOVE IT OR LEAVE IT: A NEW LOOK AT SIGNAL FIDELITY MEASURES. IEEE SIGNAL PROCESSING MAGAZINE, JANUARY.

CHEEMA, P. K & KAUR, K. (2014). COMPARISON OF TEXT WATERMARKING APPROACHES WITH THE PROPOSED APPROACH BASED ON ENCRYPTION TECHNIQUES USED FOR CREATING WATERMARKS. INTERNATIONAL JOURNAL OF ADVANCED RESEARCH IN COMPUTER AND COMMUNICATION ENGINEERING, VOL. 3, ISSUE 7, JULY.

STALLINGS, W. (2005). CRYPTOGRAPHY AND NETWORK SECURITY PRINCIPLES AND PRACTICES – 4ª EDIÇÃO. ED. PRENTICE HALL.

ZIM, H. S. (1948). CODES AND SECRET WRITING (ABRIDGED EDITION) – 4 ª EDIÇÃO. ED. SCHOLASTIC BOOK SERVICES, 115 P.

VICKI, V. (2009). CRIPTOGRAFIA NUMABOA – FREQUÊNCIA DE OCORRÊNCIA DE LETRAS NO

PORTUGUÊS. DISPONÍVEL EM: <HTTP://WWW.NUMABOA.COM/CRIPTOGRAFIA/CRIPTOANALISE/310-FREQUENCIA-NO-PORTUGUES>. ACESSO EM: 28 DE MAR. DE 2016.

PRATT, F. (1942). SECRET AND URGENT: THE STORY OF CODES AND CIPHERS. ED. BLUE RIBBON BOOKS, PP.254-5.

PEREC, G. (1976). ALPHABETS. ED. ÉDITIONS GALILÉE.

BEUTELSPACHER, A. (2005). KRYPTOLOGIE - 7ª EDIÇÃO. ED. WIESBADEN.

LINN, J. PRIVACY ENHANCEMENT FOR INTERNET ELECTRONIC MAIL. REQUEST FOR COMMENTS – 989, 1987.

GONZALEZ, R. C. & WOODS, R. E. (2010). PROCESSAMENTO DIGITAL DE IMAGENS – 3ª ED. EDITORA PEARSON.

DAVARZANI, R. & YAGHMAIE, K. (2009). FARSI TEXT WATERMARKING BASED ON CHARACTER CODING. INTERNATIONAL CONFERENCE ON SIGNAL PROCESSING SYSTEMS – IEEE.

GITHUB. (2016). TESSERACT-OCR. DISPONÍVEL EM: <HTTPS://GITHUB.COM/TESSERACT-OCR>. ACESSO EM: 17 DE FEV. DE 2016.

WANG, Z., SHEIKH, H. R. & BOVIK, A. C. (2003). OBJECTIVE VIDEO QUALITY ASSESSMENT. THE HANDBOOK OF VIDEO DATABASES: DESIGN AND APPLICATIONS. ED. CRC PRESS, PP. 1041-1078.

SIMONE, F. ET AL (2009). SUBJECTIVE EVALUATION OF JPEG XR IMAGE COMPRESSION. APPLICATIONS OF DIGITAL IMAGE PROCESSING XXXII, SAN DIEGO, CA, USA.

FERREIRA, F. P. (2015). PROTEÇÃO DA PROVA DOCUMENTAL IMPRESSA E DIGITALIZADA COM A UTILIZAÇÃO DE WATERMARKING. THE NINTH INTERNATIONAL CONFERENCE ON FORENSIC COMPUTER SCIENCE.