

JAQUELINE FERREIRA DA SILVA

INSERÇÃO E EXTRAÇÃO DE MARCA D'ÁGUA EM IMAGENS DIGITAIS USANDO A
TRANSFORMADA WAVELET

Ilha Solteira
2014

JAQUELINE FERREIRA DA SILVA

INSERÇÃO E EXTRAÇÃO DE MARCA D'ÁGUA EM IMAGENS DIGITAIS USANDO A
TRANSFORMADA WAVELET

Tese apresentada à Faculdade de Engenharia do Campus de Ilha Solteira – UNESP como parte dos requisitos para obtenção do título de Doutora em Engenharia Elétrica. Especialidade: Automação.

Prof. Dr. Francisco Villarreal Alvarado
Orientador

Prof. Dr. Marco Aparecido Queiroz Duarte
Coorientador

Ilha Solteira
2014

FICHA CATALOGRÁFICA

Desenvolvido pelo Serviço Técnico de Biblioteca e Documentação

- S586i Silva, Jaqueline Ferreira.
Inserção e extração de marca d'água em imagens digitais usando a transformada wavelet / Jaqueline Ferreira Silva. -- Ilha Solteira: [s.n.], 2014
140 f. : il.
- Tese (doutorado) - Universidade Estadual Paulista. Faculdade de Engenharia de Ilha Solteira. Área de conhecimento: Automação, 2014
- Orientador: Francisco Villarreal Alvarado
Co-orientador: Marco Aparecido Queiroz Duarte
Inclui bibliografia
1. Processamento de imagens. 2. Transformada wavelet. 3. Marca d'Água digital.



UNIVERSIDADE ESTADUAL PAULISTA
CAMPUS DE ILHA SOLTEIRA
FACULDADE DE ENGENHARIA DE ILHA SOLTEIRA

CERTIFICADO DE APROVAÇÃO

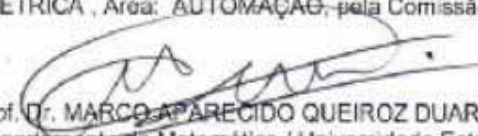
TÍTULO: Inserção e extração de marca d'água em imagens digitais usando a transformada wavelet

AUTORA: JAQUELINE FERREIRA DA SILVA

ORIENTADOR: Prof. Dr. FRANCISCO VILLARREAL ALVARADO

CO-ORIENTADOR: Prof. Dr. MARCO APARECIDO QUEIROZ DUARTE

Aprovada como parte das exigências para obtenção do Título de DOUTOR EM ENGENHARIA ELÉTRICA, Área: AUTOMAÇÃO, pela Comissão Examinadora:



Prof. Dr. MARCO APARECIDO QUEIROZ DUARTE

Departamento de Matemática / Universidade Estadual de Mato Grosso do Sul



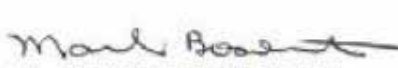
Prof. Dr. CARLOS ROBERTO MINUSSI

Departamento de Engenharia Elétrica / Faculdade de Engenharia de Ilha Solteira



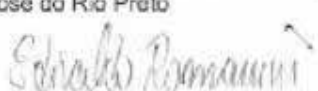
Prof. Dr. AILTON AKIRA SHINODA

Departamento de Engenharia Elétrica / Faculdade de Engenharia de Ilha Solteira



Prof. Dr. MAURILIO BOAVENTURA

Departamento de Matemática Aplicada / Instituto de Biociências, Letras e Ciências Exatas de São José do Rio Preto



Prof. Dr. EDIVALDO ROMANINI

Departamento de Ciências Exatas / Universidade Federal de Mato Grosso do Sul

Data da realização: 21 de fevereiro de 2014.

DEDICATÓRIA

Aos meus pais.

Ao meu filho Luiz Lorenzo, que desde o primeiro momento em que soube que crescias dentro de mim foi o meu sustento, para propor um novo mundo de possibilidades.

AGRADECIMENTOS

Em primeiro lugar a Deus que iluminou o meu caminho durante esta caminhada e permitiu que mais um sonho se realizasse.

Ao meu professor orientado Dr. Francisco Villarreal Alvarado, pela orientação, incentivo e paciência e principalmente por acreditar no desenvolvimento deste trabalho.

Ao professor, Dr. Marco Aparecido Queiroz Duarte, por ter me incentivado desde a graduação a seguir a vida acadêmica. Por não ter desistido de compartilhar seus conhecimentos no desenvolvimento deste trabalho e por ter sido além de um educador e coorientador, um amigo, entendendo e tendo paciência em todos os meus momentos de fraqueza, nunca deixando faltar uma palavra amiga dizendo que eu conseguiria chegar ao final de mais um objetivo. Por ter ajudado a me levantar, mostrando-me o caminho nas horas mais difíceis.

Aos meus pais, pelo carinho e dedicação, que sempre fizeram o possível para que eu chegasse até aqui.

Aos meus familiares, em especial a tia Judite e o tio Vagner, que no início desta jornada muitas vezes se privaram de várias coisas para que eu pudesse dar continuidade aos estudos.

Aos meus professores de graduação do curso de Matemática da UEMS de Cassilândia e aos professores do curso de Pós Graduação em Engenharia Elétrica – DEE, que compartilharam seus conhecimentos no decorrer do curso.

Aos amigos que torceram e me acompanharam, demonstrando companheirismo, Alex, Ana Claudia, Cássio Fernando, Jackeline, Tatiana e Viviane e ao demais, que de forma direta ou indireta me ajudaram.

Aos colegas de trabalho pelo convívio, incentivo, apoio, compreensão e pela amizade.

Aos alunos que me ensinaram mais do que pude ensina-los.

“Determine que algo pode e deve ser feito, e então você achará o caminho para fazê-lo”

Abraham Lincoln

RESUMO

O crescente uso de arquivos digitais, que circulam nos meios de comunicação, leva o usuário a recorrer a técnicas de segurança contra manipulações indevidas. A marca d'água é considerada uma informação adicional que pode garantir a segurança, além de detectar e localizar alterações numa imagem marcada de acordo com o algoritmo criptográfico empregado. Em geral, sinais digitais como imagens são arquivos vulneráveis a manipulações maliciosas devido ao meio em que circulam. A manutenção da integridade e autenticidade de uma imagem pode ser obtida através de marcas d'água digitais. Em termos criptográficos, a marca d'água inserida na imagem hospedeira deve ser a mais compacta possível e seu processamento deve ser eficaz. Após um levantamento teórico sobre a aplicação da marca d'água em imagens e, posteriormente, uma análise dos principais métodos de inserção, extração e verificação de marca d'água, embasado nos métodos que apresentaram melhores desempenhos, apresenta-se neste trabalho, um método de inserção, extração e verificação de marca d'água. O método proposto, implementado no domínio wavelet, juntamente com manipulações matriciais simples empregadas na criptografia, e tem como objetivo fornecer uma marca d'água robusta diante de vários tipos de ataques digitais. O método permite inserir a marca d'água sem prejudicar a qualidade visual da imagem hospedeira e, após os ataques, extraí-la com sucesso, apresentando correlação satisfatória entre a marca d'água inserida e a extraída. Os programas de processamento de imagens, usando Transformada Wavelet e dos métodos de inserção, extração e verificação, foram desenvolvidos no ambiente do MATLAB[®]. Para a verificação da eficiência do método proposto, foram realizados experimentos em três imagens diferentes e duas marcas de dimensões diferentes.

Palavras-chave: Processamento de imagens. Transformada wavelet. Marca d'água digital.

ABSTRACT

The growing use of digital files through the media takes the user to employ security techniques against tampering attacks. The watermark is considered an additional information that can ensure security, detect and track changes in an image marked according to the cryptographic algorithm deployed. In general, digital signals such as images files are vulnerable to tampering attacks due to the way in which they circulate. Through digital watermarks, it is possible to obtain authenticity of an image. In cryptographic terms, the watermark embedded in the host image must be as compact as possible and its processing must be effective. After a theoretical survey on the implementation of the watermark images and, later, an analysis of the main methods of insertion, extraction and verification of the watermark, grounded by better performances, we present in this paper, a method of insertion, extraction and verification of the watermark. The proposed method, implemented in the wavelet domain, along with simple matrix manipulations used in cryptography aims to provide a robust watermark on various types of digital attacks. The method allows the inserting of the watermark without affecting the visual quality of the host image and after the attacks, extract it successfully, presenting a correlation between the watermark inserted and extracted close to optimum. The image processing programs via Wavelet transformed and methods of insertion, extraction and verification were developed in the MATLAB ® environment, which makes the manipulations in the host image and the watermark easier whereas the images are read as pixel matrix. Finally, we show how the very original results shown here suggest other types of attacks and increase the robustness of the watermark.

Key-words: Images processing. Wavelet transformed. Digital watermark.

LISTA DE FIGURAS

Figura 1	Imagem da cédula de R\$ 50,00 de 256×256 pixels; (a) Marca d'água autêntica; (b) Marca d'água falsa.	27
Figura 2	Ilustração de marca d'água perceptível na imagem Cisne 256×256 pixels.	28
Figura 3	Imagem hospedeira: (a) Raio-X 256×256 pixels; (b) Lenna 256×256 pixels.	29
Figura 4	(a) Imagem Cisne 2048×2048 pixels considerada a marca d'água; (b) Raio-X 2048×2048 pixels autenticada por (a); (c) Lenna 2048×2048 pixels autenticada por (a).	30
Figura 5	(a) Cisne 32×32 pixels considerada a marca d'água; (b) Raio-X 256×256 pixels autenticada por (a); (c) Lenna 256×256 pixels autenticada por (a).	30
Figura 6	(a) Marca d'água pseudoaleatória de tamanho $n = 256$; (b) Raio X 256×256 pixels autenticada por (a); (c) Lenna 256×256 pixels autenticada por (a).	31
Figura 7	(a) Marca d'água aleatória de tamanho $n = 256$; (b) Raio-X 256×256 pixels autenticada por (a); (c) Lenna 256×256 pixels autenticada por (a).	32
Figura 8	(a) Marca d'água binária 32×32 pixels; (b) Raio-X 32×32 pixels autenticada por (a); (c) Lenna 32×32 pixels autenticada por (a).	32
Figura 9	(a) Marca d'água inserida 32×32 pixels; (b) Marca d'água extraída 32×32 pixels.	33
Figura 10	Classificação da Marca d'água.	34
Figura 11	Processo de codificação e decodificação de dados.	36
Figura 12	Esquema de criptografia de uma marca d'água.	36
Figura 13	Esquema ilustrativo da criptografia simétrica.	37
Figura 14	Esquema ilustrativo da criptografia assimétrica.	39
Figura 15	Criptografia Arnold' Cat Map: (a) Nível 1; (b) Nível 2; (c) Nível 96; (d) Nível 187; (e) Nível 191; (f) Nível 192.	41
Figura 16	(a) Imagem original; (b) Matriz que representa a intensidade dos pixels da imagem.	42
Figura 17	Cisalhamento na direção x.	43
Figura 18	Resultado do cisalhamento na direção y.	43
Figura 19	Resultado do cisalhamento na direção x e y.	43
Figura 20	Representação esquemática da resultante do primeiro passo do algoritmo Arnold's Cat Map.	45
Figura 21	Representação esquemática da resultante do segundo passo do algoritmo	45

	Arnold's Cat Map aplicado uma vez.	
Figura 22	Esquema da geração de assinatura digital.	47
Figura 23	Esquema para verificar assinatura digital.	47
Figura 24	Inserção de vários tipos de marca d'água em um único documento; (a) Imagem hospedeira Lenna; (b) Marca d'água aleatória; (c) marca d'água pseudoaleatória; (d) Marca d'água binária; (e) Marca d'água imagem; (f) Imagem marcada com (a), (b), (c), (d) e (e).	55
Figura 25	Inserção de vários tipos de marca d'água com a mesma característica em um único documento; (a) Imagem hospedeira Lenna; (b) Marca d'água Cisne; (c) Marca d'água Cass; (d) Imagem marcada com (b) e (c).	56
Figura 26	Representação esquemática do sistema de inserção de marca d'água.	57
Figura 27	(a) Imagem original 64×64 pixels; (b) Imagem dividida em 64 blocos de dimensão 8×8 pixels.	59
Figura 28	(a) Marca d'água 32×32 pixels; (b) Marca d'água replicada; (c) Imagem hospedeira representada por 64 blocos marcados por (b).	60
Figura 29	(a) Ataque de rotação; (b) Ataque de recorte; (c) Ataque de filtro; (d) Ataque de ruído.	63
Figura 30	(a) Imagem hospedeira Lenna 256×256 pixels; (b) Marca d'água 32×32 pixels replicada; (c) Imagem marcada pelo método Wong.	66
Figura 31	Ataque a um banco de dados.	67
Figura 32	Reconstrução da marca d'água.	67
Figura 33	(a) Marca d'água 32×32 pixels reconstruída; (b) Imagem marcada.	68
Figura 34	Comparação dos blocos das imagens.	68
Figura 35	Representação esquemática da estrutura do banco de filtros da DWT.	73
Figura 36	Representação esquemática dos estágios de decomposição wavelet bidimensional padrão de uma imagem.	74
Figura 37	Representação esquemática dos estágios de decomposição wavelet bidimensional não-padrão de uma imagem.	74
Figura 38	Representação esquemática dos estágios de decomposição wavelet bidimensional não-padrão em dois níveis de resolução.	75
Figura 39	Hierarquia de sub-bandas de frequência de uma imagem decomposta pela DWT bidimensional até o nível 2.	76
Figura 40	Inserção de marca d'água numa imagem no domínio wavelet.	77
Figura 41	Extração de marca d'água numa imagem no domínio wavelet.	78
Figura 42	Método de inserção de marca d'água proposto por Cox et al. (1997) usando a	86

DWT bidimensional.

Figura 43	Método de extração de marca d'água proposto por Cox et al. (1997) usando a DWT bidimensional.	86
Figura 44	Preparação da região na imagem hospedeira para receber a marca d'água proposto pelo método Sanghyn et al. (2002).	87
Figura 45	Inserção da marca d'água proposto por Sanghyn et al. (2002).	88
Figura 46	Inserção de marca d'água proposta por Hajjara, Abdallah e Hudaib (2009).	89
Figura 47	Extração da marca d'água proposta por Hajjara, Abdallah e Hudaib (2009).	90
Figura 48	(a) Imagem hospedeira 256×256 pixels; (b) Marca d'água pseudoaleatória; (c) Marca d'água aleatória; (d) Marca d'água binária 8×8 pixels.	91
Figura 49	(a) Imagem marcada pelo método de Cox et al. (1997); (b) Marca d'água inserida; (c) Marca d'água extraída.	92
Figura 50	(a) Imagem marcada pelo método de Sanghyn et al. (2002); (b) Marca d'água inserida; (c) Marca d'água extraída.	92
Figura 51	(a) Imagem marcada pelo método de Hajjara, Abdallah e Hudaib (2009); (b) Marcas d'água inseridas; (c) Marca d'água extraída.	92
Figura 52	Preparação da região hospedeira da marca d'água.	96
Figura 53	(a) Marca d'água binária; (b) Sub-banda de frequência da marca d'água; (c) Blocos correspondentes as sub-bandas de frequência.	98
Figura 54	Criptografia usando o algoritmo ACM.	99
Figura 55	Troca de posições dos elementos simétricos em relação à diagonal secundária em um bloco.	99
Figura 56	Troca de posições dos elementos simétricos em relação à diagonal secundária nos blocos criptografados pelo algoritmo ACM: (a) Blocos B1_crip, B2_crip, B3_crip e B4_crip; (b) Blocos B1_crip_diag, B2_crip_diag, B3_crip_diag e B4_crip_diag.	100
Figura 57	Inserção aleatória dos blocos nos quatro cantos da sub-banda HL_2 .	100
Figura 58	Finalização da etapa de inserção da marca d'água.	101
Figura 59	Representação esquemática da extração da região onde a marca d'água foi inserida.	102
Figura 60	Preparação da marca d'água inserida.	102
Figura 61	Representação esquemática da extração dos blocos.	103
Figura 62	Representação esquemática da troca de posições dos elementos simétricos em relação à diagonal secundária: (a) Quatro regiões organizadas após a troca dos elementos simétricos com relação à diagonal secundária no processo de criptografia; (b) Quatro regiões organizadas no processo inverso da troca dos	103

elementos simétricos com relação à diagonal secundária no processo de criptografia.

Figura 63	Representação esquemática do passo 5.	104
Figura 64	Representação esquemática do cálculo da correlação.	105
Figura 65	Representação esquemática do resultado do passo 7.	105
Figura 66	Imagens: (a) Cass 2048×2048 pixels; (b) Lenna 2048×2048 pixels; (c) Cisne 2048×2048 pixels.	107
Figura 67	(a) Marca d'água 32×32 pixels; (b) Marca d'água 16×16 pixels.	108
Figura 68	(a) Imagem original Cass 2048×2048 pixels; (b) Imagem marcada com a marca d'água 32×32 pixels e (c) Imagem marcada com a marca d'água 16×16 pixels.	109
Figura 69	Marcas d'água 32×32 pixels extraídas da imagem Cass 2048×2048 pixels, após ataque de compressão com TC de: (a) 30%; (b) 40% e (c) 50%.	109
Figura 70	Marcas d'água 32×32 pixels extraídas da imagem Cass 2048×2048 pixels após ataque ruidoso seguido de compressão com TC de: (a) 30%; (b) 40% e (c) 50%.	109
Figura 71	Marcas d'água 32×32 pixels extraídas da imagem Cass 2048×2048 pixels após ataque de compressão JPEG (a) 30% e (b) Marca d'água extraída após inserção proposta pelo método Hajjara, Abdallah e Hudaib (2009) 30%.	109
Figura 72	Marcas d'água 16×16 pixels, extraídas da imagem Cass 2048×2048 pixels, após ataque de compressão com TC de: (a) 30%; (b) 40% e (c) 50%.	110
Figura 73	Marcas d'água 16×16 pixels, extraídas da imagem Cass 2048×2048 pixels após ataque ruidoso seguido de compressão com TC de: (a) 30%; (b) 40% e (c) 50%.	110
Figura 74	Marcas d'água 16×16 pixels, extraídas da imagem Cass 2048×2048 pixels após ataque de compressão JPEG (a) 30% e (b) Marca d'água extraída após inserção proposta pelo método Hajjara, Abdallah e Hudaib (2009) 30%.	110
Figura 75	(a) Imagem original Cass 1024×1024 pixels; (b) Imagem (a) marcada com a marca d'água 32×32 pixels e (c) Imagem (a) marcada com a marca d'água 16×16 pixels.	113
Figura 76	Marcas d'água 32×32 pixels, extraídas da imagem Cass 1024×1024 pixels, após ataque de compressão com TC de: (a) 30%; (b) 40% e (c) 50%.	113
Figura 77	Marcas d'água 32×32 pixels, extraídas da imagem Cass 1024×1024 pixels, após ataque ruidoso seguido de compressão com TC de: (a) 30%; (b) 40% e (c) 50%.	113
Figura 78	Marcas d'água 32×32 pixels, extraídas da imagem Cass 1024×1024 pixels, após ataque de: compressão JPEG (a) 30% e (b) após inserção proposta pelo método Hajjara, Abdallah e Hudaib (2009) 30%.	114

Figura 79	Marcas d'água 16×16 pixels, extraídas da imagem Cass 1024×1024 pixels, após ataque de compressão com TC de: (a) 30%; (b) 40% e (c) 50%.	114
Figura 80	Marcas d'água 16×16 pixels, extraídas da imagem Cass 1024×1024 pixels, após ataque ruidoso seguido de compressão com TC de: (a) 30%; (b) 40% e (c) 50%.	114
Figura 81	Marcas d'água 16×16 pixels, extraídas da imagem Cass 1024×1024 pixels, após ataque de compressão JPEG (a) 30% e (b) após inserção proposta pelo método Hajjara, Abdallah e Hudaib (2009) 30%.	114
Figura 82	(a) Imagem original Lenna 2048×2048 pixels; (b) Imagem (a) marcada com marca d'água 32×32 pixels e (c) Imagem (a) marcada com marca d'água 16×16 pixels.	117
Figura 83	Marcas d'água 32×32 pixels, extraídas da imagem Lenna 2048×2048 pixels, após ataque de compressão com TC de: (a) 30%; (b) 40% e (c) 50%.	117
Figura 84	Marcas d'água 32×32 pixels, extraídas da imagem Lenna 2048×2048 pixels, após ataque ruidoso seguido de compressão com TC de: (a) 30%; (b) 40% e (c) 50%.	117
Figura 85	Marcas d'água 32×32 pixels, extraídas da imagem Lenna 2048×2048 pixels, após ataque de compressão JPEG (a) 30% e(b) após inserção proposta pelo método Hajjara, Abdallah e Hudaib (2009) 30%.	118
Figura 86	Marcas d'água 16×16 pixels, extraídas da imagem Lenna 2048×2048 pixels, após ataque de compressão com TC de: (a) 30%; (b) 40% e (c) 50%.	118
Figura 87	Marcas d'água 16×16 pixels, extraídas da imagem Lenna 2048×2048 pixels, após ataque ruidoso seguido de compressão com TC de: (a) 30%; (b) 40% e (c) 50%.	118
Figura 88	Marcas d'água 16×16 pixels, extraídas da imagem Lenna 2048×2048 pixels, após ataque de compressão JPEG (a) 30% e(b) após inserção proposta pelo método Hajjara, Abdallah e Hudaib (2009) 30%.	118
Figura 89	(a) Imagem original 1024×1024 pixels; (b) Imagem (a) marcada com marca d'água 32×32 pixels e (c) Imagem (a) marcada com marca d'água 16×16 pixels.	121
Figura 90	Marcas d'água 32×32 pixels, extraídas da imagem Lenna 1024×1024 pixels, após ataque de compressão com TC de: (a) 30%; (b) 40% e (c) 50%.	121
Figura 91	Marcas d'água 32×32 pixels, extraídas da imagem Lenna 1024×1024 pixels, após ataque ruidoso seguido de compressão com TC de: (a) 30%; (b) 40% e (c) 50%.	121
Figura 92	Marcas d'água 32×32 pixels, extraídas da imagem Lenna 1024×1024 pixels, após ataque de compressão JPEG (a) 30% e(b) após inserção proposta pelo método Hajjara, Abdallah e Hudaib (2009) 30%.	122
Figura 93	Marcas d'água 16×16 pixels, extraídas da imagem Lenna 1024×1024 pixels, após ataque de compressão com TC de: (a) 30%; (b) 40% e (c) 50%.	122

Figura 94	Marcas d'água 16×16 pixels, extraídas da imagem Lenna 1024×1024 pixels, após ataque ruidoso seguido de compressão com TC de: (a) 30%; (b) 40% e (c) 50%.	122
Figura 95	Marcas d'água 16×16 pixels, extraídas da imagem Lenna 1024×1024 pixels, após ataque de compressão JPEG (a) 30% e(b) após inserção proposta pelo método Hajjara, Abdallah e Hudaib (2009) 30%.	123
Figura 96	(a) Imagem original Cisne 2048×2048 pixels; (b) Imagem marcada com a marca d'água 32×32 pixels e (c) Imagem marcada com a marca d'água 16×16 pixels.	125
Figura 97	Marcas d'água 32×32 pixels, extraídas da imagem Cisne 2048×2048 pixels, após ataque de compressão com TC de: (a) 30%; (b) 40% e (c) 50%.	125
Figura 98	Marcas d'água 32×32 pixels, extraídas da imagem Cisne 2048×2048 pixels, após ataque ruidoso seguido de compressão com TC de: (a) 30%; (b) 40% e (c) 50%.	126
Figura 99	Marcas d'água 32×32 pixels, extraídas da imagem Lenna Cisne 2048×2048 pixels, após ataque de compressão JPEG (a) 30% e(b) após inserção proposta pelo método Hajjara, Abdallah e Hudaib (2009) 30%.	126
Figura 100	Marcas d'água 16×16 pixels, extraídas da imagem Cisne 2048×2048 pixels, após ataque de compressão com TC de: (a) 30%; (b) 40% e (c) 50%.	126
Figura 101	Marcas d'água 16×16 pixels, extraídas da imagem Cisne 2048×2048 pixels, após ataque ruidoso seguido de compressão com TC de: (a) 30%; (b) 40% e (c) 50%.	126
Figura 102	Marcas d'água 16×16 pixels, extraídas da imagem Lenna Cisne 2048×2048 pixels, após ataque de compressão JPEG (a) 30% e(b) após inserção proposta pelo método Hajjara, Abdallah e Hudaib (2009) 30%.	127
Figura 103	(a) Imagem original Cisne 1024×1024 pixels; (b) Imagem marcada com a marca d'água 32×32 pixels e (c) Imagem marcada com a marca d'água 16×16 pixels.	129
Figura 104	Marcas d'água 32×32 pixels, extraídas da imagem Cisne 1024×1024 após ataque de compressão com TC de: (a) 30%; (b) 40% e (c) 50%.	129
Figura 105	Marcas d'água 32×32 pixels, extraídas da imagem Cisne 1024×1024 pixels, após ataque ruidoso seguido de compressão com TC de: (a) 30%; (b) 40% e (c) 50%.	129
Figura 106	Marcas d'água 32×32 pixels, extraídas da imagem Lenna Cisne 1024×1024 pixels, após ataque de compressão JPEG (a) 30% e (b) após inserção proposta pelo método Hajjara, Abdallah e Hudaib (2009) 30%.	130
Figura 107	Marcas d'água 16×16 pixels, extraídas da imagem Cisne 1024×1024 após ataque de compressão com TC de: (a) 30%; (b) 40% e (c) 50%.	130

- Figura 108 Marcas d'água 16×16 pixels, extraídas da imagem Cisne 1024×1024 pixels, após ataque ruidoso seguido de compressão com TC de: (a) 30%; (b) 40% e (c) 50%. 130
- Figura 109 Marcas d'água 16×16 pixels, extraídas da imagem Lenna Cisne 1024×1024 pixels, após ataque de compressão JPEG (a) 30% e (b) após inserção proposta pelo método Hajjara, Abdallah e Hudaib (2009) 30%. 131

LISTA DE TABELAS

Tabela 1	Tabela <i>hash</i>	48
Tabela 2	Tabela <i>hash</i> preenchida pelos quatro primeiros elementos sem colisão.	49
Tabela 3	Tabela <i>hash</i> preenchida após a primeira colisão.	50
Tabela 4	Tabela <i>hash</i> preenchida até que apareça uma nova colisão.	50
Tabela 5	Tabela <i>hash</i> preenchida após a colisão do elementos 8.	50
Tabela 6	Tabela <i>hash</i> preenchida após a colisão do elementos 9.	51
Tabela 7	Tabela <i>hash</i> preenchida até nova colisão.	51
Tabela 8	Tabela <i>hash</i> preenchida após a colisão do elemento 11.	51
Tabela 9	Tabela <i>hash</i> preenchida após a colisão dos elementos 12.	52
Tabela 10	Tabela <i>hash</i> preenchida após as colisões dos elementos 13, 14 e 15.	52
Tabela 11	Tabela <i>hash</i> preenchida após a colisão do elemento 16.	52
Tabela 12	Tabela <i>hash</i> preenchida pelos elementos quando é percorrido as colunas da matriz A .	53
Tabela 13	Tabela <i>hash</i> preenchida pelos elementos da matriz $A_{4 \times 3}$.	54
Tabela 14	Métricas obtidas após aplicação dos métodos analisados	93
Tabela 15	Valores da PSNR e o nível de correlação após ataques de: Compressão com perda 30%; 40% e 50%; Ruidoso seguido de compressão 30%; 40% e 50%; Compressão JPEG 30% e Hajjara, Abdallah e Hudaib (2009) 30%, aplicados na imagem Cass 2048×2048 pixels.	111
Tabela 16	Valores do nível de correlação após ataque de compressão 30%; ataque ruidoso seguido de compressão 30%; ataque de compressão JPEG 30% e Hajjara, Abdallah e Hudaib (2009) 30%, aplicados na imagem Cass 2048×2048.	112
Tabela 17	Valores da PSNR e o nível de correlação após ataques de: Compressão com perda 30%; 40% e 50%; Ruidoso seguido de compressão 30%; 40% e 50%; Compressão JPEG 30% e Hajjara, Abdallah e Hudaib (2009) 30%, aplicados na imagem Cass 1024×1024 pixels.	115
Tabela 18	Valores do nível de correlação após ataque de compressão 30%; ataque ruidoso seguido de compressão 30%; ataque de compressão JPEG 30% e Hajjara, Abdallah e Hudaib (2009) 30%, aplicados na imagem Cass 1024×1024.	116
Tabela 19	Valores da PSNR e o nível de correlação após ataques de: Compressão com perda 30%, 40% e 50%; Ruidoso seguido de compressão 30%; 40% e 50%; Compressão JPEG 30% e Hajjara, Abdallah e Hudaib (2009) 30%, aplicados	119

na imagem Lenna 2048×2048 pixels.

Tabela 20	Valores médios do nível de correlação após ataque de compressão 30%; ataque ruidoso seguido de compressão 30%; ataque de compressão JPEG 30% e Hajjara, Abdallah e Hudaib (2009) 30%, aplicados na imagem Lenna 2048×2048 pixels.	120
Tabela 21	Valores da PSNR e o nível de correlação após ataques de: Compressão com perda 30%, 40% e 50%; Ruidoso seguido de compressão 30%; 40% e 50%; Compressão JPEG 30% e Hajjara, Abdallah e Hudaib (2009) 30%, aplicados na imagem Cass 1024×1024 pixels.	123
Tabela 22	Valores médios do nível de correlação após ataque de compressão 30%, ataque ruidoso seguido de compressão 30%; ataque de compressão JPEG 30% e Hajjara, Abdallah e Hudaib (2009) 30%, aplicados na imagem Lenna 1024×1024 pixels.	124
Tabela 23	Valores da PSNR e o nível de correlação após ataques de: Compressão com perda 30%, 40% e 50%; Ruidoso seguido de compressão 30%; 40% e 50%; Compressão JPEG 30% e Hajjara, Abdallah e Hudaib (2009) 30%, aplicados na imagem Cisne 2048×2048 pixels.	127
Tabela 24	Valores médios do nível de correlação após ataque de compressão 30%, ataque ruidoso seguido de compressão 30%; ataque de compressão JPEG 30% e Hajjara, Abdallah e Hudaib (2009) 30%, aplicados na imagem Cisne 2048×2048 pixels.	128
Tabela 25	Valores da PSNR e o nível de correlação após ataques de: Compressão com perda 30%, 40% e 50%; Ruidoso seguido de compressão 30%; 40% e 50%; Compressão JPEG 30% e Hajjara, Abdallah e Hudaib (2009) 30%, aplicados na imagem Cisne 1024×1024 pixels.	132
Tabela 26	Valores médios do nível de correlação após ataque de compressão 30%; ataque ruidoso seguido de compressão 30%; ataque de compressão JPEG 30% e Hajjara, Abdallah e Hudaib (2009) 30%, aplicados na imagem Cisne 1024×1024 pixels.	133

LISTA DE ABREVIATURAS

ACM	Criptografia Arnold's Cat Map
CPR	Chave Privada
dB	Decibéis
dB 6	Função Wavelet de Daubechies Nível 6
DWT	Transformada Wavelet Discreta
DWTB	Transformada Wavelet Discreta Bidimensional
GIF	Graphics Interchange Format
HVS	Sistema Visual Humano
IDWTB	Transformada Wavelet Discreta Inversa
JPEG	Joint Pictures Expert Group
kBytes	Quilobytes
kHz	Quilohertz
MATLAB [®]	Matrix Laboratory
MSE	Mean Squared Error
NC	Correlação Normalizada
PNG	Portable Network Graphics
PSNR	Peak Signal-to-Noise Ratio
PN	Sequência Pseudoaleatória
RSA	Criptografia Ronald AS
TC	Taxa de compressão

LISTA DE SÍMBOLOS

x, y	Coordenadas cartesianas
M, N	Número de linhas e colunas de uma matriz $M \times N$
L	Número máximo de níveis e faixa na decomposição wavelet
K	Número máximo de interações do algoritmo ACM
$d(x)$	Resolução horizontal
$d(y)$	Resolução vertical
$\log_2(x)$	Logaritmo de um número x na base 2
V_j	Espaço de Escala 2^j
h_g	Coeficientes de aproximação do nível j da TWD
g_g	Coeficientes de detalhe do nível j da TWD
W_j	Complemento ortogonal de V_j
$\oplus$	Soma direta de conjuntos
$h[n]$	Filtro passa-baixa
$g[n]$	Filtro passa-alta
$\lceil x \rceil$	Menor inteiro maior ou igual a x
$\lfloor x \rfloor$	Maior inteiro menor ou igual a x

SUMÁRIO

1	INTRODUÇÃO	22
1.1	Motivação	22
1.2	Objetivos	24
1.3	Metodologia	25
1.4	Estrutura do trabalho	26
2	FUNDAMENTOS BÁSICOS DE MARCA D'ÁGUA DIGITAL	27
2.1	Aplicação de marca d'água em imagens digitais	29
2.2	Classificação de marca d'água em termos de remoção	34
2.3	Marca d'água e criptografia	35
2.3.1	Criptografia simétrica	37
2.3.2	Criptografia assimétrica	39
2.4	Criptografia Cat Map	40
2.5	Assinatura digital	45
2.5.1	Função <i>hash</i>	46
3	MÉTODOS DE INSERÇÃO E EXTRAÇÃO DE MARCA D'ÁGUA	55
3.1	Métodos de inserção	56
3.2	Métodos de extração	57
3.3	Métodos de verificação	58
3.4	Algoritmo Wong	58
3.4.1	Inserção	59
3.4.2	Extração e verificação	61
3.5	Possíveis ataques aplicados em imagens autenticadas por marca d'água	62
3.5.1	Ataques visuais	64
3.5.2	Ataques estruturais	64
3.5.3	Ataques estatísticos	64
3.6	Ataques à marca d'água	65
3.6.1	Ataque recortar e colar e ataque de falsificação	65
3.6.2	Ataque ruidoso	69
3.6.3	Ataque de compressão	70
4	TRANSFORMADA WAVELET	71
4.1	Transformada Wavelet Discreta	71
4.2	Transformada Wavelet Discreta Bidimensional	73
4.2.1	Decomposição padrão	73
4.2.2	Decomposição não-padrão	74
4.3	Inserção de marca d'água no domínio wavelet	75
4.3.1	Sub-bandas de alta frequência	76
4.3.2	Sub-bandas de baixa frequência	77
4.4	Extração de marca d'água no domínio wavelet	77
5	MÉTODOS DE INSERÇÃO E EXTRAÇÃO DE MARCA D'ÁGUA EM IMAGENS NO DOMÍNIO WAVELET	79
5.1	Método Cox et al.	81
5.1.1	Algoritmo de inserção	82
5.1.2	Algoritmo de extração	83
5.2	Implementação do método de Cox et al. com a DWT bidimensional	84

5.3	Método de Sanghyn et. al. (2002).	86
5.4	Método de Hajjara, Abdallah e Hudaib (2009).	88
5.4.1	Algoritmo de inserção	88
5.4.2	Algoritmo de extração	89
5.5	Cálculo da PSNR e da Correlação Normalizada (NC)	90
5.6	Testes com os métodos analisados	91
6	METODOLOGIA PROPOSTA	94
6.1	Primeira etapa	95
6.1.1	Preparação da imagem hospedeira	96
6.1.1.1	Algoritmo de preparação	96
6.1.2	Preparação da marca d'água	97
6.2	Segunda etapa	98
6.2.1	Criptografia da marca d'água	98
6.3	Terceira etapa	100
6.3.1	Inserção da marca d'água	100
6.3.2	Aplicação da IDWT bidimensional para a reconstrução da imagem decomposta pela DWT bidimensional	101
6.4	Quarta etapa	101
6.4.1	Algoritmo de extração	102
7	TESTES E RESULTADOS	107
7.1	Experimento 1	108
7.2	Experimento 2	112
7.3	Experimento 3	116
7.4	Experimento 4	120
7.5	Experimento 5	125
7.6	Experimento 6	129
	CONSIDERAÇÕES FINAIS	134
	REFERÊNCIAS	136

1 INTRODUÇÃO

Neste capítulo é apresentada uma sucinta explanação sobre a pesquisa desenvolvida, na qual é descrita a motivação para a escolha do assunto pesquisado assim como os objetivos almejados, as técnicas que sustentam a metodologia empregada, a real contribuição da pesquisa e sua originalidade.

1.1 Motivação

O crescimento do uso da tecnologia digital, juntamente com a difusão da internet, têm originado grandes problemas envolvendo a manipulação de dados que trafegam na rede (LOPES et al., 2004), isso porque, em qualquer tipo de avanço tecnológico, surgem também os desafios que colocam à prova a segurança das técnicas empregadas, tornando a tecnologia não tão perfeita.

A internet é o canal de comunicação mais utilizado para distribuição, comercialização, armazenamento e transmissão de dados dos mais diferentes tipos, como por exemplo, textos, sons, vídeos e imagens. Oferece, ainda, recursos dos mais variados tipos de aplicações o que torna os arquivos alvos fáceis para manipulações indevidas.

Há uma infinidade de técnicas que procura assegurar a integridade dos dados digitais. Um simples exemplo é o uso de antivírus, cuja técnica tem como objetivo impedir ataques ao sistema computacional. É comum a invasão de um determinado vírus em um computador mesmo que esteja sendo empregada uma técnica de segurança, isso porque dificilmente a segurança que envolve uma técnica persista por muito tempo. Pesquisas surgem com frequência buscando melhoria no que já é empregado.

Para essa eventual melhoria, o crucial é encontrar o ponto fraco da técnica empregada. Este fator é o que proporciona vulnerabilidade aos materiais digitais que circulam no canal ao qual tal técnica é empregada, ou seja, pode-se dizer que a internet, por ser o canal de comunicação mais usado, acaba proporcionando uma insegurança à propriedade intelectual. Dentre os materiais digitais que circulam nos canais de comunicação, as imagens estão entre os tipos de arquivos mais visados por manipulações indevidas.

Essencialmente representadas em forma digital, as imagens são tipos de sinais cada vez mais presentes em nosso cotidiano, e a cada dia tem despertado a necessidade de

processamentos indispensáveis. Desde as imagens usadas para o mais simples entretenimento - como as que circulam nos meios de comunicação - até as aplicações mais importantes, que são baseadas especificamente por meio de imagens. Por exemplo, imagens biomédicas depositadas em bancos de dados encontrados em centros hospitalares (PORTILLA; SIMONCELLI, 2000).

As imagens, em especial, acabam sendo alvos de manipulações das informações nelas contidas. Essas manipulações podem ser facilmente empregadas usando *software* de domínio livre que atualmente podem ser encontrados na internet. Esses *software* são capazes de realizar mudanças que consistem em melhorar esteticamente, redimensionar, adicionar ou remover informações.

Em aplicações práticas, para fins digitais, qualquer uma dessas manipulações causa perda de informações. Uma das alternativas para conter qualquer tipo de fraude ou manipulação maliciosa é atribuída o uso de marca d'água (LOPES et al., 2004).

A marca d'água digital é uma das técnicas viáveis para coibir manipulações indevidas. De princípio, ela não surgiu especificamente para ser aplicada em imagens. Por volta de 1954, para proteger a autoria de músicas, eram inseridos códigos de identificação, baseados no Código Morse. Tais códigos foram criados com a aplicação de um filtro de 1kHz na música, sendo que a presença ou a ausência de energia nessa frequência indicava letras, semelhantes ao Código Morse, garantindo a autoria pretendida (COX; MILLER; BLOOM, 2000; COX et al., 1997).

A disseminação das técnicas de marca d'água digital em imagens se deu a partir dos anos 90 com o crescente uso de documentos digitais. As primeiras publicações científicas envolvendo marca d'água foram realizadas em 1993 (FREDERES, 2007; KATZENBEISSER; PETITCOLAS, 2000). Desde então, têm ocorrido várias situações que envolvem a necessidade de aplicação da técnica de marca d'água para garantir direitos autorais em imagens, proteção e garantia da autoria na divulgação de obras, seja ela de alto grau intelectual, científico ou subproduto da fama das celebridades.

O incentivo para o uso de marca d'água visando assegurar direitos autorais é uma questão aberta no mundo todo do ponto de vista jurídico e cultural, pois, atualmente, o acesso e a troca de informações ganharam uma abertura e uma velocidade extraordinária, colocando em contratempo os limites entre o direito público e o direito privado.

Ao disponibilizar arquivos seja pela internet, em bancos de dados, ou simples ato de divulgar um trabalho impresso, o autor está consciente de que outras pessoas utilizarão este material. Não há como separar o público que tem intenção de utilizar indevidamente as

imagens dos que não tem esse objetivo. O acesso aberto às informações acaba formando a ideia de que, nesses canais de comunicação, tudo é de todos, acarretando a perda de autoria em que o arquivo circula. Por essa razão, em muitos casos, é necessária a utilização da marca d'água, visando coibir manipulações nas informações dos materiais, garantindo, assim, os direitos autorais sobre os mesmos.

Por mais favorável que seja o uso de marca d'água, principalmente para a comprovação quando a mesma é retirada, ainda há opiniões contrárias sobre seu uso. Essas opiniões alegam que existem outras formas de proteger imagens, por exemplo, diminuindo a qualidade, o tamanho ou adicionando informações na configuração da imagem. Mas o uso de marca d'água ainda parece ser o método mais efetivo, principalmente para fins científicos que envolvem imagens com configurações e informações delicadas.

1.2 Objetivos

Os objetivos desta pesquisa são sintetizados a seguir.

- a) levantamento bibliográfico sobre os conceitos envolvendo o emprego de marca d'água em imagens digitais, desde a fundamentação de sua importância para a garantia da segurança das informações digitais, até as técnicas que envolvem o processo de manipulação incluindo a criptografia;
- b) análise de técnicas que empregam a marca d'água para garantir autenticidade de imagens digitais. A técnica considerada pioneira na área é a que foi proposta por Cox et al. (1997). Em seguida, foram analisadas outras pesquisas mais recentes baseadas na inserção, extração e verificação de marca d'água. Esta segunda etapa tem como objetivo proporcionar uma familiarização prática sobre os processos que envolvem a manipulação de marca d'água e também de possíveis ataques;
- c) fundamentar a importância do uso da transformada wavelet para implementação de técnicas de inserção e extração de marca d'água;
- d) análise do desempenho dos principais métodos de inserção, extração e verificação de marca d'água no domínio wavelet, apontando suas vantagens e desvantagens diante de possíveis ataques;
- e) implementar um método de inserção, extração e verificação de marca d'água no domínio wavelet usando uma marca d'água robusta diante de possíveis ataques como a compressão e adição de ruído seguido de compressão. Nesta proposta usa-se o esquema criptografia Arnold's Cat Map com manipulações matriciais simples.

1.3 Metodologia

Após um levantamento teórico e uma análise dos principais métodos de inserção, extração e verificação de marca d'água que apresentam melhores desempenhos, embasado na aplicação em imagens, foi desenvolvido um método de inserção, extração e verificação de marca d'água, sendo este implementado no domínio wavelet.

A implementação da técnica proposta consiste, primeiramente, em preparar a imagem hospedeira, sendo esta decomposta pela transformada wavelet discreta bidimensional (DWTB) em apenas um nível de decomposição (SILVA; DUARTE; VILLAREAL, 2013). Para assim escolher dentre as quatro sub-bandas de frequência (*LL*, *HL*, *LH* e *HH*), a que absorva marca d'água sem agredir a qualidade visual da imagem hospedeira.

A técnica empregada para a decomposição da imagem hospedeira foi proposta por (HAJJARA; ABDALLAH; HUDAIB, 2009), que emprega a DWTB em dois níveis, sendo o último nível diferenciado das aplicações usuais onde a decomposição segue na sub-banda de alta frequência que contém os detalhes da imagem na horizontal (*HL*) ao invés de ser na sub-banda de baixa frequência que contém a aproximação da imagem processada (*LL*).

A marca d'água recebe o mesmo tratamento que a imagem hospedeira, porém a DWTB é aplicada apenas uma vez resultando nas quatro sub-bandas de frequência (*LL*, *HL*, *LH* e *HH*). Cada uma delas será classificada como blocos. Com essa operação a marca d'água decomposta passa a ser representada por quatro subimagens.

A segunda etapa consiste em aplicar a criptografia nos blocos representantes da marca d'água decomposta. A criptografia empregada é a proposta por Vladimir Igorevich Arnold (HUANG et al., 2010), conhecida como Arnold's Cat Map - ACM. Esta técnica muda os pixels de posições proporcionando um efeito visual caótico reversível para garantir mais segurança nesta mesma etapa. Após os blocos estarem criptografados é aplicada uma técnica também reversível, que trata de uma aplicação comum em matrizes, esta aplicação troca elementos simétricos com relação à diagonal secundária da matriz de posições.

Na terceira etapa é realizada a inserção dos blocos criptografados em quatro cantos da sub-banda *HL₂* de forma aleatória, ou seja, há 24 possíveis conjuntos de posições. Para finalizar o processo é aplicado a Transformada Wavelet Discreta Bidimensional Inversa - IDWTB duas vezes para obter a imagem marcada.

Na quarta etapa, é feito o processo inverso da inserção, ou seja, a extração. Primeiro, aplica-se a Transformada Wavelet Discreta Bidimensional - DWTB na imagem marcada, como foi feito na primeira etapa com a imagem hospedeira resultando na sub-banda *HL₂* marcada,

retira-se os quatro blocos de suas respectivas posições. Aplica-se a criptografia ACM reversa e a IDWTB para obter a marca d'água extraída. Na quinta etapa, calcula-se a correlação entre a marca d'água inserida e a extraída, para verificar a semelhança entre as mesmas.

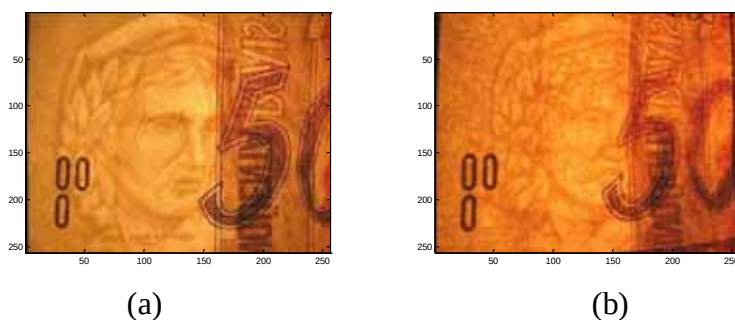
1.4 Estrutura do trabalho

O texto é organizado inicialmente em um capítulo abordando os fundamentos básicos de marca d'água para autenticação de imagens digitais incluindo a criptografia. Sendo este o Capítulo 2. No Capítulo 3 é apresentado o funcionamento dos métodos de inserção, extração e verificação de marca d'água. No Capítulo 4 é feito um estudo sobre a Teoria Wavelet com seus principais fundamentos matemáticos aplicados em imagens. No Capítulo 5 é feita uma análise dos principais métodos descritos na literatura. No Capítulo 6 é apresentada uma proposta para a inserção, extração e verificação de marca d'água no domínio wavelet, baseada no que foi estudado, implementada no Software *MATLAB*[®]. No Capítulo 7 são apresentados os resultados obtidos aplicando o método proposto e no Capítulo 8 as considerações finais, na qual se apresenta a conclusão da pesquisa e sugestões para trabalhos futuros.

2 FUNDAMENTOS BÁSICOS DE MARCA D'ÁGUA DIGITAL

A primeira concepção de marca d'água é associá-la à imagem inserida nas cédulas de dinheiro ou a logotipos que aparecem em vídeos ou imagens digitais. São em materiais não digitais que se pode ter a noção de como a marca d'água é vista em um material digital. Toma-se, como exemplo, a análise de uma cédula qualquer da moeda de Real que ao ser colocada contra a luz normal exhibe marcas e indiscutivelmente é um dos itens mais importantes das cédulas em papel moeda como ilustra a Figura 1. Neste caso, a marca d'água é uma imagem única formada por concentração de massa de papel durante a sua fabricação.

Figura 1 - Imagem da cédula de R\$ 50,00 de 256×256 pixels; (a) Marca d'água autêntica; (b) Marca d'água falsa.



Fonte: Fraudes... (2013).

Essa mesma ideia pode ser utilizada para trabalhar com marca d'água em imagens digitais. Em certos pontos, em ambas as aplicações, tem-se os mesmos aspectos. Por exemplo, a marca d'água, se desejar, poderá ser visível ao Sistema Visual Humano - HVS, em determinada situação, ser única e não interferir nas informações contidas no material, pois em alguns casos ela pode até danificar o trabalho. Isso depende da marca e do quanto ela aparece. Quando ela começa a sobrepor os principais pontos da imagem hospedeira, a marca d'água é considerada inconveniente, por isso é necessário bom senso. Se a marca d'água inserida resultar em um trabalho bem feito, ela não depreciará a arte, como pode ser visto em vários trabalhos (SIMON, 2010). Porém, não é apenas por esse aspecto que a marca d'água deve ser caracterizada, pois para imagens que visam o contexto científico o tipo de marca d'água perceptível não é uma situação a ser recomendada, como ilustra na Figura 2.

Figura 2 - Ilustração de marca d'água perceptível na imagem Cisne 256×256 pixels.



Fonte: Elaborada pela própria autora.

As marcas d'água perceptíveis são usadas principalmente para inibir o uso comercial indevido e podem ser usadas tanto em imagens como em vídeo e áudio. Geralmente, aparecem sobrepostas, sem prejudicar muito a sua percepção e são usadas para expor imagens em locais públicos, como páginas na internet, sem o risco de alguém copiá-las e usá-las comercialmente.

Este tipo de marca d'água é pouco usado, pois é muito sensível a ataques. Por se ter a localização exata da marca d'água, um atacante pode focar seus esforços nesta região tentando removê-la. No caso da mídia ser uma imagem, uma simples operação de recorte poderá remover a marca d'água. Neste caso, se for executado um processo de verificação da autenticidade da imagem, o processo mesmo não irá detectar a presença de marca d'água e será praticamente impossível que o proprietário prove direitos sobre a referida marca d'água. Em outros casos, as características visuais da marca d'água poderão ser copiadas para autenticação de imagens indevidas. No geral, estes sistemas servem apenas como um sinal de advertência para indicar que a mídia digital é de certo proprietário (JOHNSON, 1999).

Já as marcas d'água imperceptíveis são utilizadas principalmente para garantir propriedade de direitos autorais e autenticação de imagens, pois elas são invisíveis. Mas, quando se encontra uma imagem ilegal, a marca que não está visível ao HVS poderá ser extraída desta cópia ilegal, provando assim os direitos autorais do seu proprietário, ou ainda que tal mídia tenha sido alterada.

Quando se diz que a marca d'água deve ser visível ao HVS em certas situações, no caso de imagens digitais, essa escolha dependerá da finalidade da aplicação que, em muitos casos, não é viável.

O modo como a marca d'água é inserida é um dos fatores que distinguem o tratamento que cada tipo de material deve ter ao receber uma marca d'água, ou seja, em material digital. Esses métodos são resumidos em quais tipos de processamento a imagem hospedeira poderá

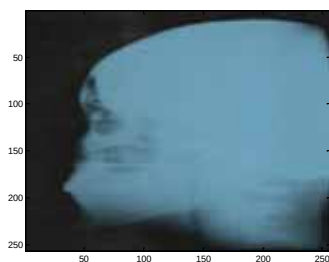
sofrer sem que a marca d'água inserida seja danificada e possa ser facilmente extraída para verificações de autenticidade.

2.1 Aplicação de marca d'água em imagens digitais

Em linguagem mais específica, voltada para a aplicação de marca d'água em imagens, a marca d'água é considerada como uma informação adicional que a imagem carrega. Esse tipo de informação pode ser uma imagem significativa, um logotipo, um sinal com propriedades bem definidas ou um código binário (assinatura digital) construído a partir do conteúdo da própria imagem digital, garantindo, desta forma, sua integridade e os direitos autorais sobre a mesma.

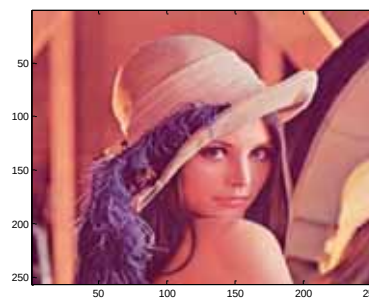
Um cuidado que se deve ter, ao usar marca d'água, é o de evitar que a marca venha a interferir de forma brusca nas informações da imagem hospedeira a qual ela será inserida. O tipo de marca d'água a ser usada depende muito das características da imagem hospedeira e da finalidade de seu uso. Na Figura 3, há uma imagem de caráter científico (a) e outra de caráter artístico (b), que servirão como imagens hospedeiras para alguns tipos de marca d'água. A imagem (a) Raio-X é de propriedade da própria autora, enquanto a imagem (b) Lenna, foi escolhida por ser considerada “Benchmark” na área de processamento de imagens, obtida em <http://www.ece.rice.edu/~wakin/images/>.

Figura 3 - Imagem hospedeira: (a) Raio-X 256×256 pixels; (b) Lenna 256×256 pixels.



(a)

Fonte: (a) Elaborada pela própria autora.



(b)

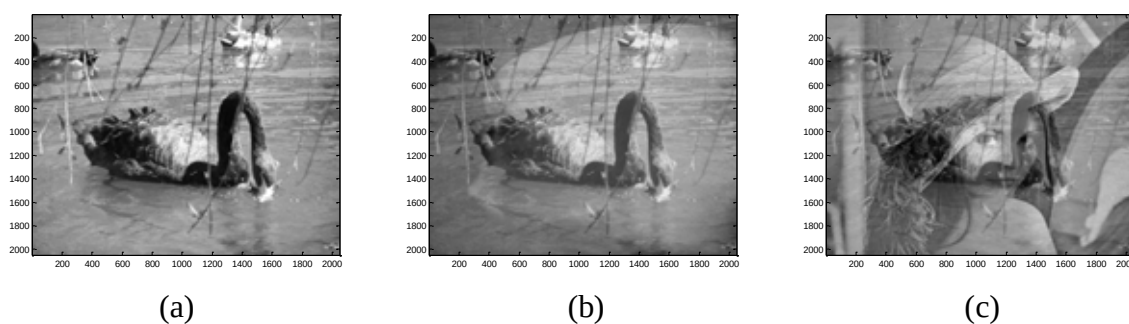
Fonte: The Lenna... (1997).

Marca d'água sobreposta: Este tipo de marca d'água é conhecido como sendo um logotipo, geralmente são marcas d'água perceptíveis. Um cuidado que se deve ter é que, em alguns casos, dependendo da imagem hospedeira, esse tipo de marca d'água pode prejudicar a

qualidade visual da imagem. Por esse motivo, um dos requisitos é que, em caso de ser outra imagem, ela deve possuir dimensão menor que a imagem hospedeira.

Por exemplo, uma imagem, seja ela biomédica ou artística, não poderá receber uma marca d'água como sendo outra imagem com a mesma dimensão, o que provocaria confusão não se sabendo ao certo qual é a imagem hospedeira e qual é a marca d'água. Isso comprometeria o diagnóstico e até mesmo a segurança das informações originais contidas na imagem. Uma melhor ilustração é realizada na Figura 4, na qual pode-se perceber claramente a confusão entre imagem hospedeira e marca d'água.

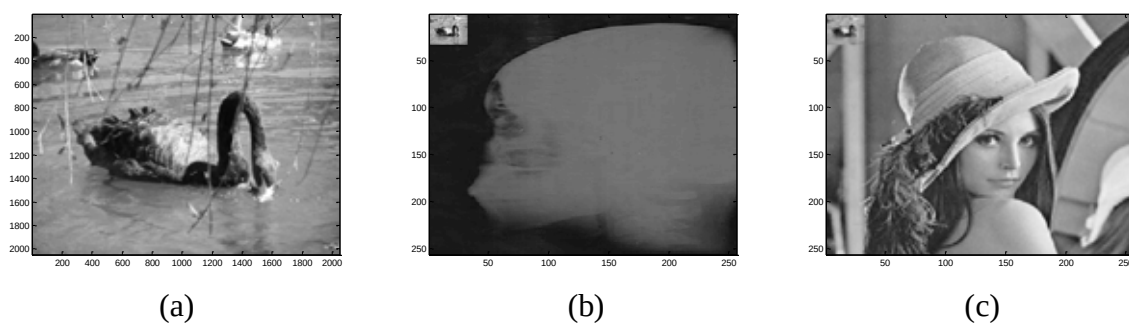
Figura 4 - (a) Imagem Cisne 2048×2048 pixels considerada a marca d'água; (b) Raio-X 2048×2048 pixels autenticada por (a); (c) Lenna 2048×2048 pixels autenticada por (a).



Fonte: Elaborada pela própria autora.

Uma alternativa para o uso desse tipo de marca d'água seria aplicar uma marca d'água com dimensão menor que a imagem hospedeira. É possível observar na Figura 5 que, de acordo com o local da inserção, a marca poderá prejudicar menos o conteúdo da imagem hospedeira, como ilustra a Figura 5 (b) e (c), porém não deixa de ser alvo fácil de uma possível manipulação, como um recorte.

Figura 5 - (a) Cisne 32×32 pixels considerada a marca d'água; (b) Raio-X 256×256 pixels autenticada por (a); (c) Lenna 256×256 pixels autenticada por (a).



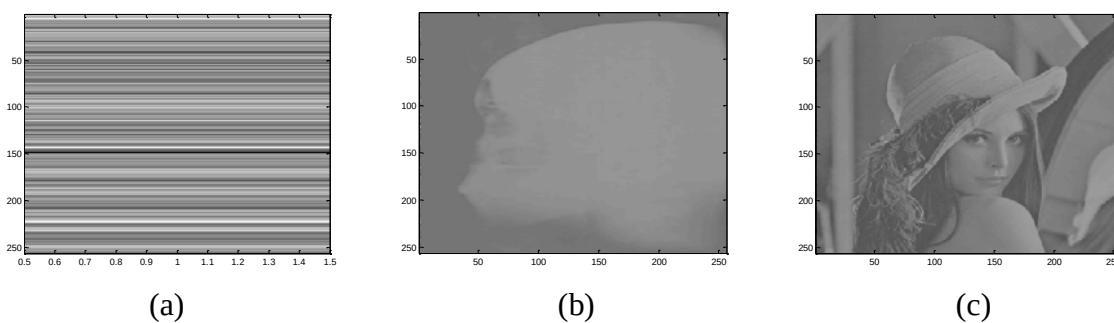
Fonte: Elaborada pela própria autora.

Esse problema pode ser evitado optando, primeiramente, por uma marca d'água imperceptível e de dimensão menor que a imagem hospedeira. As marcas d'água consideradas imperceptíveis são do tipo pseudoaleatória, aleatória e binária.

A marca d'água, independentemente de ser uma imagem, um sinal pseudoaleatório, aleatório ou binário, ela é apresentada como uma matriz bidimensional de números inteiros que corresponde à medida discreta de radiância espectral de cada um de seus elementos, cada elemento desta matriz é chamado de pixel da imagem (GONZÁLES; WOODS, 2000). Tal característica matemática das imagens digitais facilita muito para que sejam feitas operações sobre estas imagens.

Marca d'água pseudoaleatória: Este tipo de marca d'água não compromete uma análise visual da imagem hospedeira, isso porque, geralmente, seus pixels possuem valores bem menores que os pixels da imagem hospedeira o que a torna imperceptível já que, ao ser adicionada, ela não interferirá nas características visuais da imagem hospedeira, funcionando, dessa forma, como se fosse adicionado um ruído leve na imagem, interferindo o mínimo possível. Isso pode ser comprovado na ilustração das imagens autenticadas na Figura 6.

Figura 6 - (a) Marca d'água pseudoaleatória de tamanho $n = 256$; (b) Raio X 256×256 pixels autenticada por (a); (c) Lenna 256×256 pixels autenticada por (a).



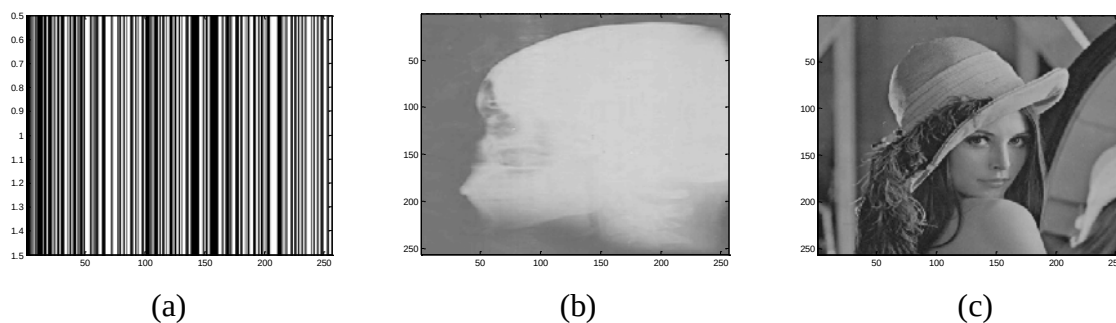
Fonte: Elaborada pela própria autora.

Marca d'água aleatória: Numa marca d'água aleatória os valores dos pixels são $\{-1,1\}$. Esse tipo de marca d'água não é muito usado para autenticar imagens devido ao trabalho de autenticar cada cópia, que compromete o processo de extração baseado em sistema cego ou semicego do qual não requer a marca d'água inserida (SANS, 2008).

A autenticação nesse caso, poderá ser composta por informações do fornecedor da imagem que assim ficará mais difícil para que o receptor da imagem marcada tente sobrescrever a marca d'água com outra imagem qualquer, pois terá muito trabalho. E,

dependendo da aleatoriedade da marca, prejudicará até a qualidade da imagem. Na Figura 7 é ilustrado a autenticação de uma imagem com a marca d'água aleatória.

Figura 7 - (a) Marca d'água aleatória de tamanho $n = 256$; (b) Raio-X 256×256 pixels autenticada por (a); (c) Lenna 256×256 pixels autenticada por (a).

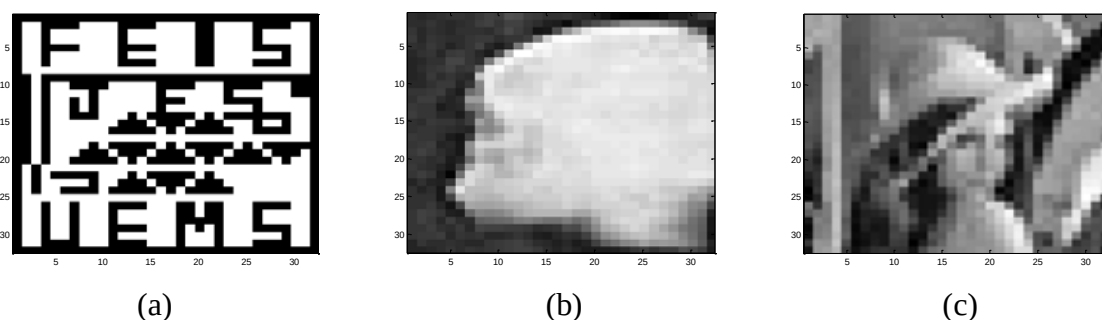


Fonte: Elaborada pela própria autora.

Marca d'água binária: É o tipo de marca d'água mais aplicada em imagens, pois não interfere na qualidade visual da imagem hospedeira e nem no seu conteúdo digital, já que os valores dos pixels da imagem hospedeira são muito maiores que os da marca d'água, o que a torna imperceptível, como é o caso das marcas d'água pseudoaleatória e aleatória.

Essa característica pode ser observada na Figura 8, onde a imagem hospedeira não sofre mudanças bruscas em sua qualidade visual mesmo com a marca d'água cobrindo totalmente a imagem. Se o objetivo é garantir a integridade de uma imagem, neste caso, o recomendado seria usar uma marca d'água binária.

Figura 8 - (a) Marca d'água binária 32×32 pixels; (b) Raio-X 32×32 pixels autenticada por (a); (c) Lenna 32×32 pixels autenticada por (a).



Fonte: Elaborada pela própria autora.

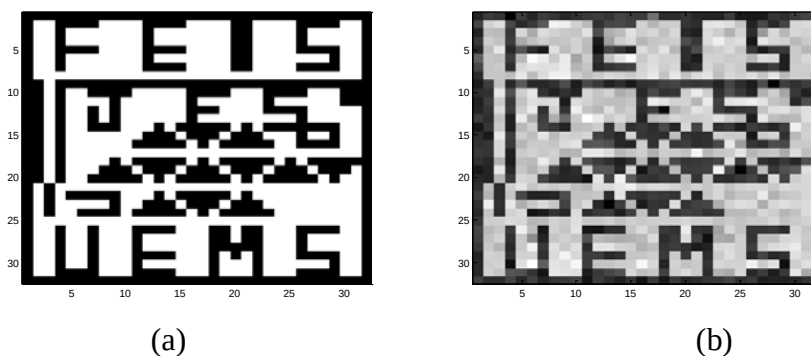
A aplicação de marca d'água varia de acordo com o objetivo que se deseja. Porém, por se tratar de um conteúdo digital, uma imagem marcada deve ser considerada autêntica mesmo que o seu código tenha sofrido algum tipo de alteração, desde que não mude a essência da

informação contida na imagem devido a tratamentos usuais como, por exemplo, recortes, inserções, mudança de formato, nitidez, contraste e compressões (BARNI; BARTOLINI, 2004).

Ao marcar uma imagem, é preciso definir quais as características que serão garantidas: as informações da imagem hospedeira ou as informações da marca d'água inserida. Isso porque, no método de inserção, um dos requisitos para ser considerada uma boa marca d'água é que a marca não interfira visual e digitalmente no conteúdo da imagem hospedeira. Já no processo de extração essa garantia não é tão efetiva.

O ideal seria que, no processo de extração, tanto a imagem hospedeira quanto a marca d'água sofressem o mínimo possível de distorção, para que a imagem extraída possa ser utilizada assim como a marca d'água. Porém, isso dificilmente acontece. Ou a imagem hospedeira sofrerá perda de informações ou a marca d'água não será 100% a mesma inserida, porém, podendo ser considerada autêntica com certa margem de erro, como pode ser observado na Figura 9.

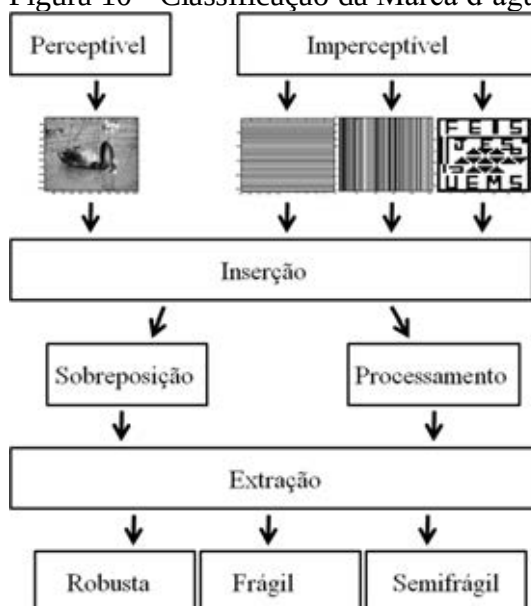
Figura 9 - (a) Marca d'água inserida 32×32 pixels; (b) Marca d'água extraída 32×32 pixels.



Fonte: Elaborada pela própria autora.

Algumas distorções consideradas aceitáveis ocorrem, pois os métodos de processamento, principalmente na extração, são métodos baseados na perda de informações. Por exemplo, se uma imagem está autenticada com marca d'água e esta vem a sofrer uma compressão, tanto a imagem hospedeira quanto a marca d'água inserida perderão informações, perda considerada natural ao processamento. Esta perda de informações em marcas d'água é um fator que as classificam em termos de processamento em robusta, frágil ou semifrágil. Conforme, ilustra a Figura 10.

Figura 10 - Classificação da Marca d'água.



Fonte: Elaborada pela própria autora.

A escolha do tipo de marca d'água a ser utilizada depende do objetivo de seu uso, que se baseia na finalidade para a qual ela será utilizada (COX; MILLER; BLOOM, 2000; MOHANTY, 1999).

2.2 Classificação de marca d'água em termos de remoção

Perceptível ou imperceptível, pseudoaleatória, aleatória ou binária, não é o tipo de marca d'água que determina se ela será robusta, frágil ou semifrágil, e sim a dificuldade em removê-la.

Quando uma imagem que possui marca d'água passa por um processamento do tipo rotação, mudança de escala, mudança de brilho, contraste ou compressão seus dados sofrem modificações. Se neste processo a marca d'água inserida mantiver suas informações originais, então esta marca d'água é considerada robusta, pois apresenta resistência diante de ataques bruscos. Normalmente, esse tipo de marca d'água é usado com o objetivo de proteger direitos autorais.

Apesar de todas as mudanças que se possa fazer na imagem hospedeira, a marca d'água robusta inserida em uma imagem, deve permanecer detectável o que possibilitará saber exatamente onde ela foi inserida, enquanto a imagem modificada continuará mantendo as características visuais da imagem original (DUARTE; SILVA; VILLARREAL, 2011).

Caso as informações da marca d'água apresentem mudanças, a marca d'água é classificada como frágil, pois apresenta extrema sensibilidade diante de qualquer modificação no conteúdo digital, o que contribui na verificação de autenticidade. Em outras palavras, essa marca d'água garante que a imagem marcada não seja editada ou adulterada, possibilitando detectar qualquer alteração.

A marca d'água semifrágil apresenta resistência a alterações suaves e sensibilidade a alterações radicais. Ou seja, é possível distinguir as alterações que não modificam o conteúdo visual. Esse tipo de marca d'água permite a compressão da imagem antes de ser transmitida ou armazenada em um banco de dados, mantendo a autenticação da imagem. Pois, para recuperar o arquivo comprimido e obter a informação original, seria necessário recuperar a marca d'água e, depois de obtida a informação original, ela poderia ser descartada (MOHANTY, 1999).

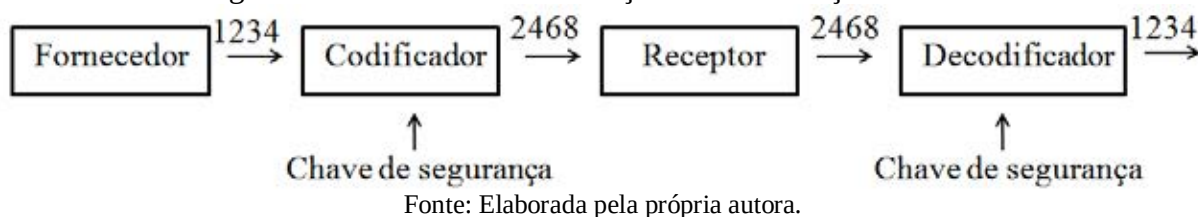
2.3 Marca d'água e criptografia

A marca d'água em si não é suficiente para garantir a integridade dos dados. Para que isso seja possível, é necessário que a marca d'água passe por mascaramento de suas informações. Esse mascaramento, geralmente, é realizado por alguma técnica de criptografia.

A criptografia é considerada a arte de escrever em códigos fornecendo uma comunicação segura entre duas partes: o fornecedor e o receptor da informação. Essas trocas de informações são feitas, normalmente, em um canal aberto de comunicação, e só é possível com o auxílio de chaves, que podem ser públicas ou privadas (VOLPI, 2001).

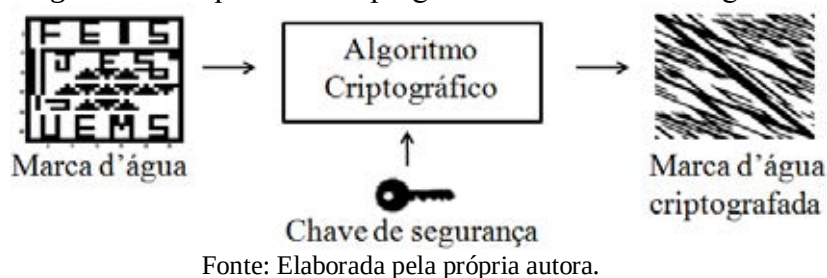
Um exemplo comum da aplicação da criptografia é atribuído ao realizar um "*home banking*" no qual o número do cartão de crédito é enviado pela internet, que por sua vez é classificada como uma rede pública. Para garantir a credibilidade financeira, o número fornecido é protegido por codificação. Este processo de codificação é chamado de cifragem. O processo para obter a informação original, a partir do arquivo cifrado, chama-se decifragem. Ambas são realizadas por programas chamados de cifradores e decifradores, ou codificadores e decodificadores, respectivamente (VOLPI, 2001). A Figura 11 ilustra o processo de codificação e decodificação de dados.

Figura 11 – Processo de codificação e decodificação de dados.



Os programas, além de receber as informações a serem cifradas ou decifradas, recebem uma chave que é utilizada para definir como irão se comportar. Sem o conhecimento da chave correta não é possível decifrar a informação que foi cifrada. A Figura 12 ilustra o processo de criptografia de uma marca d'água (VOLPI, 2001).

Figura 12 - Esquema de criptografia de uma marca d'água.



Em conjunto com a criptografia, há outra técnica chamada de esteganografia (WAYNER, 2002). A criptografia tem o propósito de impedir que as pessoas saibam o conteúdo de uma mensagem, enquanto a esteganografia se baseia em evitar que as pessoas saibam que a mensagem existe. Ou seja, se uma imagem é criptografada, o receptor sabe da existência da mensagem, porém não consegue, a princípio, lê-la. Já a esteganografia tenta fazer com que os receptores não percebam que há uma mensagem no arquivo enviado (WAYNER, 2002).

Mesmo o caso de uma marca d'água imperceptível, requer o uso da esteganografia, pois a imagem hospedeira pode passar por algum tipo de processamento para verificar se ela possui ou não marca d'água. Este processamento pode consistir, por exemplo, em analisar as regiões da imagem para ver se todas mantêm uma determinada característica. A região que se diferir das outras pode ser a que contém a marca d'água.

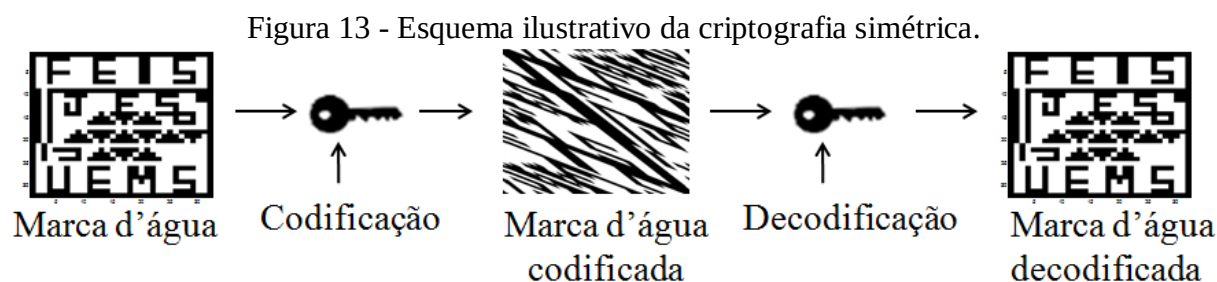
Quando se trata de segurança da informação, a criptografia é mais usada. Porém, quando uma mensagem está criptografada, ela fica destacada por potencialmente possuir uma informação secreta e interessante. A vantagem da esteganografia está relacionada ao

desconhecimento da mensagem, o que evita que muitos ataques sejam realizados (KAWAGUCHI; EASON, 1999).

Para que a comunicação seja a mais privada possível, é recomendável combinar a esteganografia com a criptografia. Dessa forma, caso seja descoberto que a mensagem está camuflada, ainda existirá um novo obstáculo a ser superado para que ela possa ser lida. A criptografia pode ser classificada em dois tipos, de acordo com o tipo de chave a ser usada: criptografia simétrica e assimétrica (BARRETO; KIM; RIJMEN, 2002).

2.3.1 *Criptografia simétrica*

Na criptografia simétrica, ilustrada na Figura 13, são realizadas a cifragem e a decifragem de uma informação através de algoritmos que utilizam a mesma chave. Como a mesma chave deve ser utilizada na cifragem e na decifragem, a chave deve ser compartilhada entre quem cifra e quem decifra os dados.



Os algoritmos que são usados na criptografia simétrica são mais simples e mais rápidos do que os algoritmos usados na criptografia assimétrica, em consequência do fato de se usar a mesma chave, tanto para codificar como para decodificar dados, o que torna a criptografia simétrica adequada à codificação e à decodificação de uma grande quantidade de dados.

A criptografia simétrica não é uma das técnicas mais seguras e modernas que se tem. Porém, o exemplo a ser ilustrado servirá para mostrar como uma só chave (simétrica) é usada para embaralhar e desembaralhar uma mensagem, neste caso a escolhida é a matriz $I_{M \times N}$, com $M = N$.

$$I = \begin{bmatrix} 1 & 3 & 5 \\ 2 & 4 & 6 \\ 3 & 7 & 11 \end{bmatrix}_{3 \times 3} \quad (1)$$

Antes que cada uma das partes, que usam uma chave simétrica, possa transmitir informações de modo seguro ambos precisam saber qual a chave usada, no caso ilustrado a chave será a matriz $C_{M \times N}$, também com $M = N$.

$$C = \begin{bmatrix} 12 & 12 & 12 \\ 12 & 12 & 12 \\ 12 & 12 & 12 \end{bmatrix}_{3 \times 3} \quad (2)$$

A matriz I será criptografada com uma determinada chave C de segurança, que por sua vez deve apresentar as mesmas características matemáticas e dimensão da imagem a ser criptografada. A Equação 3 resume o método de codificação.

$$IC_{M \times N} = I_{M \times N} - C_{M \times N} \quad (3)$$

sendo

I : imagem a ser protegida (cifrada);

C : chave de segurança;

IC : imagem cifrada.

Tem-se:

$$IC = \begin{bmatrix} -11 & -9 & -7 \\ -10 & -8 & -6 \\ -9 & -5 & -1 \end{bmatrix}_{3 \times 3} \quad (4)$$

A equação algébrica 5 resume o método de decodificação.

$$I_{M \times N} = IC_{M \times N} + C_{M \times N} \quad (5)$$

$$I = \begin{bmatrix} 1 & 3 & 5 \\ 2 & 4 & 6 \\ 3 & 7 & 11 \end{bmatrix}_{3 \times 3} \quad (6)$$

Deste modo, a imagem cifrada poderá ser transmitida de forma protegida e seu receptor poderá obter a imagem original apenas somando a chave à imagem cifrada. Se ambas as partes já estão de acordo com qual chave usar, antes de iniciar a transmissão, então a criptografia simétrica é o suficiente. Entretanto, este acordo prévio nem sempre é possível.

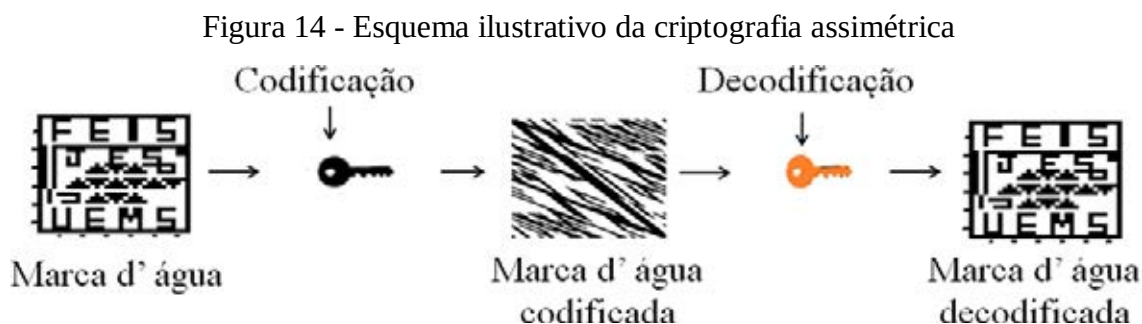
O processo de compartilhamento de chaves deve ser feito de forma segura, uma vez que todos que conhecem a chave podem decifrar a informação cifrada ou mesmo reproduzir outra informação cifrada. Esta é uma das principais desvantagens da criptografia simétrica, pois cria um problema de gerenciamento de segurança. O problema de gerenciamento de segurança existe justamente porque a organização deve enviar essa chave de criptografia a todos que

requisitarem acesso aos dados criptografados. Para solucionar e evitar problemas provenientes desse tipo de criptografia usa-se a criptografia assimétrica (STALLINGS, 1999).

2.3.2 *Criptografia assimétrica*

A criptografia assimétrica usa duas chaves diferentes, porém matematicamente relacionadas, para criptografar e descriptografar dados. Essas chaves são conhecidas como chaves privadas e chaves públicas, ou ainda, em conjunto, são conhecidas como par de chaves.

Para entender como funciona a criptografia assimétrica, pode-se imaginar um arquivo a ser salvo, armazenado e posteriormente editado. Para salvar o arquivo é usado um código diferente daquele usado para abri-lo. Assim, ao criptografar uma imagem usa-se uma chave na codificação e uma na decodificação, conforme ilustra a Figura 14.



Se os dados forem criptografados por meio de chave pública, só poderão ser descriptografados com o uso da chave privada. Mas, se os dados forem criptografados por meio da chave privada só poderão ser descriptografados com o uso da chave pública (BARRETO; KIM; RIJMEN, 2002). Este é um dos fatores que fornece confidencialidade na transmissão e recepção de dados criptografados por meio de criptografia assimétrica.

A criptografia assimétrica é considerada mais segura do que a criptografia simétrica, porque a chave usada para criptografar os dados é diferente daquela usada para descriptografá-los.

Como a criptografia assimétrica usa um par de chaves, o processo de criptografia é muito mais lento já que os algoritmos são mais complexos do que na criptografia simétrica. Um sistema assimétrico muito usado é proposto por Ron Rivest, Adi Shamir e Len Adleman, em 1977 - RSA. Este sistema utiliza resultados conhecidos da Teoria dos Números para poder

garantir uma grande segurança no processo de decifração. Por isso, há a necessidade de se trabalhar com números primos.

1. Escolha dois números primos: $p \in \mathbb{N}$ e $q \in \mathbb{N}$, sendo neste caso $p=3$ e $q=7$. Calcule o valor de n dado pela Equação 7.

$$n = p * q \quad (7)$$

- $n = 21$

2. Calcule o valor da Função de Euler $\varphi(n)$ dado pela Equação 8.

$$\varphi(n) = (p-1) * (q-1) \quad (8)$$

- $\varphi(n) = 12$

3. Escolha um número primo em relação a $\varphi(n)$ e chame-o de “ e ”, sendo $e \in \mathbb{N}$, tal que $1 < e < \varphi(n)$.

- $e = 5$;

4. Determine “ d ” pela Equação 9.

$$d = \frac{1}{e} \bmod \varphi(n) \quad (9)$$

Onde “ $\bmod$ ” é o a função que retorna o resto inteiro da divisão do inverso multiplicativo de e por $\varphi(n)$.

- $d=0$

Portanto, a chave pública $C_{pública}$ consiste em $C_{pública}=\{e,n\}$ e a chave privada $C_{privada}$ consiste em $C_{privada}=\{d,n\}$.

As equações para criptografar e descriptografar são mais complexas do que as da técnica de criptografia simétrica:

$$IC_{M \times M} = I_{M \times M}^e \bmod(n) \quad (10)$$

$$I_{M \times M} = IC_{M \times M}^d \bmod(n) \quad (11)$$

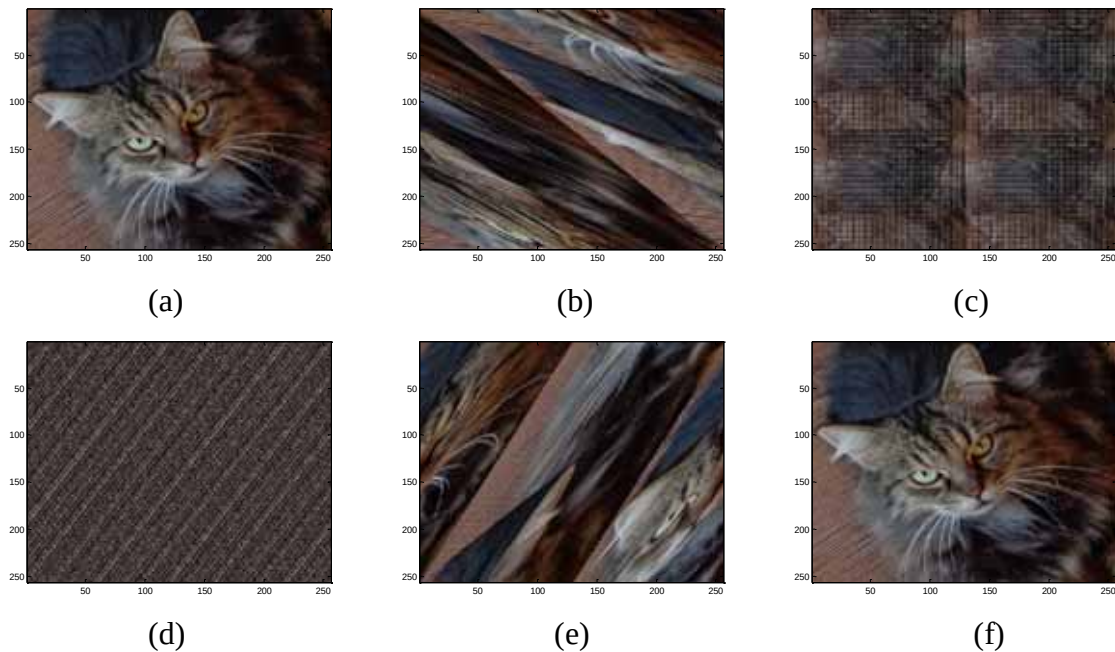
Existem duas chaves: e serve para codificar, enquanto d decodifica a mensagem.

2.4 Criptografia Cat Map

A criptografia Arnold's Cat Map - ACM é uma transformação caótica específica desenvolvida pelo matemático russo Vladimir Igorevich Arnold (ARNOLD; AVEZ, 1968) o qual aplicou uma transformação, que está por trás de uma evolução aparentemente aleatória de um sistema, a uma imagem feita de seu gato, por isso chamada de Arnold's Cat Map.

A técnica proposta por Arnold é considerada um sistema discreto, pois processa o sinal discreto resultando em saídas discretas. A técnica se baseia numa transformação da imagem em tons de cinza por meio de fundamentos de Álgebra Linear que reorganiza cada um dos pixels da imagem mudando-os de posição, como se fossem embaralhados em uma ordem aparentemente desorganizada. Porém, ao repetir várias vezes tal transformação, a imagem original voltará a aparecer. Essa transformação pode ser observada na Figura 15 ao ser realizada na imagem Cat, que é de propriedade da autora.

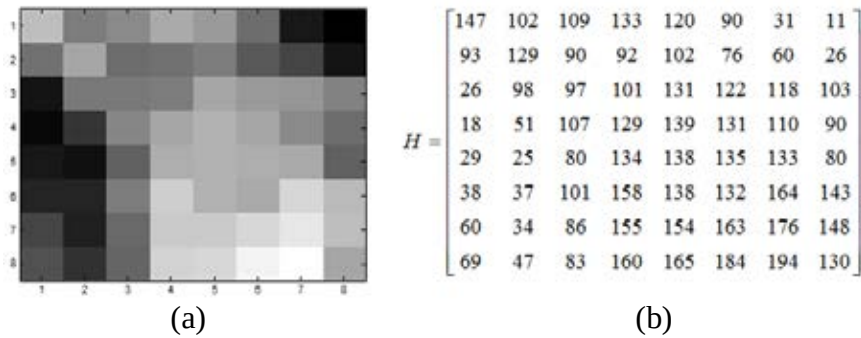
Figura 15 - Criptografia Arnold' Cat Map: (a) Nível 1; (b) Nível 2; (c) Nível 96; (d) Nível 187; (e) Nível 191; (f) Nível 192.



Fonte: Elaborada pela própria autora.

A transformação ACM é composta de um cisalhamento na direção x com fator 1 seguido de um cisalhamento na direção y com fator 1. As contas são feitas usando $\text{mod}(1)$, se l é um número real, então a notação $l \text{ mod}(1)$ denota o único número do intervalo $[0,1)$ que difere de l por um número inteiro. A aplicação T leva todos os pontos de $\mathbb{R}^2$ no quadrado unitário S (ANTON; RORRES, 1994). Na Figura 16 é ilustrada uma imagem 8×8 pixels e sua representação matricial.

Figura 16 - (a) Imagem original; (b) Matriz que representa a intensidade dos pixels da imagem (a).



Fonte: Elaborada pela própria autora.

A seguir, os passos do algoritmo para realizar o cisalhamento da imagem representada pela matriz da Figura 16 (b).

Passo 1: Cisalhamento na direção x com fator 1 que origina a matriz H_x .

$$(x, y) \mapsto (x + y, y)$$

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} x + y \\ y \end{bmatrix} \text{mod}(1) \quad (12)$$

$$H_x = \begin{bmatrix} 147 & 102 & 109 & 133 & 120 & 90 & 31 & 11 \\ 93 & 129 & 90 & 92 & 102 & 76 & 60 & 26 \\ 26 & 98 & 97 & 101 & 131 & 122 & 118 & 103 \\ 18 & 51 & 107 & 129 & 139 & 131 & 110 & 90 \\ 29 & 25 & 80 & 134 & 138 & 135 & 133 & 80 \\ 38 & 37 & 101 & 158 & 138 & 132 & 164 & 143 \\ 60 & 34 & 86 & 155 & 154 & 163 & 176 & 148 \\ 69 & 47 & 83 & 160 & 165 & 184 & 194 & 130 \end{bmatrix}$$

A Figura 17 ilustra como é feito o cisalhamento na direção x em uma matriz.

Figura 17 - Cisalhamento na direção x.



Fonte: Elaborada pela própria autora.

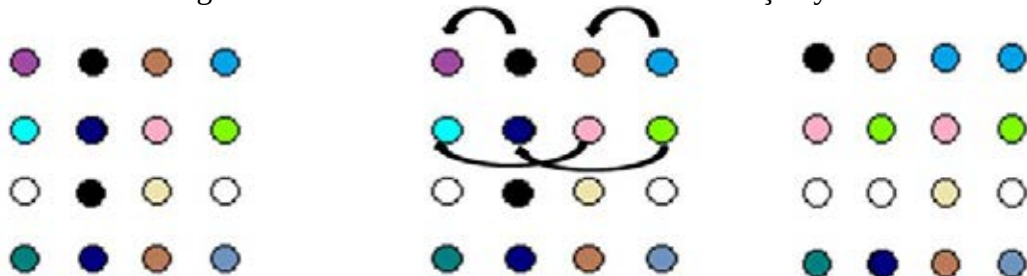
Passo 2: Cisalhamento na direção y com fator 1

$$(x, y) \mapsto (x, x + y)$$

$$\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} x \\ x + y \end{bmatrix} \text{mod}(1) \quad (13)$$

A Figura 18 ilustra como é feito o cisalhamento na direção y em uma matriz, e a Figura 19 o efeito do cisalhamento em ambas as direções x e y.

Figura 18 - Resultado do cisalhamento na direção y.



Fonte: Elaborada pela própria autora.

Figura 19 - Resultado do cisalhamento na direção x e y.



Fonte: Elaborada pela própria autora.

A técnica ACM é considerada periódica de período T , já que após T processos sucessivos de transformação a imagem original é recuperada. Essa afirmação é fundamentada pelo Teorema de Poincaré o qual afirma que os sistemas de recorrência são determinados, após um tempo, suficiente para retornar a um estado muito próximo ao estado inicial (PETERSON, 1997). Desta forma, define-se a técnica ACM.

Definição: A transformação ACM é a aplicação $T: \mathbb{R}^2 \rightarrow \mathbb{R}^2$ definida por

$$T: (x, y) \mapsto (x + y, x + 2y) \text{MOD}(N)$$

Ou, em notação matricial:

$$T \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \text{MOD}(N) \quad (14)$$

Para uma imagem $I_{M \times N}$, em cada pixels com coordenadas x e y , a técnica ACM é uma transformação dada pela Equação 15.

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & p \\ q & pq+1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \text{MOD}(N) \quad (15)$$

sendo

x e y : coordenadas dos pixels da imagem;

x' e y' : novas coordenadas da imagem.

N : dimensão da imagem;

p e q : parâmetros que preservam a região mapeada.

$x \text{MOD}(N)$ resto da divisão inteira de x por N .

Para quaisquer p e q inteiros, a Equação 16 sempre será satisfeita.

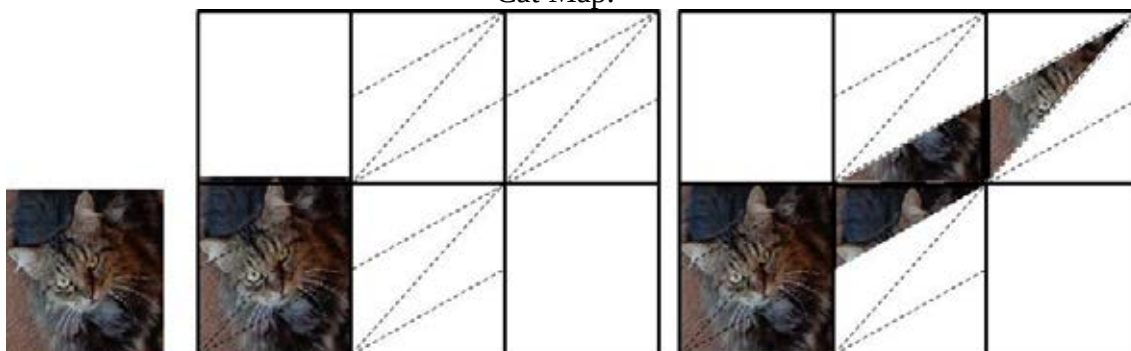
$$\det \begin{bmatrix} 1 & p \\ q & pq+1 \end{bmatrix} = 1 \quad (16)$$

A seguir é descrito o algoritmo da técnica proposta por Vladimir I. Arnold.

1. Aplicar o ACM na imagem original por meio da Equação 15.

O resultado da aplicação da equação será como se a imagem fosse recortada e esticada. Este processo é ilustrado na Figura 20.

Figura 20 - Representação esquemática da resultante do primeiro passo do algoritmo Arnold's Cat Map.



Fonte: Elaborada pela própria autora.

2. Avaliar a função *MOD* que irá dividir a imagem esticada e remontá-la em outra imagem que restaura a dimensão original da imagem como é ilustrada na Figura 21.

Figura 21 - Representação esquemática da resultante do segundo passo do algoritmo Arnold's Cat Map aplicado uma vez.



Fonte: Elaborada pela própria autora.

Ao realizar n interações é possível observar que a imagem retorna à sua posição original. Além disso, em algumas das interações intermediárias, a imagem está decomposta em faixas que parecem ter uma só direção específica.

2.5 Assinatura digital

A assinatura digital é resultado do processo de criptografia assimétrica que utiliza algoritmos de chave-pública para cifrar uma mensagem. O processo de cifrar a mensagem

com a chave-pública e decifrar com a chave-privada, ou cifrar com a chave-privada e decifrar com a chave-pública, resulta na recuperação da mensagem.

Um exemplo simples de assinatura digital é o criptograma, que é resultado da cifragem de um determinado bloco de dados por meio de chave-privada de quem assina em um algoritmo assimétrico. A verificação da assinatura é feita “decifrando-se” o criptograma com a chave-pública correspondente. Se o resultado for satisfatório, a assinatura é considerada autêntica. Na prática, não há assinatura digital, o que há é um resumo, obtido por meio do seu processamento através do que se denomina a função *hash*.

2.5.1 *Função hash*

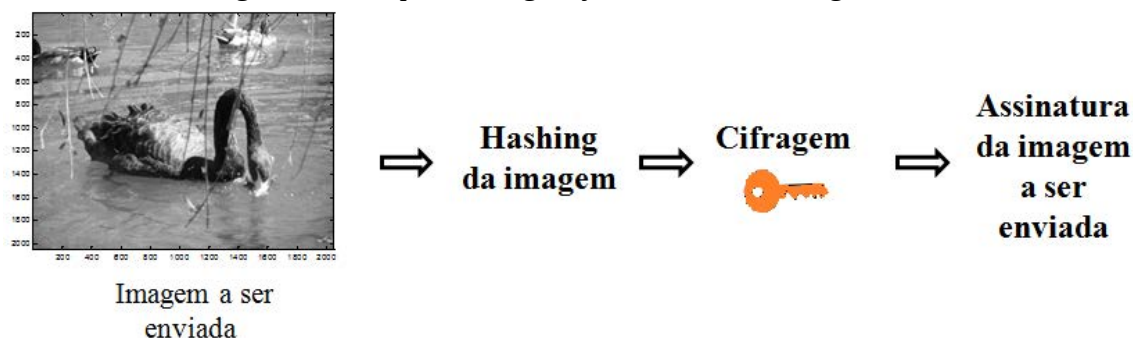
É uma função criptográfica que tem como finalidade computar um resumo de mensagem ao criar uma assinatura digital. Normalmente, esta função gera uma saída de tamanho fixo de 128 a 256 bits, independentemente do tamanho da entrada. A esta saída se denomina função *hash* da mensagem, que está matematicamente relacionada com a entrada, servindo como uma imagem representativa compacta da mensagem, ou seja, um resumo. Este resumo, também pode ser chamado de impressão digital ou "*messagedigest*". Para ter utilidade criptográfica, a função *hash* deve ser computacionalmente:

- a) simples, eficiente e rápida, para se calcular o *hash* da mensagem;
- b) inviável obter uma mensagem original a partir de seu *hash*;
- c) impossível duas entradas resultarem no mesmo *hash*, ou seja, os possíveis valores de *hash* são estatisticamente equiprováveis.

Arquivos, como imagens, recebem o mesmo tratamento que um arquivo de texto. Particularmente, no caso de imagens, elas podem apresentar dimensões arbitrárias. Então a imagem é comprimida e um resumo é criado. Este resumo é um código com um número fixo de bits, chamado de resultado *hash*.

A ideia básica é que o resultado *hash* forneça uma identidade única para uma determinada imagem, tendo como base que a proteção de uma pequena identidade é mais fácil de ser obtida do que a proteção da imagem como um todo. A Figura 22 ilustra como gerar uma assinatura de uma imagem digital.

Figura 22 - Esquema da geração de assinatura digital.



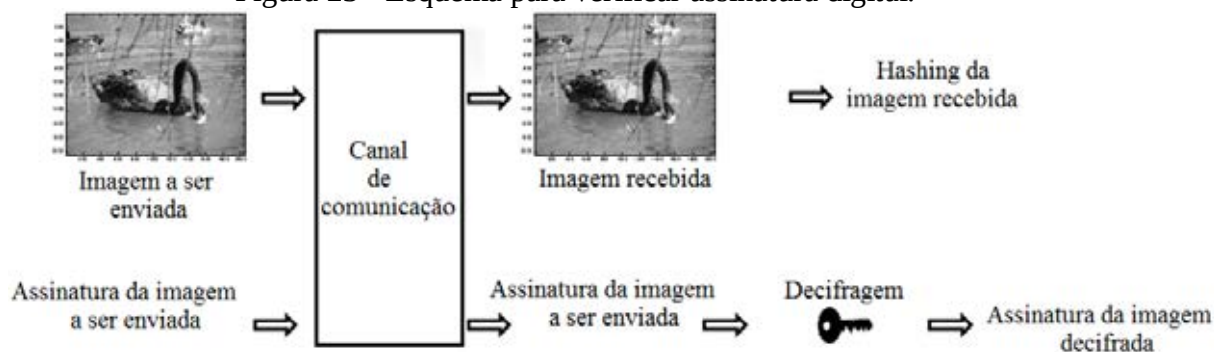
Fonte: Elaborada pela própria autora.

Uma função *hash* utilizada para autenticação digital deve ter certas propriedades que a torna segura para uso criptográfico, dentre elas estão:

- impossibilidade de decifrar uma mensagem mesmo conhecendo o *messagedigest*, pois a descoberta de uma mensagem que dê um *hash* possibilita que a mensagem falsa seja substituída por uma mensagem autêntica. Além disso, também permite que a mensagem seja rejeitada de forma desleal alegando que, na realidade, o arquivo foi assinado com uma mensagem diferente, dando um *hash* ao mesmo valor e violando assim a propriedade de não-repúdio das assinaturas digitais;
- impossibilidade que duas mensagens distintas venham a fornecer um mesmo *hash*, já que duas mensagens distintas que apresentem um *hash* ao mesmo valor possibilitam um tipo de ataque no qual alguém é induzido a assinar uma mensagem que dá um *hash* ao mesmo valor como sendo outra mensagem com um conteúdo totalmente diferente.

A Figura 23 ilustra o processo de verificação da assinatura digital de uma imagem.

Figura 23 - Esquema para verificar assinatura digital.



Fonte: Elaborada pela própria autora.

Se a assinatura decifrada for igual ao *hash* da imagem recebida então o receptor da imagem sabe que documento recebido é cópia fiel do original. Caso contrário, ou não foi o fornecedor que o enviou ou assinou, ou o documento foi adulterado após a assinatura, ou ambos. O algoritmo a seguir descreve o processo para obter o *hash* de da matriz A que representa uma imagem de dimensão 4×4 pixels.

$$A = \begin{bmatrix} 147 & 102 & 109 & 133 \\ 93 & 129 & 90 & 92 \\ 26 & 98 & 97 & 101 \\ 18 & 51 & 107 & 129 \end{bmatrix}_{4 \times 4}$$

Passo 1: Calcular a dimensão da tabela *hash* aplicando a Equação 17, considerando o número de colunas. A Tabela 1 apresenta as casas que compõe a tabela *hash*.

$$u = 2^N \quad (17)$$

$$\bullet \quad u = 2^4 = 16$$

Tabela 1 - Tabela *hash*

Casa 0	Casa 1	Casa 2	Casa 3	Casa 4	Casa 5	Casa 6	Casa 7
Casa 8	Casa 9	Casa 10	Casa 11	Casa 12	Casa 13	Casa 14	Casa 15

Fonte: Elaborada pela própria autora

Passo 2: Calcular a função *hash* aplicando a Equação 18 para cada elemento da matriz A .

$$H = \begin{bmatrix} 147 & 102 & 109 & 133 \\ \text{elemento1} & \text{elemento2} & \text{elemento3} & \text{elemento4} \\ 93 & 129 & 90 & 92 \\ \text{elemento5} & \text{elemento6} & \text{elemento7} & \text{elemento8} \\ 26 & 98 & 97 & 101 \\ \text{elemento9} & \text{elemento10} & \text{elemento11} & \text{elemento12} \\ 18 & 51 & 107 & 129 \\ \text{elemento13} & \text{elemento14} & \text{elemento15} & \text{elemento16} \end{bmatrix}$$

$$h(A) = H \bmod(u) \quad (18)$$

sendo:

A : elemento i ;

$h(A)$: casa que deverá ser ocupada;

mod: representa a aritmética módulo *b*, isto é, o resto inteiro da divisão de *a* por *b*

$147 \bmod (16) = 3$	$102 \bmod (16) = 6$	$109 \bmod (16) = 13$	$133 \bmod (16) = 5$
$93 \bmod (16) = 13$	$129 \bmod (16) = 1$	$90 \bmod (16) = 10$	$92 \bmod (16) = 12$
$26 \bmod (16) = 10$	$98 \bmod (16) = 2$	$97 \bmod (16) = 1$	$101 \bmod (16) = 5$
$18 \bmod (16) = 2$	$51 \bmod (16) = 3$	$107 \bmod (16) = 11$	$129 \bmod (16) = 1$

Passo 3: Inserir cada valor na tabela *hash*, o que pode se tornar complicado se o caso de colisão não for resolvido. Então, nesse caso, se verifica se o índice correspondente ao valor da função de *hash* relativo ao número já estava preenchido. Se sim, esse valor irá para a posição anterior à casa que deveria ocupar. Caso contrário, basta inserir o valor nesse índice da Tabela 1.

Elemento 1, casa 3; Elemento 2, casa 6; Elemento 3, casa 13; Elemento 4, casa 5;
 Elemento 5, casa 13; Elemento 6, casa 1; Elemento 7, casa 10; Elemento 8, casa 12;
 Elemento 9, casa 10; Elemento 10, casa 2; Elemento 11, casa 1; Elemento 12, casa 5;
 Elemento 13, casa 2; Elemento 14, casa 3; Elemento 15, casa 11; Elemento 16, casa 1;

A Tabela 2 a seguir ilustra a colocação de cada um dos elementos nas casas correspondentes.

Tabela 2 - Tabela *hash* preenchida pelos quatro primeiros elementos sem colisão.

Casa 0	Casa 1	Casa 2	Casa 3	Casa 4	Casa 5	Casa 6	Casa 7
			147 <i>elemento1</i>		133 <i>elemento4</i>	102 <i>elemento2</i>	
Casa 8	Casa 9	Casa 10	Casa 11	Casa 12	Casa 13	Casa 14	Casa 15
					109 <i>elemento3</i>		

Fonte: Elaborada pela própria autora

- Colisão: elemento 5 na casa 13 que já está ocupada. Portanto, deverá ser colocado na casa anterior a 13 que esteja vazia, ou seja, na casa 12, como apresenta a Tabela 3.

Tabela 3 - Tabela *hash* preenchida após a primeira colisão.

Casa 0	Casa 1	Casa 2	Casa 3	Casa 4	Casa 5	Casa 6	Casa 7
			147 <i>elemento1</i>		133 <i>elemento4</i>	102 <i>elemento2</i>	
Casa 8	Casa 9	Casa 10	Casa 11	Casa 12	Casa 13	Casa 14	Casa 15
				93 <i>elemento5</i>	109 <i>elemento3</i>		

Fonte: Elaborada pela própria autora.

O processo continua até que apareça uma nova colisão como preenchido na Tabela 4.

Tabela 4 - Tabela *hash* preenchida até que apareça uma nova colisão.

Casa 0	Casa 1	Casa 2	Casa 3	Casa 4	Casa 5	Casa 6	Casa 7
	129 <i>elemento6</i>		147 <i>elemento1</i>		133 <i>elemento4</i>	102 <i>elemento2</i>	
Casa 8	Casa 9	Casa 10	Casa 11	Casa 12	Casa 13	Casa 14	Casa 15
		90 <i>elemento7</i>		93 <i>elemento5</i>	109 <i>elemento3</i>		

Fonte: Elaborada pela própria autora

- Colisão: elemento 8 na casa 12 que já está ocupada. Portanto deverá ser colocado na casa anterior a casa 12 que esteja vazia, ou seja, na casa 11, como apresentado na Tabela 5.

Tabela 5 - Tabela *hash* preenchida após a colisão do elementos 8.

Casa 0	Casa 1	Casa 2	Casa 3	Casa 4	Casa 5	Casa 6	Casa 7
	129 <i>elemento6</i>		147 <i>elemento1</i>		133 <i>elemento4</i>	102 <i>elemento2</i>	
Casa 8	Casa 9	Casa 10	Casa 11	Casa 12	Casa 13	Casa 14	Casa 15
		90 <i>elemento7</i>	92 <i>elemento8</i>	93 <i>elemento5</i>	109 <i>elemento3</i>		

Fonte: Elaborada pela própria autora

- Colisão: elemento 9 na casa 10 que já está ocupada. Portanto, deverá ser colocado na casa anterior a casa 10 que esteja vazia, ou seja, na casa 9, como apresentado na Tabela 6.

Tabela 6 - Tabela *hash* preenchida após a colisão do elementos 9.

Casa 0	Casa 1	Casa 2	Casa 3	Casa 4	Casa 5	Casa 6	Casa 7
	129 <i>elemento6</i>		147 <i>elemento1</i>		133 <i>elemento4</i>	102 <i>elemento2</i>	
Casa 8	Casa 9	Casa 10	Casa 11	Casa 12	Casa 13	Casa 14	Casa 15
	26 <i>elemento9</i>	90 <i>elemento7</i>	92 <i>elemento8</i>	93 <i>elemento5</i>	109 <i>elemento3</i>		

Fonte: Elaborada pela própria autora

O processo continua até que apareça uma nova colisão, como apresentado na Tabela 7.

Tabela 7 - Tabela *hash* preenchida até nova colisão.

Casa 0	Casa 1	Casa 2	Casa 3	Casa 4	Casa 5	Casa 6	Casa 7
	129 <i>elemento6</i>	98 <i>elemento10</i>	147 <i>elemento1</i>		133 <i>elemento4</i>	102 <i>elemento2</i>	
Casa 8	Casa 9	Casa 10	Casa 11	Casa 12	Casa 13	Casa 14	Casa 15
	26 <i>elemento9</i>	90 <i>elemento7</i>	92 <i>elemento8</i>	93 <i>elemento5</i>	109 <i>elemento3</i>		

Fonte: Elaborada pela própria autora.

- Colisão: elemento 11 na casa 1 que já está ocupada. Portanto, deverá ser colocado na casa anterior a 1 que esteja vazia, ou seja, na casa 0, como apresentado na Tabela 8.

Tabela 8 - Tabela *hash* preenchida após a colisão do elemento 11.

Casa 0	Casa 1	Casa 2	Casa 3	Casa 4	Casa 5	Casa 6	Casa 7
97 <i>elemento11</i>	129 <i>elemento6</i>	98 <i>elemento10</i>	147 <i>elemento1</i>		133 <i>elemento4</i>	102 <i>elemento2</i>	
Casa 8	Casa 9	Casa 10	Casa 11	Casa 12	Casa 13	Casa 14	Casa 15
	26 <i>elemento9</i>	90 <i>elemento7</i>	92 <i>elemento8</i>	93 <i>elemento5</i>	109 <i>elemento3</i>		

Fonte: Elaborada pela própria autora

- Colisão: elemento 12 na casa 5 que já está ocupada, portanto deverá ser colocado na casa anterior a 5 que esteja vazia, ou seja, na casa 4, como apresentado na Tabela 9.

Tabela 9 - Tabela *hash* preenchida após a colisão do elementos 12.

Casa 0	Casa 1	Casa 2	Casa 3	Casa 4	Casa 5	Casa 6	Casa 7
97 <i>elemento11</i>	129 <i>elemento6</i>	98 <i>elemento10</i>	147 <i>elemento1</i>	101 <i>elemento12</i>	133 <i>elemento4</i>	102 <i>elemento2</i>	
Casa 8	Casa 9	Casa 10	Casa 11	Casa 12	Casa 13	Casa 14	Casa 15
	26 <i>elemento9</i>	90 <i>elemento7</i>	92 <i>elemento8</i>	93 <i>elemento5</i>	109 <i>elemento3</i>		

Fonte: Elaborada pela própria autora

- Colisão: elemento 13 na casa 2 que já está ocupada. Portanto, deverá ser colocado na casa anterior a casa 2 que esteja vazia, ou seja, na casa 15.
- Colisão: elemento 14 na casa 3 que já está ocupada. Portanto, deverá ser colocado na casa anterior a 3 que esteja vazia, ou seja, na casa 14.
- Colisão: elemento 15 na casa 11 que já está ocupada. Portanto, deverá ser colocado na casa anterior a 11 que esteja vazia, ou seja, na casa 8.

A colocação dos elementos 13, 14 e 15 são apresentados na Tabela 10.

Tabela 10 - Tabela *hash* preenchida após as colisões dos elementos 13, 14 e 15.

Casa 0	Casa 1	Casa 2	Casa 3	Casa 4	Casa 5	Casa 6	Casa 7
97 <i>elemento11</i>	129 <i>elemento6</i>	98 <i>elemento10</i>	147 <i>elemento1</i>	101 <i>elemento12</i>	133 <i>elemento4</i>	102 <i>elemento2</i>	
Casa 8	Casa 9	Casa 10	Casa 11	Casa 12	Casa 13	Casa 14	Casa 15
107 <i>elemento15</i>	26 <i>elemento9</i>	90 <i>elemento7</i>	92 <i>elemento8</i>	93 <i>elemento5</i>	109 <i>elemento3</i>	51 <i>elemento14</i>	18 <i>elemento13</i>

Fonte: Elaborada pela própria autora

- Colisão: elemento 16 na casa 1 que já está ocupada. Portanto, deverá ser colocado na casa anterior a 1 que esteja vazia, ou seja, na casa 7, como apresentado na Tabela 11.

Tabela 11 - Tabela *hash* preenchida após a colisão do elemento 16.

Casa 0	Casa 1	Casa 2	Casa 3	Casa 4	Casa 5	Casa 6	Casa 7
97 <i>elemento11</i>	129 <i>elemento6</i>	98 <i>elemento10</i>	147 <i>elemento1</i>	101 <i>elemento12</i>	133 <i>elemento4</i>	102 <i>elemento2</i>	129 <i>elemento16</i>
Casa 8	Casa 9	Casa 10	Casa 11	Casa 12	Casa 13	Casa 14	Casa 15
107 <i>elemento15</i>	26 <i>elemento9</i>	90 <i>elemento7</i>	92 <i>elemento8</i>	93 <i>elemento5</i>	109 <i>elemento3</i>	51 <i>elemento14</i>	18 <i>elemento13</i>

Fonte: Elaborada pela própria autora

Desta forma o *hash* do conjunto *A*, será o vetor:

$$A_{hash} = [97 \ 129 \ 98 \ 147 \ 101 \ 133 \ 102 \ 129 \ 107 \ 26 \ 90 \ 92 \ 93 \ 109 \ 51 \ 18].$$

Se for considerado a colocação dos elementos percorrendo as colunas da matriz temos a seguinte ordem dos elementos na matriz *A*.

$$A = \begin{bmatrix} 147 & 102 & 109 & 133 \\ \text{elemento1} & \text{elemento5} & \text{elemento9} & \text{elemento13} \\ 93 & 129 & 90 & 92 \\ \text{elemento2} & \text{elemento6} & \text{elemento10} & \text{elemento14} \\ 26 & 98 & 97 & 101 \\ \text{elemento3} & \text{elemento7} & \text{elemento11} & \text{elemento15} \\ 18 & 51 & 107 & 129 \\ \text{elemento4} & \text{elemento8} & \text{elemento12} & \text{elemento16} \end{bmatrix} \quad (19)$$

Elemento 1, casa 3; Elemento 5, casa 6; Elemento 9, casa 13; Elemento 13, casa 5;
 Elemento 2, casa 13; Elemento 6, casa 1; Elemento 10, casa 10; Elemento 14, casa 12;
 Elemento 3, casa 10; Elemento 7, casa 2; Elemento 11, casa 1; Elemento 15, casa 5;
 Elemento 4, casa 2; Elemento 8, casa 3; Elemento 12, casa 11; Elemento 16, casa 1;

A Tabela 12 apresenta a alocação dos elementos de acordo com a casa que eles deverão ocupar, originando desta forma o *hash* da matriz *A*.

Tabela 12 - Tabela *hash* preenchida pelos elementos quando é percorrido as colunas da matriz *A*.

Casa 0 98 <i>elemento7</i>	Casa 1 129 <i>elemento6</i>	Casa 2 18 <i>elemento4</i>	Casa 3 147 <i>elemento1</i>	Casa 4 101 <i>elemento15</i>	Casa 5 133 <i>elemento13</i>	Casa 6 102 <i>elemento5</i>	Casa 7 129 <i>elemento16</i>
Casa 8 92 <i>elemento14</i>	Casa 9 90 <i>elemento10</i>	Casa 10 26 <i>elemento3</i>	Casa 11 107 <i>elemento12</i>	Casa 12 109 <i>elemento9</i>	Casa 13 93 <i>elemento2</i>	Casa 14 97 <i>elemento11</i>	Casa 15 107 <i>elemento8</i>

Fonte: Elaborada pela própria autora

Desta forma o *hash* do conjunto *A*, será o vetor:

$$A_{hash} = [98 \ 129 \ 18 \ 147 \ 101 \ 133 \ 102 \ 129 \ 92 \ 90 \ 26 \ 107 \ 109 \ 93 \ 97 \ 107].$$

No caso descrito todos os elementos da matriz *A* ocuparam a tabela que forma o *hash*, mas isso nem sempre é possível, por exemplo, considere a matriz *A* dada a seguir.

$$A = \begin{bmatrix} 1 & 2 & 4 \\ \text{elemento1} & \text{elemento1} & \text{elemento1} \\ 0 & 5 & 6 \\ \text{elemento1} & \text{elemento1} & \text{elemento1} \\ 8 & 9 & -1 \\ \text{elemento1} & \text{elemento1} & \text{elemento1} \\ -3 & -4 & -5 \\ \text{elemento1} & \text{elemento1} & \text{elemento1} \end{bmatrix}_{4 \times 3} \quad (20)$$

Elemento 1, casa 1; Elemento 2, casa 2; Elemento 3, casa 3; Elemento 4, casa 0;
 Elemento 5, casa 5; Elemento 6, casa 6; Elemento 7, casa 0; Elemento 8, casa 1;
 Elemento 9, casa 7; Elemento 10, casa 5; Elemento 11, casa 4; Elemento 12, casa 3;

A Tabela 13 a seguir ilustra a colocação de cada elemento nas casas correspondentes.

Tabela 13 - Tabela *hash* preenchida pelos elementos da matriz $A_{4 \times 3}$.

Casa 0	Casa 1	Casa 2	Casa 3	Casa 4	Casa 5	Casa 6	Casa 7
0 <i>elemento4</i>	1 <i>elemento1</i>	2 <i>elemento2</i>	3 <i>elemento3</i>	9 <i>elemento8</i>	5 <i>elemento5</i>	6 <i>elemento6</i>	8 <i>elemento7</i>

Fonte: Elaborada pela própria autora

Desta forma o *hash* do conjunto A , será o vetor:

$$A_{hash} = [0 \ 1 \ 2 \ 3 \ 9 \ 5 \ 6 \ 8]$$

A forma de se evitar colisões ilustradas anteriormente é chamada de *linear probing* (ROCHA; RODRIGUES; TADDEO, 2006). Este tipo de resolução de colisões é muito parecido com a resolução do tipo encadeamento separado só que neste caso todos os valores são introduzidos na própria tabela de *hash* sem a utilização dessa estrutura de dados adicionais. Para este tipo de resolução de colisões a tabela de *hash* deverá ter dois tipos de dados. Esses tipos de dados são:

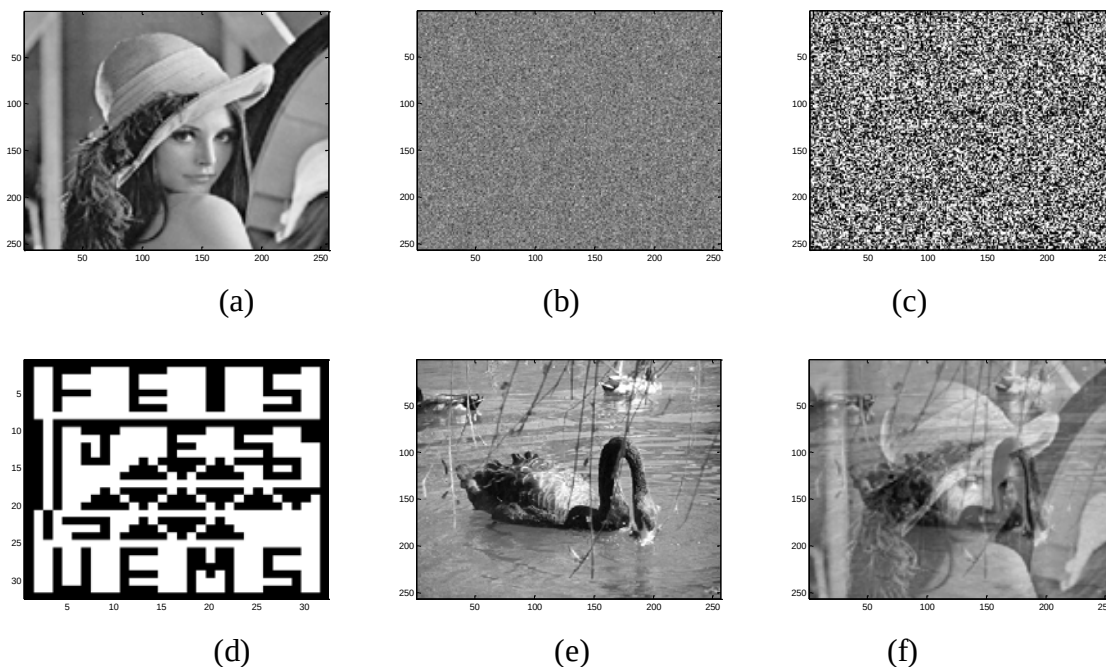
- Qualquer tipo predefinido (inteiros, caracteres, decimais);
- Ponteiros.

3 MÉTODOS DE INSERÇÃO E EXTRAÇÃO DE MARCA D'ÁGUA

A inserção de uma marca d'água implica que o arquivo onde se esta inserindo a marca seja alterado. No caso de imagens, os pixels da imagem serão alterados. O que se almeja com os sistemas de marcas d'água invisíveis é que estas alterações nos pixels da imagem não sejam perceptíveis ao sistema visual humano (HVS), isto é, a imagem marcada seja visualmente igual à imagem original. Este processo é possível decorrente do fato de que o sistema visual humano tem menor sensibilidade para detectar variações de cor do que variações de luminância (GONZÁLES; WOODS; EDDINS, 2009).

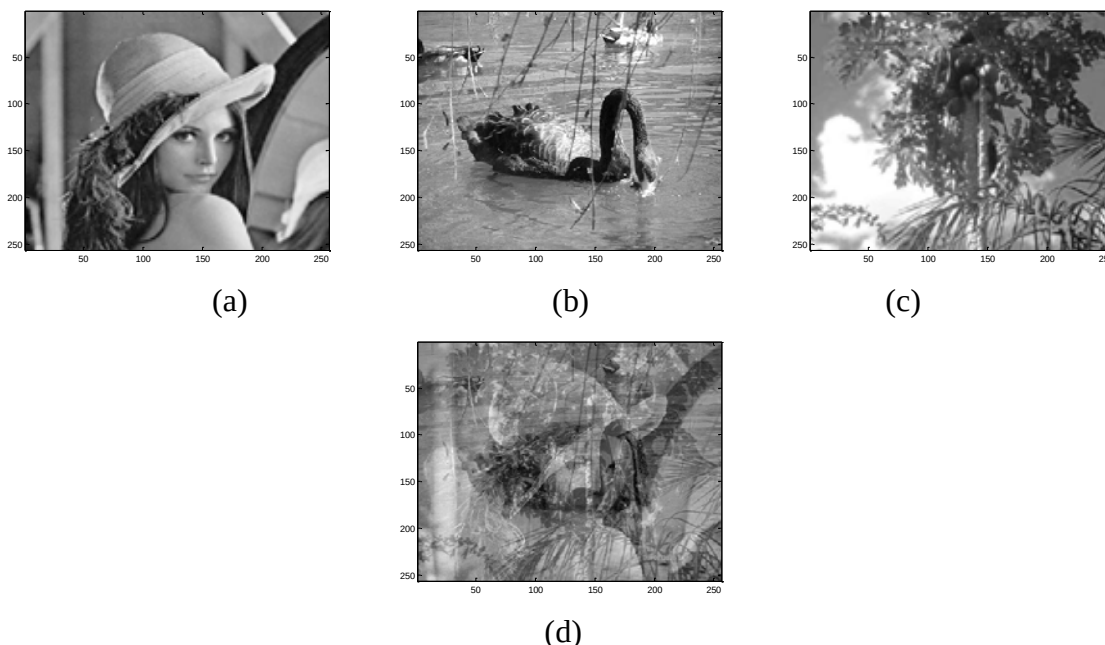
Pode se usar vários tipos de marcas d'água digitais em um único documento como é ilustrado na Figura 24 ou várias marcas d'água com a mesma característica como ilustra a Figura 25.

Figura 24 - Inserção de vários tipos de marca d'água em um único documento; (a) Imagem hospedeira Lenna; (b) Marca d'água aleatória; (c) marca d'água pseudoaleatória; (d) Marca d'água binária; (e) Marca d'água imagem; (f) Imagem marcada com (a), (b), (c), (d) e (e).



Fonte: Elaborada pela própria autora.

Figura 25 - Inserção de vários tipos de marca d'água com a mesma característica em um único documento; (a) Imagem hospedeira Lenna; (b) Marca d'água Cisne; (c) Marca d'água Cass; (d) Imagem marcada com (b) e (c).



Fonte: Elaborada pela própria autora.

Porém, tal esquema precisa de algoritmos sofisticados para maior controle de inserção e recuperação do documento original, principalmente quando se tratar de marcas d'água frágeis.

Ao trabalhar com uma marca d'água numa imagem digital deve-se ter bem definidos os processos de inserção, extração e verificação que, respectivamente, consistem como a marca d'água será inserida na imagem, como ela será extraída e a forma de verificar se realmente a marca extraída é a mesma que foi inserida.

3.1 Métodos de inserção

Existem várias maneiras para inserir uma marca d'água numa imagem digital (LOPES et al., 2004). Assim como em qualquer outro tipo de processamento é importante que o processo não provoque a mínima alteração possível na imagem. Para tanto, uma marca d'água perceptível deve ser inserida em locais que não possuam muitas informações de modo que a imagem não seja poluída com a informação, contando que, esse tipo de marca, possa não sofrer ataques de recorte.

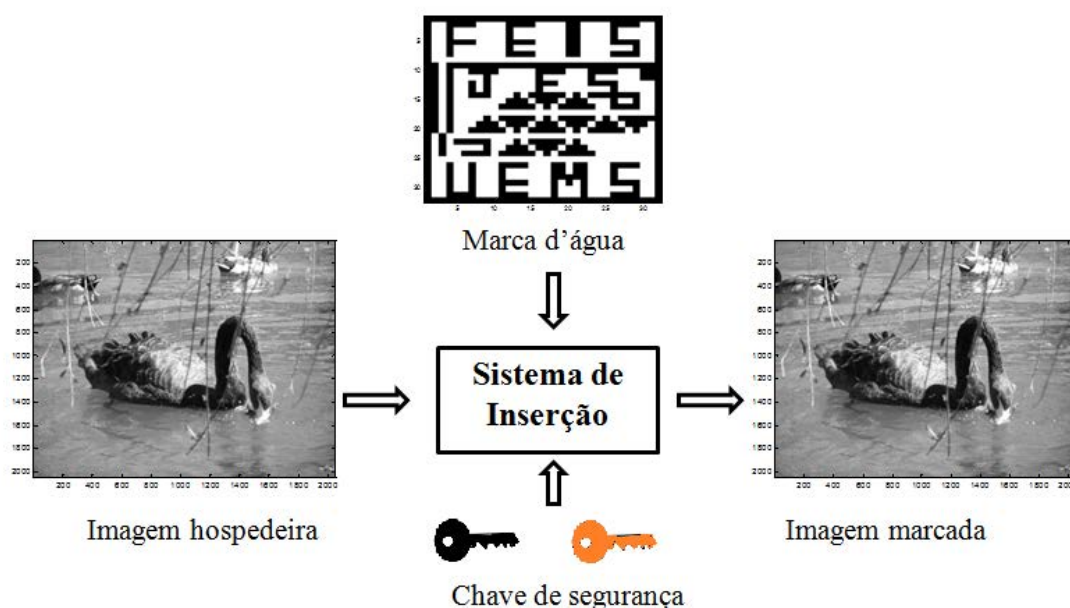
As marcas d'água imperceptíveis também devem ser inseridas em regiões que não comprometem uma análise precisa. Embora, visualmente essas não apareçam, mas as mesmas

podem comprometer um estudo do ponto de vista de frequência ou estatístico da imagem. As regiões onde a marca d'água podem ser inseridas são identificadas por ferramentas que apresentam características que satisfaçam as condições de processamento, dentre as quais está a Transformada Wavelet (SANS, 2008).

Por se tratar de uma ferramenta rica e autêntica, o uso da Transformada Wavelet permite analisar, de forma precisa, as informações contidas em imagens digitais. O seu uso não se limita apenas ao tratamento de imagens, mas também em diversas áreas do processamento de sinais (MARQUES FILHO; VIEIRA NETO, 1999).

O sistema de inserção precisa receber, como entrada, a imagem hospedeira, a marca d'água e a chave de segurança que pode ser pública ou privada. A resposta do processamento será, por exemplo, a imagem marcada conforme ilustrado na Figura 26.

Figura 26 - Representação esquemática do sistema de inserção de marca d'água.



Fonte: Elaborada pela própria autora.

3.2 Métodos de extração

Os métodos de extração são métodos baseados na extração de informações que a imagem hospedeira carrega, neste caso a marca d'água. Os métodos de extração são classificados como cego, semicego ou não-cego.

Método cego: não requer a imagem original nem a marca d'água inserida. O objetivo é retirar a marca d'água da imagem hospedeira sem saber onde ela se localiza ou como ela é.

Método semicego: não requer a imagem original, mas sim a marca d'água inserida para que a mesma seja comparada com a extraída.

Método não-cego: requer a marca d'água inserida e a imagem original, isso porque será necessário o arquivo original para achar pistas de onde se localiza a marca dentro do arquivo marcado ou apenas responder se o arquivo contém a marca d'água.

O método de recuperação a ser empregado depende do tipo de marca d'água usada e da finalidade da aplicação. Por isso, não é possível dizer qual é o mais robusto, pois sua robustez dependerá da aplicação (LOPES et al., 2004).

3.3 Métodos de verificação

Em conjunto com os métodos de extração, são utilizados algoritmos de verificação baseados em chaves de segurança para comprovar as informações que a marca d'água carrega. Esses métodos podem ser de caráter público ou privado. A marca d'água digital será considerada pública se a técnica adotada para recuperá-la é de conhecimento público. Caso não seja de conhecimento público, a marca d'água digital é considerada privada e sua recuperação será praticamente impossível sem autorização (CHIRIGATI; KIKUCHI; GOMES, 2009).

Praticamente todas as marcas d'água que exigem um método de recuperação não-cego são naturalmente privadas, pois espera-se que somente os autores dos documentos originais possam recuperá-las. Os algoritmos de detecção privados requer o compartilhamento de chaves secretas. A mesma chave que é utilizada na inserção também é utilizada na detecção da marca d'água, de forma que a capacidade de verificação da marca d'água privada está associada à capacidade de produzir outras marcas d'água em seu nome. Deste modo, as marcas d'água, cujos algoritmos de detecção são privados, ficam sujeitas aos problemas do compartilhamento de chaves. Porém, são mais simples e eficientes do que os públicos.

3.4 Algoritmo Wong

Ping Wah Wong é um dos pioneiros na utilização de técnicas de assinatura digital para a obtenção de marcas d'água (WONG, 1998). O método de Wong para inserção de marcas

d'água numa imagem em níveis de cinza, usando chave pública, pode ser sumarizado conforme descrito nos dois itens a seguir.

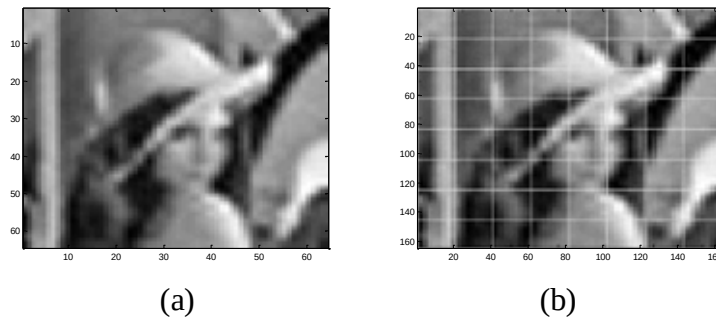
3.4.1 Inserção

Passo1: Seja $J_{M \times N}$ a representação de uma imagem em que se deseja inserir uma marca d'água. Particiona-se $J_{M \times N}$ em n blocos J_t ($0 < t < n$) de tamanho máximo 8×8 pixels (os blocos das bordas podem ser menores). Caso a imagem seja quadrada de dimensão M , o número de blocos será dado pela Equação 21.

$$n = \left(\frac{M}{8} \right)^2 \quad (21)$$

Cada bloco será chamado de J_t e será marcado separadamente. A Figura 27 ilustra uma divisão de blocos de uma imagem relativamente pequena com dimensão 64×64 pixels, apresentando um total de 64 blocos a serem marcados.

Figura 27 - (a) Imagem original 64×64 pixels; (b) Imagem dividida em 64 blocos de dimensão 8×8 pixels.



Fonte: Elaborada pela própria autora.

Passo 2: Seja MA uma imagem binária visualmente significativa a ser usada como base da marca d'água. Esta imagem é replicada periodicamente ou redimensionada para obter uma imagem grande o bastante para cobrir $J_{M \times N}$ inteiramente. Para cada bloco J_t haverá um bloco binário correspondente MA_t . Para determinar quantas vezes a marca d'água será replicada usa-se a Equação 22. A Figura 28 ilustra a marca d'água 32×32 pixels replicada de acordo com a Equação 22.

$$marca_replicada = \left(\frac{nN^2}{M^2} \right) \quad (22)$$

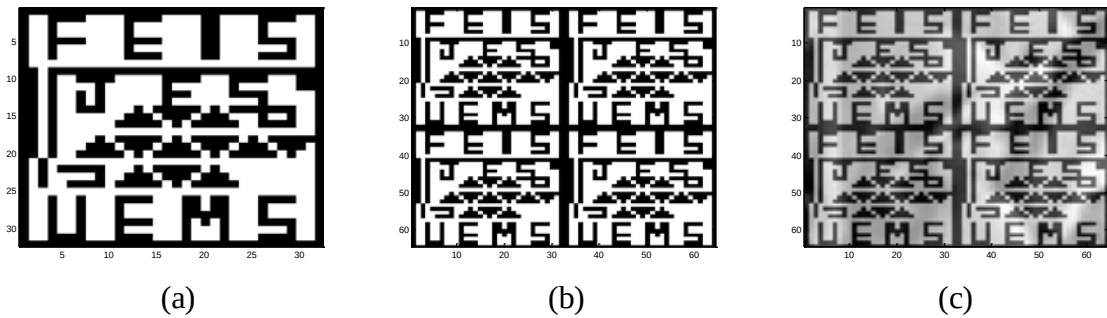
onde

n : número de blocos;

N : dimensão dos blocos;

M : dimensão da marca d'água.

Figura 28 - (a) Marca d'água 32×32 pixels; (b) Marca d'água replicada; (c) Imagem hospedeira representada por 64 blocos marcados por (b).



Fonte: Elaborada pela própria autora.

Passo 3: Usando uma função *hash* criptograficamente segura H , calcula-se o código de integridade dado pela Equação 23.

$$H_{M \times N} = H(M, N, J_t^*) \quad (23)$$

onde

H : função *hash*

N : dimensão dos blocos;

M : dimensão da marca d'água.

J_t^* : Blocos criptografados.

Passo 4: Calcula-se o ou-exclusivo (operação de subtração ou adição binária) de H_t com o bloco MA_t , obtendo-se o código marcado $\hat{H}_t$.

onde

H_t : código marcado.

MA_t : Bloco

$\hat{H}_t$: novo bloco marcado.

Passo 5: Criptografa-se $\hat{H}_t$ com a chave privada CPR (*Chave PRivada*), gerando, assim, a assinatura digital representada pela Equação 24.

$$ASS_t = E_{CPR}(\hat{H}_t) \quad (24)$$

ASS_t : assinatura digital.

E_{CPR} : assinatura digital.

$\hat{H}_t$: bloco criptografado.

Passo 6: Insere-se ASS_t nos bits menos significativos dos pixels de I_t^* , obtendo-se o bloco marcado:

$$B_t = I_t^* \oplus ASS_t \quad (25)$$

ASS_t : assinatura digital.

I_t^* : bloco criptografado.

B_t : novo bloco.

3.4.2 Extração e verificação

O algoritmo para extração e verificação é descrito a seguir:

Passo 1; Seja $IM_{M \times N}$ uma imagem marcada. Particiona-se esta imagem em n blocos B_t , como em 2.4.1.

Passo 2: Usando a mesma função de *hash* H escolhida para a inserção da marca d'água, calcula-se o índice de integridade dado pela Equação 26:

$$H_t = H(M, N, X_t^*) \quad (26)$$

Passo 3: Extrai-se o conteúdo do nível da marca d'água B° de B_t e decifra-se o resultado usando a chave pública do fornecedor da mensagem, obtendo-se o bloco decifrado BD_t .

Passo 4: Calcula-se o ou-exclusivo de H_t com o bloco BD_t , obtendo-se o bloco de verificação BV_t . Se BV_t e ASS_t forem iguais, declara-se autêntica a imagem marcada. Caso contrário, declara-se que a imagem marcada IM foi alterada no bloco B_t .

3.5 Possíveis ataques aplicados em imagens autenticadas por marca d'água

O aumento de usuários que movimentam as redes de comunicação, seja esse meio de comunicação a internet ou um banco de dados, fez com que crescessem também os tipos de ataque às imagens disponíveis nesses meios, o que as tornam alvo preferido dos falsificadores.

Desta forma, o direito à imagem ou a própria imagem tem adquirido extrema importância com a rápida evolução tecnológica nos meios de comunicação. Um modo de coibir qualquer fraude ou manipulação indevida numa imagem é a técnica da inserção de marca d'água, que é considerada basicamente como um código identificador.

Assim, como qualquer outro modo de segurança, uma imagem com marca d'água fica exposta a ataques que podem extrair a marca, modificá-la, ou ainda danificá-la. Um ataque é visto como qualquer processamento na imagem marcada que pode prejudicar a detecção ou extração da marca d'água.

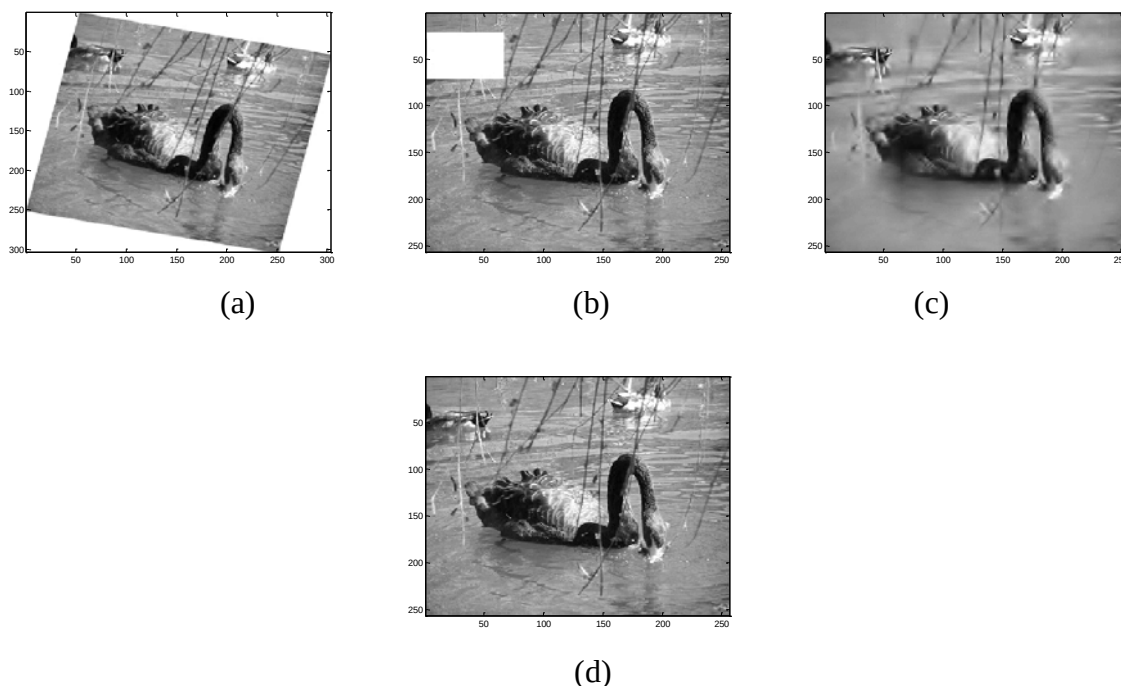
Esses ataques procuram driblar o receptor da imagem durante a extração da marca d'água provocando ilusão de que uma determinada imagem não possua uma marca d'água ou que a marca d'água inserida possui outro proprietário.

Existem várias modalidades de ataques (MENDES, 2008). Por isso, um fator importante para garantir a eficácia de um método de autenticação de imagens digitais, por meio de marca d'água, é conhecer os ataques existentes, pois este é um requisito que ajudará nas fases do desenvolvimento e avaliação dos métodos de autenticação de imagens. Dentre os ataques mais comuns estão: rotação, adição de ruído, recorte, aplicação de algum tipo de filtro e compressão, como ilustra a Figura 29.

Um ataque planejado poderá modificar o conteúdo digital e adulterar a imagem sem prejudicar a marca d'água de forma que o receptor reconheça a imagem adulterada como sendo autêntica. Ou ainda, fazer o mascaramento da região em que uma determinada marca d'água é inserida em outras imagens transmitidas ao receptor de modo que o servidor seja adulterado.

Para evitar um ataque, como por exemplo, o de substituir parte de uma imagem por outra, a marca d'água é inserida tendo a capacidade de indicar as regiões danificadas da imagem adulterada. Algumas técnicas de extração de marcas d'água detectam rapidamente alterações aleatórias, mas falham ao detectar uma modificação cuidadosamente projetada (BARRETO, 2003).

Figura 29 - (a) Ataque de rotação; (b) Ataque de recorte; (c) Ataque de filtro; (d) Ataque de ruído.



Fonte: Elaborada pela própria autora.

É extremamente difícil desenvolver um método de inserção e extração com uma marca d'água segura contra todos os tipos de ataques por causa da dificuldade de lidar com todas as características de uma marca d'água, mesmo porque a maioria dos algoritmos de marca d'água concentra-se em apenas alguns requisitos, sendo possível sua aplicação em uma gama restrita de circunstâncias.

O problema está no fato de que algumas operações em imagens ora são exigidas, ora são proibidas (BARRETO, 2003). Portanto, o uso de alguns métodos de processamento depende de sua aplicabilidade, o que não impede a realização de um bom processamento, disponibilizando de ferramentas que possibilitem analisar as características da imagem original de modo que a marca d'água inserida provoque o mínimo de distorção na imagem a ser processada, além de procurar aperfeiçoar a complexidade computacional.

A complexidade computacional é um dos requisitos mais importantes para atender a tecnologia atual oferecida, por causa do grande número de arquivos digitais que são transmitidos e armazenados via internet ou via banco de dados. Os tipos de ataques são visuais, estruturais e estatísticos.

3.5.1 Ataques visuais

São ataques baseados na inspeção visual do arquivo, de modo a encontrar falhas. Por exemplo, um algoritmo de esteganografia pode fazer com que uma imagem tenha mudanças perceptíveis nas cores, o que colabora para uma fácil inspeção visual. O uso desses ataques visuais pode ser suficiente para perceber que há alguma mensagem escondida.

3.5.2 Ataques estruturais

Ataques estruturais buscam identificar mudanças na estrutura dos arquivos que sugerem algum tipo de manipulação, por exemplo, esconder informações em imagens do formato GIF ou PNG. Usando o método do bit menos significativo pode não ser eficiente, já que as cores parecidas geralmente não estão próximas umas das outras nas palhetas de cores (CHIRIGATI; KIKUCHI; GOMES, 2009). Assim, a mudança de um bit pode alterar da cor de azul escuro para rosa claro, o que deixa a mudança perceptível.

Uma maneira de resolver esse problema é escolher uma palheta menor e, então, duplicar as cores que podem ser usadas para esconder uma mensagem. Dessa forma, uma mudança em um bit menos significativo não altera drasticamente a cor daquele pixel. Porém, essas palhetas são mais fáceis de serem detectadas, levando o esteganalista a perceber que há alguma informação por trás da imagem (CHIRIGATI; KIKUCHI; GOMES, 2009).

Outra maneira de resolver esse problema é simplesmente alterar a ordem das cores, para que as similares fiquem próximas umas das outras. Contudo, essa técnica também pode ser detectada se o método de reordenação é conhecido ou fácil de ser identificado. Além dessas mudanças estruturais, os esteganalistas podem usar testes estatísticos para verificar a existência de informações escondidas.

3.5.3 Ataques estatísticos

Atualmente, muitos estudos vêm sendo realizados, buscando-se métodos estatísticos cada vez mais eficientes para arquivos de áudio (ÖZER et al., 2003) e imagens (FARID, 2001). As chamadas estatísticas de primeira ordem, como o teste do chi-quadrado, podem ser utilizadas para medir a quantidade de redundância e distorção de um arquivo (KESSLER, 2004).

No que diz respeito a imagens, é possível medir o número de pares de cores próximas, as quais diferem no máximo de uma unidade em cada um dos componentes vermelho, verde e azul. Arquivos que são construídos naturalmente possuem uma quantidade muito menor desses pares do que aqueles que foram usados para esconder alguma mensagem, já que aproximar cores similares elimina possíveis mudanças drásticas no arquivo (WAYNER, 2002).

Realizar estatísticas baseadas nessa quantidade pode-se tornar um excelente indicador. Uma melhoria no processo pode ser obtida calculando-se a ordem em que esses pares aparecem, pois eles possuem igual frequência de ocorrência em imagens que possuem uma informação escondida, diferentemente do que acontece em imagens naturais.

É importante ressaltar que as melhores técnicas de esteganálise são aquelas direcionadas especificamente a determinados algoritmos (WAYNER, 2002). Quando se sabe qual *software* foi utilizado para realizar a esteganografia, o esteganalista consegue ter uma melhor análise do processo. Soluções mais gerais possuem muito menos eficácia que as específicas.

3.6 Ataques à marca d'água

Os métodos de inserção e extração de marca d'água formam uma área de pesquisa extremamente ativa e novas técnicas aparecem com grande frequência. Para demonstrar os principais tipos de processamento na imagem marcada que podem prejudicar a detecção ou extração da marca d'água é preciso que sejam aplicados ataques em algumas dessas técnicas.

Por Wong (WONG, 1998,1998) ter sido um dos pioneiros na inserção de marca d'água, o seu método de inserção e extração será testado por meio de ataques, sendo assim apontadas algumas fraquezas criptográficas do mesmo (BARRETO, 2003).

3.6.1 Ataque recortar e colar e ataque de falsificação

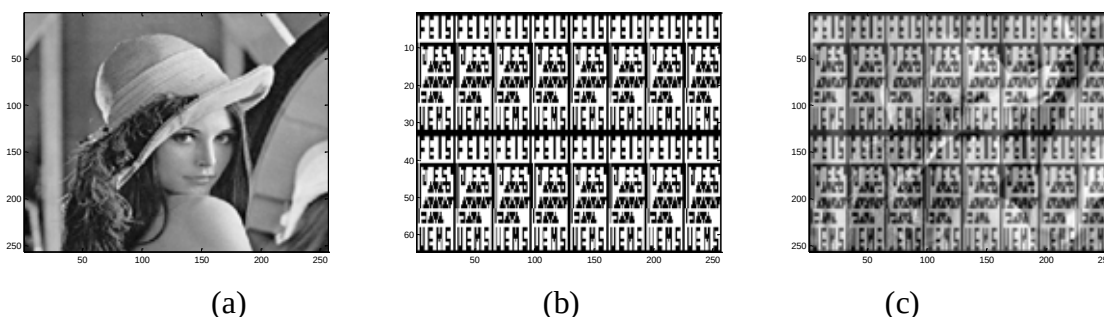
O ataque de recortar é muito aplicado em imagens que possuem uma marca d'água visível, que não é o foco desse trabalho. Para exemplificar um ataque desse tipo, tem-se como exemplo uma imagem na qual a marca d'água é inserida em um dos cantos. Facilmente, uma operação de recorte poderá retirá-la. Porém, se tal marca é inserida no centro da imagem, o recorte inutilizará a imagem hospedeira, já que sua qualidade visual será prejudicada.

Esse exemplo mostra a importância na escolha do local da inserção da marca, independente de ser uma marca d'água perceptível ou imperceptível. Além disso, a marca

d'água não pode prejudicar visualmente a imagem hospedeira. Porém, deve dificultar qualquer ataque, como é o caso de recorte.

Já o ataque de recortar e colar, em meio aos diversos tipos de ataques, é considerado simples e indetectável pelo esquema de Wong (WONG, 1998; WONG; MENON, 2001), porém pode ser utilizado com intenções de prejudicar a imagem marcada ou a marca d'água inserida. A Figura 30 ilustra o esquema de inserção de marca d'água pelo método Wong.

Figura 30 - (a) Imagem hospedeira Lenna 256×256 pixels; (b) Marca d'água 32×32 pixels replicada; (c) Imagem marcada pelo método Wong.



Fonte: Elaborada pela própria autora.

Na Figura 31, a ilustração (c) é considerada um conjunto de 256 imagens, todas elas com dimensão 8×8 pixels e marcadas separadamente com a marca d'água replicada. Para realizar tal marcação, a única informação sobre a imagem a ser marcada como ilustrada em (a), foi sobre a sua dimensão, já que a imagem hospedeira para ser marcada de acordo com método de Wong deverá ser dividida em n blocos de dimensão 8×8 pixels.

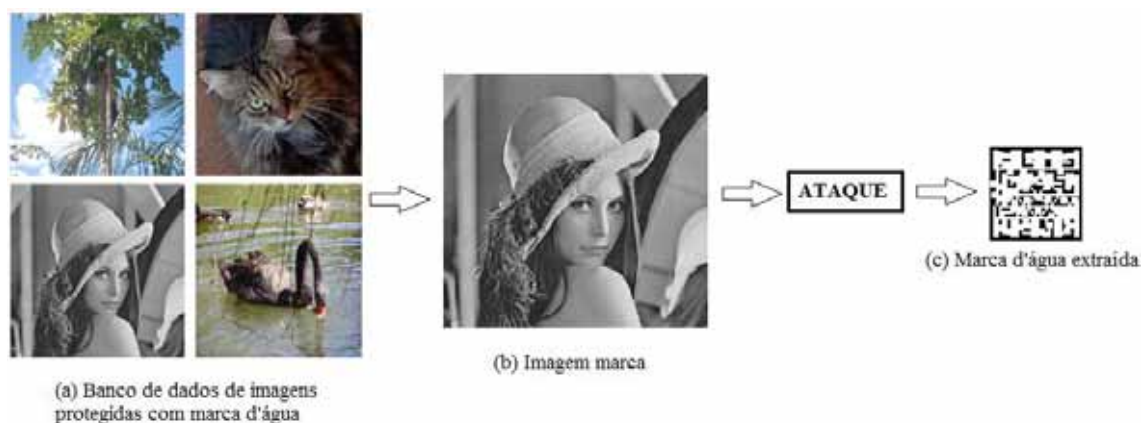
Um ataque de recortar e colar pode ser efetuado selecionando um dos 256 blocos da imagem (a) e construindo com ele uma nova imagem cuja marca d'água será falsamente verificada como legítima pelo método Wong.

Outro ataque, visando os blocos, poderá ser feito de outro modo. Por exemplo, tornando-se uma imagem a qual se deseja marcar com uma marca d'água autêntica que foi inserida em outras imagens disponíveis num banco de dados. A imagem será falsificada, ou seja, será marcada com uma marca d'água autêntica como as inseridas nas demais imagens disponíveis no banco de dados, porém não é uma imagem legítima do banco de dados a ser fraudado.

Para realizar esse ataque de falsificação é preciso que se tenha uma noção de como é a marca d'água inserida nas demais imagens. Para tanto, basta aplicar outro tipo de ataque com objetivo de extrair a marca d'água, sabendo-se que o resultado da operação não será a marca

d'água fielmente original à inserida, mas sim uma marca d'água provavelmente parecida com a autêntica.

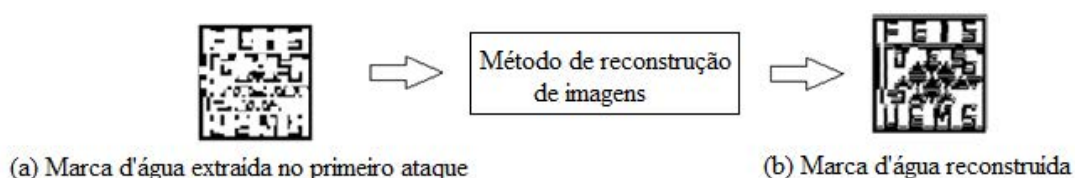
Figura 31 - Ataque a um banco de dados.



Fonte: Elaborada pela própria autora.

No segundo passo, a Figura 31 (c) poderá ser construída como sendo uma aproximação da marca d'água autêntica, para isso basta aplicar algum algoritmo baseado em reconstrução como ilustrado na Figura 32.

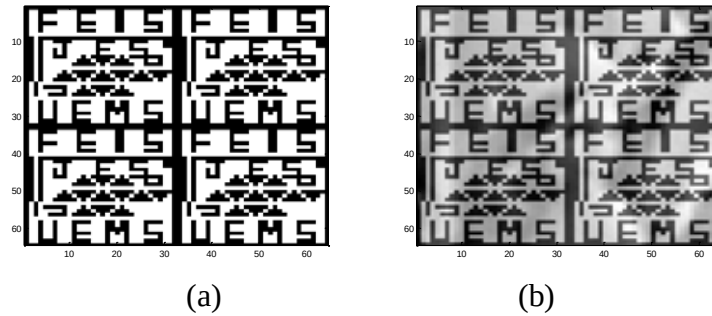
Figura 32 - Reconstrução da marca d'água.



Fonte: Elaboração da própria autora.

A mesma operação de inserção de marca d'água autêntica pelo método Wong é feita com a marca d'água reconstruída nos blocos da imagem a ser falsificada, conforme ilustra a Figura 33.

Figura 33 - (a) Marca d'água 32×32 pixels reconstruída; (b) Imagem marcada.

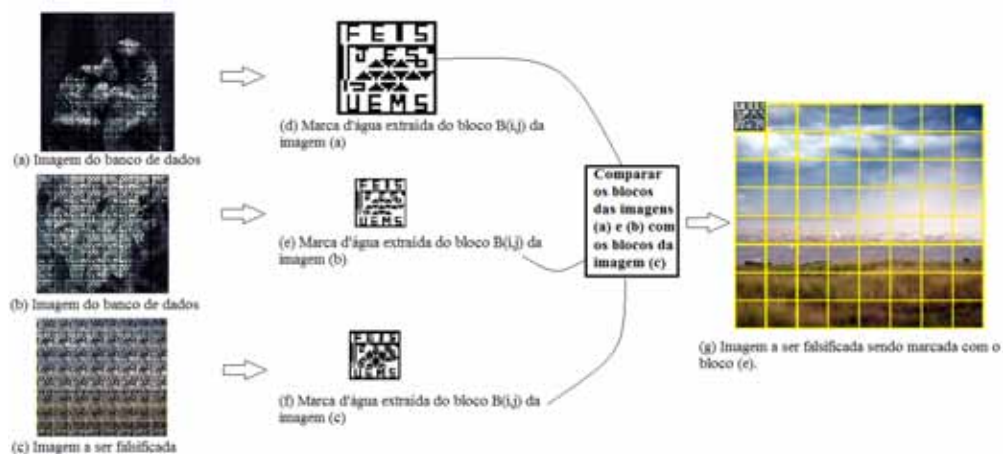


Fonte: Elaborada pela própria autora.

A Figura 33 (b) possui 64 blocos marcados. O próximo passo é realizar uma busca entre cada bloco que compõe o banco de dados, e compará-los um a um com os blocos na ilustração (c) da Figura 34, por exemplo, o bloco B_{11} da Figura 34 (c) será comparado com todos os blocos B_{11} da Figura 34 (a), (b) e (c) composta no banco de dados, obtendo assim novos blocos.

Os mais parecidos com as imagens do banco de dados são substituídos e inseridos na imagem (b) da Figura 34. Repetindo este processo para todos os blocos da Figura 34 (c), uma imagem será marcada com uma marca d'água válida. Este ataque pode ser aplicado com sucesso, mesmo usando um banco de dados relativamente pequeno.

Figura 34 - Comparação dos blocos das imagens.



Fonte: Elaborada pela própria autora.

Todos os blocos das imagens do banco de dados são comparados com os respectivos blocos da imagem a ser falsificada, isso porque vários fatores podem prejudicar o

desempenho do ataque, um deles é que nem sempre as imagens que compõem o banco de dados apresentam a mesma dimensão da imagem a ser falsificada.

Por exemplo, uma imagem de 256×256 pixels terá um número de blocos bem maior do que uma de 128×128 pixels. Além do mais, as imagens marcadas podem estar divididas em blocos de diferentes dimensões, podendo uma imagem de 256×256 pixels estar dividida em blocos de 8×8 pixels ou em blocos de 16×16 pixels, não podendo, por exemplo, ser usado o algoritmo de Wong.

Outra alternativa seria testar apenas as imagens com a mesma dimensão da imagem a ser falsificada, economizando assim o tempo na comparação, mas essa saída reincide no fato de que num banco de dados as imagens são de diversas dimensões.

3.6.2 Ataque ruidoso

Geralmente, a maioria das imagens contém uma degradação natural causada pelo ruído gaussiano devido ao meio em que foi gerada ou transmitida. Esse ruído pode prejudicar a qualidade visual da imagem ou não, e, para lidar com tais ruídos prejudiciais à qualidade da imagem, é atribuído o uso de filtros que visam eliminar tais informações indesejadas. Existem inúmeras pesquisas voltas para eliminação de ruído em imagens digitais e outros sinais envolvendo modelos matemáticos que têm apresentado soluções satisfatórias na resolução de eventuais problemas (D'IPPÓLITO, 2005; SOARES, 2009).

O ruído, além de ser um componente, às vezes natural numa imagem, pode também ser usado como uma arma no ataque a imagens protegidas por marca d'água e, então, ser inserido de modo proposital para que a marca d'água seja danificada. Mesmo a marca d'água binária apresenta as mesmas características computacionais de uma imagem qualquer. Ao inserir a marca d'água numa imagem, ambas absorverão as informações ruidosas que são adicionadas.

Como a absorção é em ambas as partes, tanto pela imagem hospedeira como pela marca d'água, o processamento de redução de ruído a ser aplicado não irá tratar separadamente as três informações embutidas no arquivo que são a imagem hospedeira, a marca d'água e o ruído, então os três componentes estão sujeitos à perda de informações. Dependendo do ruído adicionado e do filtro aplicado, a qualidade visual da imagem hospedeira será comprometida assim como a marca d'água. E, num processo de extração da marca d'água poderá fornecer como saída uma marca d'água não autêntica à inserida.

3.6.3 Ataque de compressão

O processo de compressão de dados age no arquivo de modo a converter informações com a finalidade de reduzir o tamanho da informação original para facilitar o armazenamento e para melhorar a velocidade de transmissão dessas informações. Existe uma variedade de métodos para compressão para vários tipos de dados, sejam eles textos, imagens ou áudio (MARQUES FILHO; VIEIRA NETO, 1999).

Os métodos de compressão de imagens têm o princípio de remover as redundâncias da informação original que a imagem carrega (SILVA, 2008). Caso a imagem apresente uma dimensão muito pequena, corre-se o risco de perda de informações. Como, usualmente, a marca d'água apresenta esta característica, ela provavelmente será alvo fácil na eliminação de redundâncias. Por esse motivo, mesmo sendo um tratamento usual que normalmente as imagens recebem, a compressão se encaixa como sendo um tipo de ataque, pois é provável a perda de informação tanto na imagem hospedeira quanto na marca d'água inserida (PAMBOUKIAN, 2007).

A compressão de imagens tem como objetivo principal a redução do máximo possível de dados de uma imagem para, então, realizar uma possível transmissão da mesma. Com o mesmo intuito, as técnicas de marcas d'água são implementadas por técnicas de compressão de dados, possibilitando, deste modo, que uma quantidade maior de dados, mesmo sendo ocultos, possa ser introduzida no processo.

A grande questão é que há aplicações que exigem marcas d'água frágeis ou semifrágeis que não resistem a alterações mínimas, mesmo que seja uma compressão JPEG (PAMBOUKIAN, 2007). A marca d'água a ser inserida numa imagem que futuramente será comprimida e transmitida num canal de comunicação deverá ser uma marca d'água robusta.

4 TRANSFORMADA WAVELET

Na área de processamento de sinais existem várias técnicas voltadas para aplicações em imagens, dentre essas técnicas está a transformada wavelet (STOLLNITS; DEROSE; SALESIN, 1996). Ao tratar de inserção de imagens, a transformada wavelet tem apresentado um ótimo desempenho quando comparado com outras técnicas encontradas na literatura especializada (DUARTE; SILVA; VILLARREAL, 2011). Neste capítulo, serão apresentadas as propriedades e as características responsáveis por fazerem da transformada wavelet uma ferramenta essencial ao processamento digital de imagens, inclusive na inserção e extração de marca d'água.

4.1 Transformada Wavelet Discreta

A Transformada Wavelet Discreta (DWT) pode ser vista como uma técnica de janelamento instantânea, o que corresponde a uma filtragem (DAUBECHIES, 1992), muito útil no processamento de sinais.

A decomposição de um sinal unidimensional pela transformada wavelet discreta é feita através de filtros, cujos coeficientes são extraídos da função wavelet usada como núcleo na transformação (DAUBECHIES, 1992; MALLAT, 1989; MALLAT, 1992).

O sinal de entrada, denotado por $c_0[n]$, é passado por dois filtros: o primeiro, um filtro passa baixa, com resposta ao impulso $h[n]$; e o segundo, um filtro passa alta, com resposta ao impulso $g[n]$. Após a filtragem, os sinais passam por uma dizimação no tempo conhecida como sub-amostragem de ordem 2, gerando a saída $c_1[n]$, que representa as componentes de baixa frequência, e $d_1[n]$, que representa os componentes de alta frequência. Do ponto de vista matemático, $c_1[n]$ contém os chamados coeficientes de aproximação e $d_1[n]$ os coeficientes de detalhes do sinal decomposto pela DWT (RIOL; VETTERLI, 1991).

Considerando que o sinal de entrada é real, as Equações 27 e 28 expressam as relações entre $c_0[n]$, $c_1[n]$ e $d_1[n]$:

$$c_1[k] = \sum_n h[n-2k]c_0[n] \quad (27)$$

$$d_1[k] = \sum_n g[n-2k]d_0[n] \quad (28)$$

sendo

h : resposta ao impulso do filtro passa baixa;

g ; resposta ao impulso do filtro passa alta;

n : número de amostras;

k : deslocamento do filtro ao longo do sinal.

A partir da obtenção dos sinais $c_1[n]$ e $d_1[n]$, são feitas as alterações em seus coeficientes, de acordo com a aplicação em questão. Dentre essas aplicações estão a compressão, a redução de ruído e a codificação.

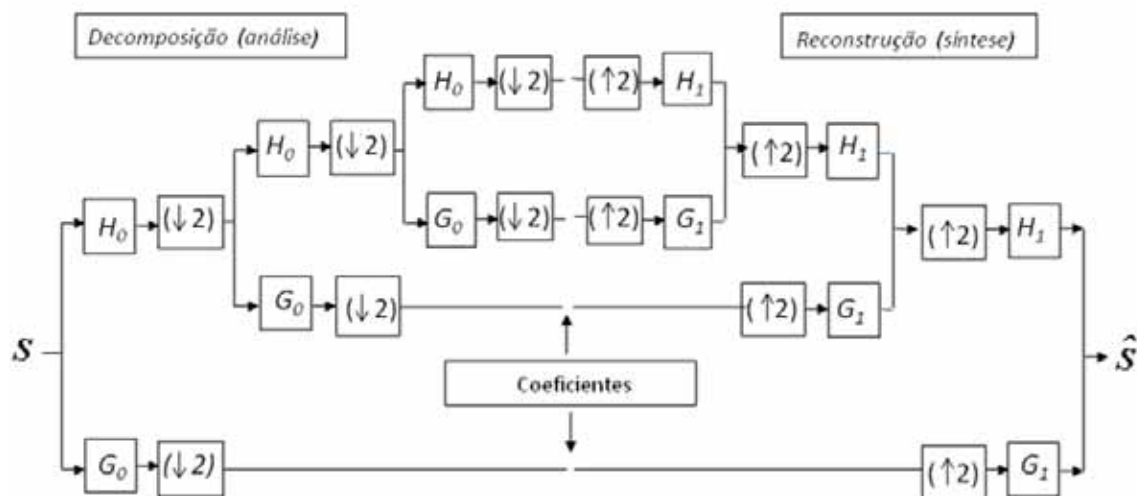
O sinal processado é reconstruído a partir de uma combinação adequada dos sinais $c_1[n]$ e $d_1[n]$, que é denominada de Transformada Wavelet Discreta Inversa (IDWT) (DAUBECHIES, 1992; MALLAT, 1992). Na reconstrução, inicialmente, adiciona-se um zero entre cada par de elementos dos sinais $c_1[n]$ e $d_1[n]$, essa operação representa uma sobre amostragem de ordem 2. Em seguida, são efetuadas as convoluções de $c_1[n]$ com $h[n]$ e de $d_1[n]$ com $g[n]$. O sinal reconstruído é a soma dos resultados das convoluções, conforme expresso na Equação 29 (DAUBECHIE, 1992):

$$c_0[k] = \sum_k h[n-2k]c_1[k] + \sum_k g[n-2k]d_1[k] \quad (29)$$

Para processar um sinal de comprimento N , a decomposição é feita em até $L = \log_2 N$ faixas, com L representando o número máximo de faixas de frequências em que o sinal pode ser decomposto, o que equivale a um banco de filtros (RIOL; VETTERLI, 1991).

Na Figura 35 é apresentada a estrutura em cascata do banco de filtros da transformada wavelet com três níveis de análise e síntese. Se a função wavelet usada como núcleo da DWT for uma função ortogonal, os filtros usados na análise e na síntese são os mesmos, isto é, $H_0 = H_1$ e $G_0 = G_1$, porém com os coeficientes em ordem inversa.

Figura 35 - Representação esquemática da estrutura do banco de filtros da DWT.



Fonte: Rioul e Vetterli (1991).

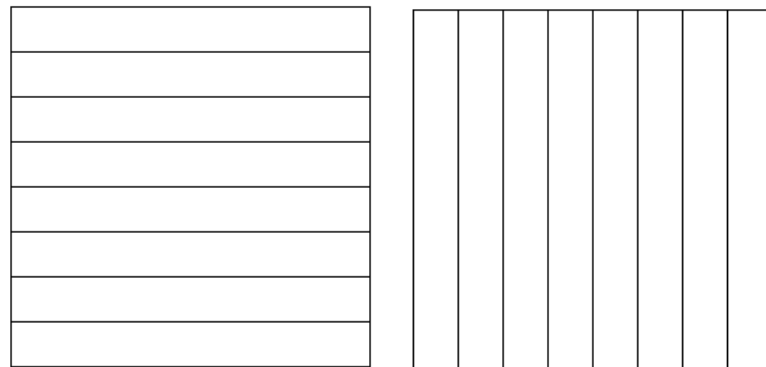
4.2 Transformada Wavelet Discreta Bidimensional

A aplicação da DWT bidimensional numa imagem é feita da mesma maneira que num sinal unidimensional, pois, como a representação discreta de uma imagem é uma matriz, basta aplicar a DWT bidimensional nas linhas ou colunas dessa matriz. Existem duas formas comuns nas quais as wavelets podem ser usadas para transformar os valores dos pixels dentro de uma imagem. Cada uma destas transformações é uma generalização bidimensional da DWT unidimensional (STOLLNITS; DEROSE; SALESIN, 1996).

4.2.1 Decomposição padrão

Para obter a decomposição padrão de uma imagem, aplica-se primeiro a DWT unidimensional a cada linha, representadas pelos blocos na horizontal, de valores de pixels. Esta operação resulta em um valor médio para cada linha. Feito isto, tratam-se estas linhas transformadas como se elas fossem uma imagem, e aplica-se a DWT unidimensional para cada coluna, representadas pelos blocos na vertical. Os valores resultantes são todos os coeficientes de detalhes, exceto por um único coeficiente que representa a média geral, como ilustra a Figura 36.

Figura 36 - Representação esquemática dos estágios de decomposição wavelet bidimensional padrão de uma imagem.

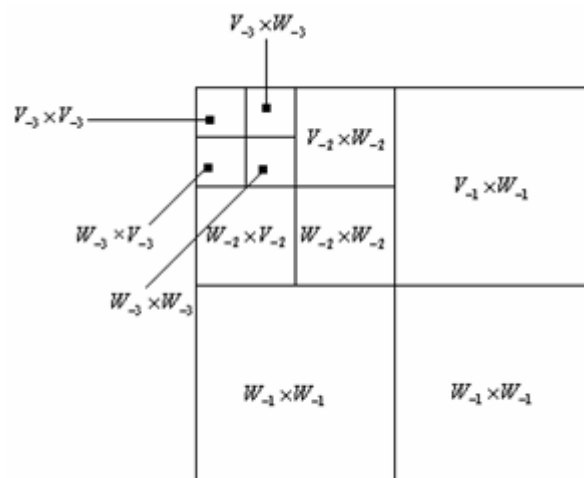


Fonte: Elaborada pela própria autora.

4.2.2 Decomposição não-padrão

Na decomposição não-padrão, são realizadas operações de decomposição alternadas entre linhas e colunas. Primeiro, aplica-se o cálculo da média nos pares horizontais e faz-se a diferença dos valores dos pixels em cada linha da matriz que representa a imagem. Depois, aplica-se o cálculo da média nos pares verticais e encontra-se a diferença para a coluna do resultado. A transformação é completada repetindo-se o processo, recursivamente, apenas no quadrante contendo as médias em ambas as direções, como ilustra a Figura 37.

Figura 37 - Representação esquemática dos estágios de decomposição wavelet bidimensional não-padrão de uma imagem.



Fonte: Elaborada pela própria autora.

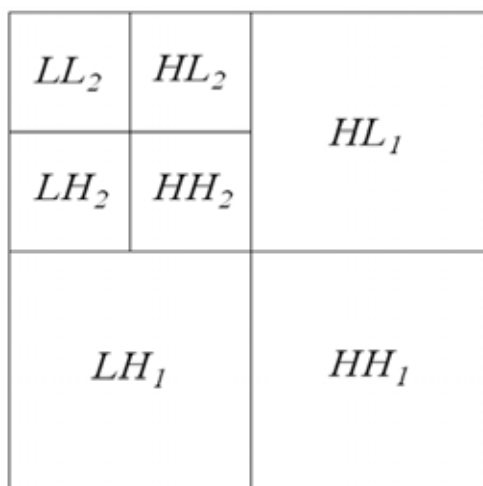
A decomposição não-padrão é mais vantajosa quando se deseja fazer mudanças na matriz, pois ela realiza uma análise de multirresolução na imagem, de acordo com suas faixas de frequências (STOLLNITS; DEROSE; SALESIN, 1996).

Do ponto de vista frequencial, na decomposição não-padrão (também chamada de DWT bidimensional), a imagem é decomposta nas direções horizontal, vertical e diagonal, resultando em uma sub-banda de baixa frequência LL e três sub-bandas de alta frequência HL , LH e HH .

Este mesmo processo é repetido na sub-banda LL para gerar o próximo nível de decomposição. A decomposição pode ser repetida nas sub-bandas LL_k até que $L = \log_2 N$ sendo N a dimensão da imagem, neste caso, trata-se de uma imagem quadrada de $N \times N$ pixels.

O processo de decomposição em sub-bandas de frequências de uma imagem pela DWT bidimensional é ilustrado na Figura 38. Numa imagem decomposta pela DWT bidimensional até o nível L , os coeficientes de detalhes horizontais estão em HL_k , os verticais em LH_k , os detalhes da diagonal estão em HH_k e a sub-banda LL_k é uma aproximação da imagem no nível L .

Figura 38 - Representação esquemática dos estágios de decomposição wavelet bidimensional não-padrão em dois níveis de resolução.



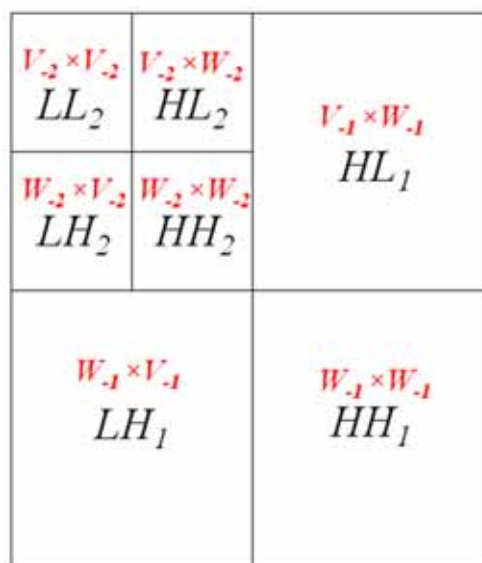
Fonte: Elaborada pela própria autora.

4.3 Inserção de marca d'água no domínio wavelet

A inserção de uma marca d'água numa imagem através da transformada wavelet é feita através da decomposição da imagem a ser marcada por meio da DWT bidimensional até um nível k .

Ao realizar a decomposição da imagem se obtém os coeficientes wavelets organizados em um grupo de sub-bandas de frequências altas e baixas. Na Figura 39 apresenta-se um esboço da hierarquia de sub-bandas de frequência de uma imagem decomposta pela DWT bidimensional até o nível 2.

Figura 39 - Hierarquia de sub-bandas de frequência de uma imagem decomposta pela DWT bidimensional até o nível 2.



Fonte: Elaborada pela própria autora.

As sub-bandas de frequência resultantes da decomposição de uma imagem pela DWT bidimensional possuem as seguintes propriedades:

- quanto menor a escala da sub-banda, menor é a sua energia e maior é a sua resolução em frequência;
- os coeficientes wavelets são maiores nas sub-bandas de menor energia;
- quanto maior o valor do coeficiente wavelet maior será sua importância visual.

4.3.1 Sub-bandas de alta frequência

As sub-bandas de altas frequências contêm detalhes como brilho e contraste. Nestas regiões, os valores correspondentes são modificados para melhorar a visualização e identificação das diferentes sub-bandas de frequências (MARQUES FILHO; VIEIRA NETO, 1999).

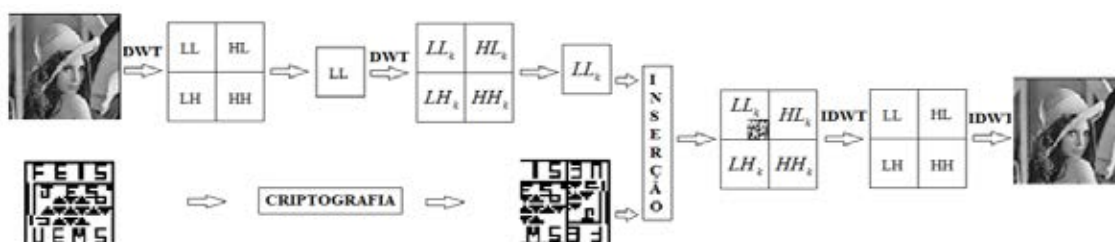
4.3.2 Sub-bandas de baixa frequência

Dentre as sub-bandas de frequências, a mais baixa é LL_k . Em particular, os coeficientes da sub-banda LL possuem algumas características específicas não encontradas nas demais sub-bandas (VALENS, 2004):

- a) contêm a maior parte da energia (forma uma aproximação da imagem original);
- b) são bem preservados quando a imagem passa por algum tipo de processamento como a compressão;
- c) possuem alta capacidade perceptual, o que as caracteriza, como uma aproximação de baixa resolução da imagem original e contêm a maior parte da energia da imagem, o que garante que a inserção de uma marca d'água de robustez razoável não provoque distorções perceptíveis na imagem.

Com alguns testes realizados e de acordo com outros trabalhos (DUARTE; SILVA; VILLARREAL, 2011; SILVA; DUARTE; VILLARREAL, 2013), a sub-banda LL_k não é a única que poderá ser usada para inserir a marca d'água (MENDES, 2008). Alguns fatores como a criptografia empregada e as características digitais da marca d'água podem determinar qual será a melhor sub-banda para a inserção da marca d'água. Na Figura 40 é ilustrado o processo de inserção de marca d'água no domínio wavelet.

Figura 40 - Inserção de marca d'água numa imagem no domínio wavelet.



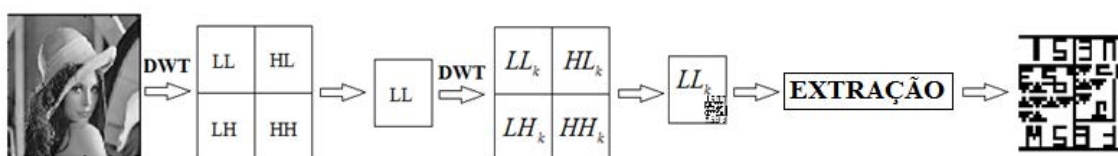
Fonte: Elaborada pela própria autora.

4.4 Extração da marca d'água no domínio wavelet

Para extrair a marca d'água, a DWT bidimensional de nível k é aplicada na imagem marcada, obtendo os coeficientes wavelets. A marca d'água é extraída dos coeficientes wavelets presentes na sub-banda LL_k utilizando um determinado algoritmo de extração.

Dependendo do algoritmo utilizado na inserção da marca d'água será necessária ou não a imagem original. A Figura 41 ilustra o processo de extração da marca d'água utilizando apenas a imagem marcada.

Figura 41 - Extração de marca d'água numa imagem no domínio wavelet.



Fonte: Elaborada pela própria autora.

Com relação ao tempo de processamento, na inserção leva-se sempre mais tempo do que na extração, devido ao fato de que, na inserção é necessário aplicar a IDWT bidimensional para obter a imagem marcada, enquanto que no processo de extração isto não é necessário.

Tanto na comparação de imagens quanto na inserção de dados, faz-se necessária uma boa localização das regiões da imagem que sofrerão a modificação, de modo que a eliminação ou adição de informações não provoque distorções ou alterações bruscas ou perceptíveis ao sistema visual humano (HVS).

A transformada wavelet, por permitir explorar as estruturas coerentes presentes na imagem e por mapear suas grandezas em várias escalas destacando suas principais características, possibilita operações como compressão e também adição de sinais, tais como uma marca d'água sem danificar o seu conteúdo digital. Além disso, a transformada wavelet inversa permite recuperar um sinal decomposto a partir dos coeficientes wavelets. A escolha da wavelet apropriada é extremamente importante para obter uma melhor aproximação ou representação do sinal original (ADDISON, 2002).

Como a imagem é um sinal bidimensional, o algoritmo para calcular a transformada wavelet discreta bidimensional é utilizado tanto na decomposição quanto na reconstrução da imagem original e pode ser aplicado utilizando a decomposição padrão ou a decomposição não-padrão. Desta forma, a imagem original e a imagem marcada por marca d'água poderão ser representadas tanto no domínio do tempo quanto no domínio da frequência.

5 MÉTODOS DE INSERÇÃO E EXTRAÇÃO DE MARCA D'ÁGUA EM IMAGENS NO DOMÍNIO WAVELET

Com o passar dos tempos, vários métodos de inserção e extração de marca d'água em imagens digitais têm sido propostos na literatura especializada, dentre eles se destacam os métodos baseados na transformada wavelet.

Um método integrado de codificação em imagens e sistema de marca d'água é apresentado por (WANG; KUO, 1998). A imagem é codificada e comprimida no domínio wavelet. A inserção da marca d'água é feita por entropia nos coeficientes wavelets. A marca usada neste método é gerada por uma distribuição gaussiana pseudoaleatória.

Em Jayawardena e Lenders (2000) é proposto um método que usa os canais de multirresolução da imagem hospedeira no domínio wavelet para inserir a marca d'água binária também através dos seus canais de multirresolução, considerando que quanto mais alto o nível de resolução usado para inserir a marca, menor será o risco de ela ser detectada por intrusos.

A inserção da marca d'água baseado no sistema visual humano (HVS), é proposto por Hsieh e Wu (2001). A marca é inserida nas regiões onde a percepção humana é menor, garantindo uma maior robustez ao método. A imagem hospedeira é decomposta em três níveis de resolução pela transformada wavelet discreta e a marca é inserida nos níveis 2 e 3. A criptografia do sistema é feito usando o algoritmo de código corretor de erros Bose-Chaudhuri-Hocquenghem - BCH. A marca d'água é uma sequência pseudoaleatória de 1000 pontos.

Em Tay e Havilcek (2003), é apresentada uma metodologia que insere a marca d'água nos canais wavelet de frequência média e usa o canal em que a marca é inserida e os filtros wavelets, usados na decomposição da imagem como chaves de segurança para o processo de extração.

O método proposto por Dote e Shaik (2003), decompõem a imagem hospedeira em 5 níveis pela DWT e a marca d'água em 1 nível. Os coeficientes transformados da marca d'água são inseridos de maneira aleatória na imagem decomposta, este tipo de inserção serve também como chave de segurança. A marca d'água pode ser uma sequência binária aleatória ou um texto.

Em Wang e Wiederhold (1998), é usado filtros de Daubechies para decompor a imagem em 4 níveis de resolução e distribui a marca d'água em diferentes áreas da imagem baseado

na suavidade da região. A chave de segurança para a extração segura é gerada por códigos corretores de erros.

Em Al-Hunaity, Najin e El-Emary (2007), usam como imagem hospedeira uma imagem comprimida no domínio wavelet dentro dos bits menos significantes (LSB) da região coberta pela marca d'água num padrão específico invisível depois da inserção, evitando a quebra da chave de segurança da marca, porém garantindo a futura extração da mesma. Para isto, a imagem é decomposta pela wavelet de Haar em dois níveis de resolução.

A metodologia proposta por Chemak, Lapayre e Bouhieu (2007), aplica o esquema lifting de decomposição wavelet na imagem hospedeira usando a wavelet biortogonal 5/3. A marca d'água é inserida nos pixels de maior intensidade nas faixas de frequências médias da imagem decomposta. A marca d'água é uma sequência de 2000 bits codificada na razão $\frac{1}{2}$ num turbo codificador. Este método é robusto e muito aplicado em proteção de imagens biomédicas.

No Brasil a técnica pioneira na inserção de marca d'água no domínio wavelet, foi proposta por Sans e Pedrini (2008), que usam a DWT para fazer a inserção da marca d'água numa imagem também baseada no HVS. A imagem hospedeira e a marca são decompostas uma única vez, depois o nível de resolução de mais baixa frequência da marca é espalhado aleatoriamente no nível de resolução de mais baixa frequência da imagem. Após esse processo a imagem é reconstruída e dividida em blocos. Cada bloco é decomposto em um nível pela DWT e são construídos e ordenados os vetores de luminosidade cujos índices servirão para determinar quais blocos receberão as bandas de frequências da marca d'água. As bandas da marca serão inseridas no mais alto nível de resolução dos blocos escolhidos.

Outra técnica brasileira baseada na transformada wavelet, foi proposta por Mendes (2008), que faz a inserção de marca d'água numa imagem digital através do esquema lifting da transformada wavelet, usando a wavelet CDF 9/7 (Cohen-Daubechies-Feauveau) biortogonal e decompondo a imagem em três níveis de resolução. A inserção, com o objetivo de garantir a transparência da marca, é feita por meio de mapeamento da imagem hospedeira no domínio wavelet. A segurança da marca é garantida por funções *hash* e chaves assimétricas. A marca d'água é inserida na banda de mais baixa frequência do nível 3 de resolução.

A aplicação de marca d'água binária foi proposta por Huang et al. (2010), que fazem a inserção de uma marca d'água binária numa imagem digital decompondo essa imagem em dois níveis pela DWT e espalhando a marca d'água nas bandas de frequência do segundo nível de resolução nas regiões onde a percepção humana é menos sensível. Como chave de

segurança é usado o algoritmo de criptografia baseado na técnica ACM. Para garantir a robustez do método várias características do HVS são exploradas, como frequência da luz, textura e luminância.

O processo de extração da marca d'água em todos os métodos citados anteriormente é feito através da inversão dos passos usados na inserção. A verificação geralmente é feita através do cálculo da similaridade entre a marca d'água extraída e a inserida. Portanto ou são métodos não cegos ou semicegos.

Além dos métodos relatados nesta seção, três métodos foram estudados em detalhes, o método de Cox et al. (1997), por se tratar de um dos primeiros a tratar o assunto (COX et al., 1997). O método de Sanghyn et al. (2002) usa a DWT e faz inserção de marca d'água binária, porém com pixels distribuídos aleatoriamente (SANGHYN et al., 2002). Finalmente o método de Hajjara, Abdallah e Hudaib (2009), que usa wavelets biortogonais na decomposição da imagem hospedeira e marcas d'água binária, porém em forma de texto (HAJJARA; ABDALLAH; HUDAIB, 2009).

Pelo fato de existirem vários métodos de inserção e/ou extração de marca d'água em imagens baseados na transformada wavelet, cada qual com suas características (SANS, 2008), como descritos anteriormente, para o desenvolvimento da metodologia proposta nesta pesquisa, foram analisados alguns métodos de inserção e extração de marca d'água em imagens digitais, desde o mais simples e pioneiro na literatura até os estudos mais recentes que apresentam resultados significativos para pesquisas que envolvem marca d'água, dentre elas três técnicas, consideradas importantes, (COX et al., 1997; SANGHYN et al., 2002; HAJJARA; ABDALLAH; HUDAIB, 2009).

Das três técnicas analisadas o que diferencia cada uma é o tratamento que a imagem e a marca d'água recebem. Porém, as três se baseiam em transformar a imagem, modificar as informações contidas na marca d'água, inseri-la, extrair e aplicar a correlação para verificar a similaridade entre a marca d'água inserida e a extraída.

Devido à grande importância do assunto, surgem continuamente novas técnicas de inserção e extração de marca d'água, especificadamente no domínio wavelet por ser uma ferramenta de ótimo desempenho (DUARTE; SILVA; VILLARREAL, 2011; SANS, 2008).

5.1 Método Cox et al. (1997)

Um dos primeiros métodos propostos para manipulação de marca d'água é o de (COX et al., 1997; COX et al., 1997; COX; MILLER; BLOOM, 2000). Este método trabalha de

forma bem simples tanto na inserção quanto na extração. A inserção é efetuada nos coeficientes sem alterar visivelmente a qualidade da imagem original.

Cox et al. (1997) basearam-se no fato de que cada coeficiente no domínio da frequência tem uma capacidade de percepção, o que faz com que certa quantidade de informação possa ser adicionada em cada frequência sem afetar notoriamente a qualidade da imagem.

A marca d'água considerada é uma sequência pseudoaleatória de tamanho 1000, e a transformada usada é a transformada discreta de cossenos DCT (COX et al., 1997; COX; MILLER; BLOOM, 2000). Este método é muito estudado e serve de subsidio para iniciantes no assunto devido a sua simplicidade, tanto na inserção quanto extração da marca d'água.

Cox et al. (1997) propõem um esquema de marca d'água digital robusto, onde a marca d'água é inserida nos coeficientes perceptivelmente mais importantes da imagem, pois estes coeficientes geralmente são menos afetados por operações de processamento de imagens, obtendo então uma maior robustez nos sistemas de marca d'água (COX et al., 1997; COX; MILLER; BLOOM, 2000).

5.1.1 *Algoritmo de inserção*

Na técnica de Cox et al. (1997) é possível realizar variações no processo de inserção da marca d'água. A seguir são descritos os passos para o processo de inserção do método de (COX et al., 1997).

Passo 1: Gerar uma sequência X pseudoaleatória com distribuição gaussiana $N[0,1]$ de tamanho $n=1000$.

$$X = \{x_1, x_2, \dots, x_{1000}\} \quad (30)$$

Passo 2: Seja I a imagem hospedeira em níveis de cinza. Aplica-se a transformada discreta de cossenos (DCT) em duas dimensões na imagem I , obtendo T através da Equação (31).

$$T = DCT(I) \quad (31)$$

Passo 3: Selecionar os 1000 maiores coeficientes obtidos no passo 2, obtendo a sequência em que ordem crescente T_{max} .

$$T_{max} = \{t_1, t_2, \dots, t_{1000}\} \quad (32)$$

Passo 4 : Modificar os coeficientes selecionados no passo 3 através da Equação 33:

$$T'_i = T_{\max_i} + \alpha X_i \quad i=1,2,...,1000; \quad (33)$$

sendo

T'_i : sequência modificada;

$T_{\max_i}$: sequência original;

X_i : marca d'água;

α : fator escalar.

O fator de escala atua como um fator quantitativo de intensidade que determina a alteração que a marca d'água irá causar na imagem hospedeira.

Passo 5 : Substituir os coeficientes originais pelos modificados;

$$T_i = T'_i \quad i=1,2,...,n; \quad (34)$$

Passo 6 : Aplicar a transformada inversa para obter a imagem marcada IX ;

$$IX = DCT_{inversa}(T) \quad (35)$$

5.1.2 Algoritmo de extração

No processo de extração da marca d'água, são utilizadas tanto a imagem marcada IX como a imagem original I (COX et al.,1997). A seguir são descritos os passos do processo de extração da marca d'água pelo método de (COX et al., 1997).

Passo 1 : Decompor as imagens, original e a imagem marcada pela DCT ;

Passo 2 : Aplicar a Equação 36 para extrair a marca d'água;

$$XE_i = \frac{T'_i - T_{\max_i}}{\alpha}, \quad i=1,2,...,n; \quad (36)$$

Passo 3 : Para se fazer alguma asserção sobre a propriedade da imagem, são comparadas as marcas d'água original X e extraída XE . Várias medidas de similaridade podem ser utilizadas para fazer a comparação dessas marcas. Cox et al. (1997), utilizaram para isso a Equação 37.

$$\text{sim}(X, XE) = \frac{XE * X}{\sqrt{XE * X}} \quad (37)$$

Para determinar se a marca d'água extraída corresponde à marca d'água original um limiar μ pode ser determinado. Caso a correlação entre as marcas seja maior que μ as marcas são consideradas correspondentes, caso a correlação seja menor que μ as marcas não são consideradas similares. Nos testes realizados por Cox et al. (1997), foi utilizado $\mu=6$ e o fator escalar $\alpha=0,1$.

A medida de similaridade adotada por Cox et al. (1997) funciona bem em marcas binárias, pois, quanto maior o número de colisões de bits entre a marca original e a marca extraída, maior será a correlação.

A desvantagem deste método está na aplicação da ferramenta de processamento que é a transformada de cossenos. Esta transformada requer mais complexidade computacional que outras transformadas usadas no processamento de imagens, como é o caso da transformada wavelet.

A transformada wavelet discreta tem apresentado bom desempenho quando se trata de processamento de imagens e uma dessas vantagens está exatamente no fato de ser mais simples de se implementar que a DCT (LOPES et al., 2004).

Outra questão que faz com que em algumas aplicações o método proposto por Cox et al. (1997), apresente outro fator negativo, está na detecção da marca d'água, que consiste em extrair a marca de uma imagem I' possivelmente marcada e calcular a correlação entre a marca d'água extraída e a marca d'água original, devido ao fato de que é preciso conhecer o local exato onde a marca d'água foi inserida e, conseqüentemente, utilizar a imagem original para o processo de extração.

Em Duarte, Silva e Villarreal (2011) é apresentada uma versão do método de Cox et al. (1997), usando a DWT.

5.2 Implementação do método de Cox et al. com a DWT bidimensional

O mais conhecido é o método de Cox et al. (1997), que insere a marca d'água nos coeficientes wavelet levando em consideração a energia dos mesmos, sendo um dos pioneiros da área de inserção e extração de marca d'água (COX et al., 1997).

A implementação do método Cox et al. (1997), com a DWT bidimensional consiste primeiramente em substituir a ferramenta de processamento, no caso a DCT pela DWT no passo 2 do algoritmo de inserção. Essa mudança permite que sejam realizados mais que dois

níveis de decomposição, quando necessários, respeitando o limite no número de decomposições. Sendo este número máximo determinado de acordo com a dimensão da imagem hospedeira.

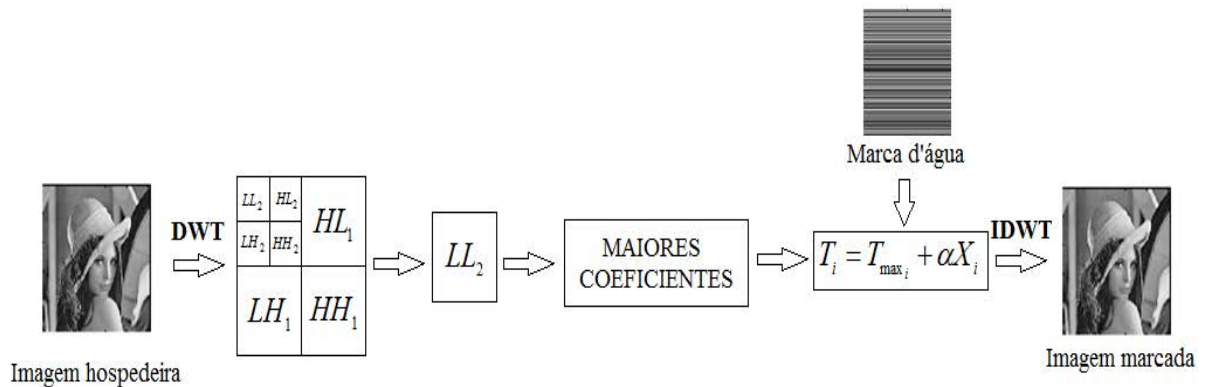
Desta forma, os coeficientes são organizados em $3k+1$ sub-bandas de frequências, sendo k o nível de decomposição, que se dividem em altas e baixas frequências. Os primeiros níveis da decomposição resultam em sub-bandas de alta frequência $\{LH_k, HH_k, HL_k\}$, ressaltando que se o objetivo da aplicação for uma possível transmissão, quanto maior o nível de decomposição, menor será a magnitude dos coeficientes e, conseqüentemente, menor será o espaço de armazenamento (MARTÍNEZ; VIOLA, 2000).

No último nível são obtidos os coeficientes de baixa frequência $\{LL_k\}$, os quais contêm a maior parte da energia da imagem, ou seja, permitem uma aproximação da imagem original. Porém, com um número menor de pixels. Por exemplo, uma imagem de 256×256 pixels, decomposta em três níveis pela DWT bidimensional, é aproximada, no terceiro nível, por uma representação de 32×32 pixels da imagem original.

Os coeficientes que formam essa nova representação da imagem original são o alvo para a inserção da marca d'água, pelo fato de apresentarem maior magnitude, ocupando mais espaço no armazenamento da imagem e também contêm fatores determinantes para a transparência da marca d'água (MARTÍNEZ; VIOLA, 2000). Desta forma após a decomposição com a DWT bidimensional, nos 1000 maiores coeficientes wavelets será inserida a marca d'água como descrito no passo 3 do algoritmo de inserção proposto por (COX et al., 1997).

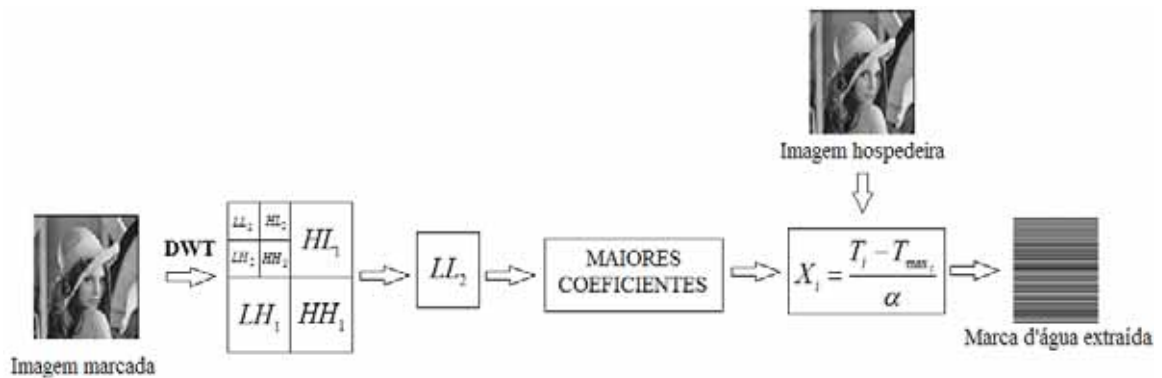
No passo 4 do algoritmo, é aplicada a DWT inversa para se ter uma imagem marcada. No processo de extração, é preciso conhecer a imagem original e a marca d'água inserida, e seguir os mesmos passos do uso da DCT, porém trocada pela DWT bidimensional. Na Figura 42 são ilustrados os passos do algoritmo que implementa o método de Cox et al. (1997) com a transformada wavelet bidimensional na inserção da marca d'água e na Figura 43 a ilustração do processo de extração da marca d'água.

Figura 42 - Método de inserção de marca d'água proposto por Cox et al. (1997) usando a DWT bidimensional.



Fonte: Elaborada pela própria autora.

Figura 43 - Método de extração de marca d'água proposto por Cox et al. (1997) usando a DWT bidimensional.



Fonte: Elaborada pela própria autora.

5.3 Método de Sanghyn et al. (2002)

O método proposto por Sanghyn et al. (2002), usa como marca d'água uma sequência aleatória do conjunto $\{-1,1\}$, isso porque uma marca d'água com tal característica se torna mais robusta, ao contrário do que acontece no método de Cox et al. (1997) que usa uma sequência pseudoaleatória. Além disso, uma marca d'água binária não degrada a qualidade visual da imagem hospedeira de forma brusca, mesmo se tratando de uma marca d'água invisível (PAMBOUKIAN, 2007).

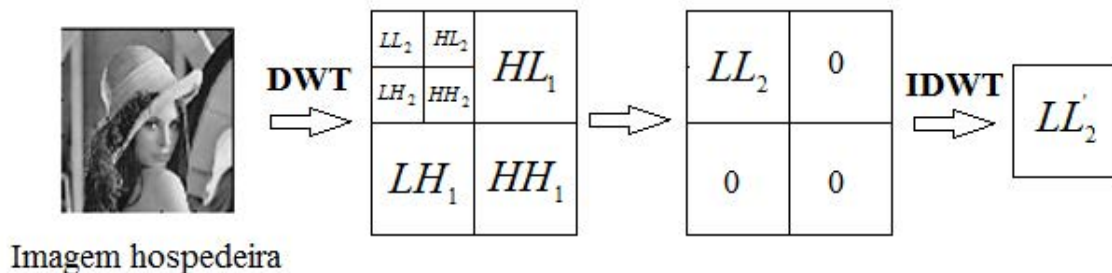
Outra vantagem do método proposto por Sanghyn et al. (2002), em relação ao método de Cox et al. (1997), é a utilização da DWT no processo de decomposição. A marca d'água, neste caso é inserida na sub-banda de frequência LL_2 , que é uma aproximação da imagem

original, visto que a marca d'água inserida no domínio da frequência se torna ainda mais robusta do que no domínio do tempo (LOPES et al., 2004).

Na extração da marca d'água, assim como o método de Cox et al. (1997), o método proposto por Sanghyn et al. (2002), requer a imagem hospedeira e a marca d'água inserida no processo de verificação de integridade da marca d'água. A comparação também é feita através da correlação entre a marca inserida e a extraída. A comparação da similaridade das marcas, por ser mais robusta, requer mais esforço do que a comparação no método Cox et al. (1997).

Na inserção de marca d'água a imagem hospedeira é decomposta pela DWT bidimensional em três níveis. A banda de frequência LL_k é, então, escolhida para a inserção. Antes, porém, esta banda é decomposta por um nível da DWT bidimensional e os coeficientes das bandas LH_{k+1} , HL_{k+1} , HH_{k+1} passar a ter valor zero, restando apenas coeficientes não nulos de LL_{k+1} . Nessa nova matriz é aplicada a DWT bidimensional inversa, obtendo LL'_k como ilustra a Figura 44.

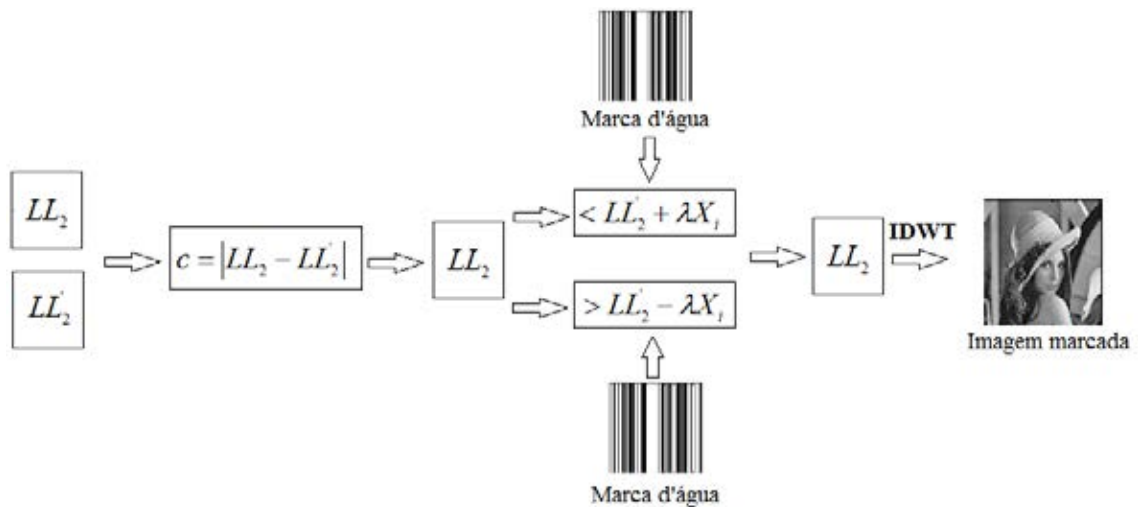
Figura 44 - Preparação da região na imagem hospedeira para receber a marca d'água proposto pelo método Sanghyn et al. (2002).



Fonte: Elaborada pela própria autora.

Os coeficientes da marca d'água são inseridos em LL_k , nos coeficientes com menores diferenças entre LL_k e LL'_k . A inserção é feita da seguinte forma: a marca d'água é a sequência binária X_i de elementos do conjunto $\{-1,1\}$ e os valores de LL_k são substituídos por $LL'_k \pm \lambda \cdot X_i$, conforme os valores de X_i , sendo λ um fator de controle de intensidade da inserção. Após esse processo, a IDWT bidimensional é aplicada em LL_k e depois na imagem inteira para obter a imagem marcada. Na Figura 45 é ilustrado todo o processo de inserção da marca d'água proposto por (SANGHYN et al., 2002)

Figura 45 - Inserção da marca d'água proposto por Sanghyn et al. (2002).



Fonte: Elaborada pela própria autora.

Na extração, necessita-se da imagem original e da imagem marcada, isto é, trata-se de um método não-cego de extração. As duas imagens são decompostas pela DWT como descrito no processo de inserção e a marca d'água é extraída comparando as bandas LL_k e LL'_k das imagens, original e marcada, fazendo o processo inverso ao de inserção. Por fim, é calculada a correlação entre a marca original e extraída para verificar suas semelhanças.

5.4 Método de Hajjara, Abdallah e Hudaib (2009)

Em Hajjara, Abdallah e Hudaib (2009) é proposto um método que usa wavelets biortogonais (no caso *splines*) para inserção e extração de marca d'água binária. A imagem é decomposta usando a DWT. A marca d'água é inserida nos coeficientes de detalhes com o objetivo de tornar a técnica resistente a vários tipos de ataques e torná-la imperceptível. Os processos de inserção e extração são descritos nas duas seções seguintes.

5.4.1 Algoritmo de inserção

Passo 1: Decompor a imagem hospedeira, usando a DWT para obter os coeficientes horizontais (HL_1);

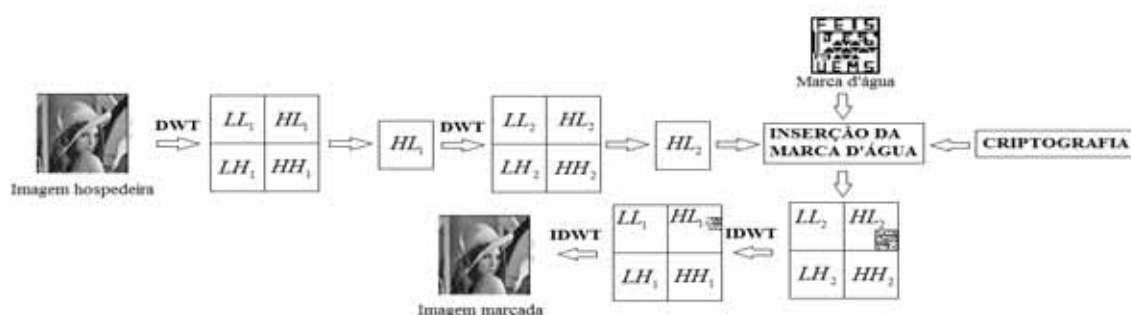
Passo 2: Decompor a sub-banda HL_1 obtida no passo 1 usando a DWT para obter um segundo nível de coeficientes de detalhes (HL_2);

Passo 3: Gerar uma sequência ruidosa pseudoaleatória (PN) sempre que o bit da marca d'água for zero, e adicione-a em HL_2 , resultante do passo 2;

Passo 4: Executar a DWT inversa duas vezes, primeiro apenas em HL_2 e depois na imagem inteira, para obter a imagem marcada.

A Figura 46 ilustra todo o processo de inserção do método proposto por (HAJJARA; ABDALLAH; HUDAIB, 2009).

Figura 46 - Inserção de marca d'água proposta por Hajjara, Abdallah e Hudaib (2009).



Fonte: Elaborada pela própria autora.

5.4.2 Algoritmo de extração

Para a extração da marca d'água os passos a seguir são aplicados na imagem, marcada:

Passo 1: Executar a DWT bidimensional para obter os coeficientes de detalhes horizontais (HL_1);

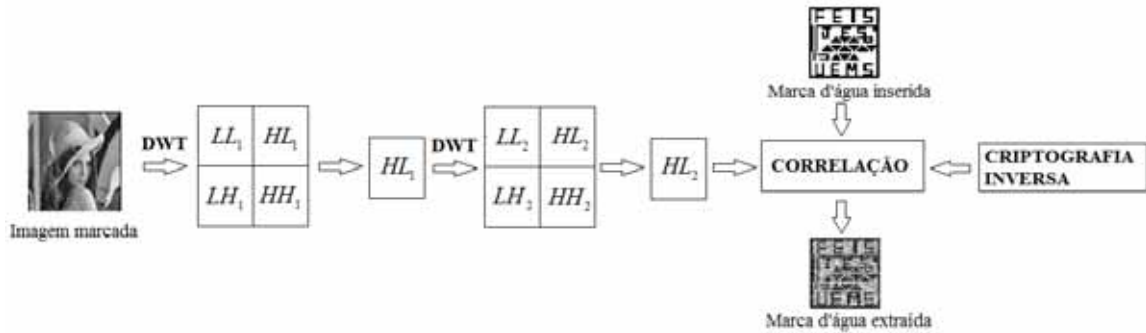
Passo 2: Decompor, novamente, HL_1 usando a DWT bidimensional para obter HL_2 ;

Passo 3: Calcular a correlação entre os coeficientes de detalhes resultantes do passo 2 (HL_2) e a sequência PN;

Passo 4: Atribuir o valor zero, que representa os pixels em preto, sempre que a correlação for maior que um determinado limiar.

A Figura 47 ilustra o processo de extração da marca d'água pelo método proposto por (HAJJARA; ABDALLAH; HUDAIB, 2009).

Figura 47 - Extração da marca d'água proposta por Hajjara, Abdallah e Hudaib (2009).



Fonte: Elaborada pela própria autora.

Após realizar um levantamento teórico sobre os métodos de inserção descritos neste capítulo, foram realizados testes para apontar as vantagens e desvantagem por meio de resultados numéricos baseados na correlação entre marcas inseridas e extraídas.

5.5 Cálculo da PSNR e da Correlação Normalizada (NC)

A *PSNR* (Peak Signal-to-Noise Ratio) será sempre calculada comparando a imagem original e a imagem marcada após o ataque. Quanto maior a *PSNR*, que é medida em decibéis (dB), menor é o nível de distorção na imagem. Quanto mais próxima de 1,0 estiver a *NC*, maior é a semelhança entre a marca d'água inserida e a extraída.

As Equações 38 e 40 apresentam, respectivamente, as formas de se calcular a *PSNR* e a correlação normalizada (NC) (HUANG et al., 2010).

$$PSNR = 10 \log_{10} \frac{d^2}{MSE} \quad (38)$$

sendo d a dimensão da imagem, e o erro quadrático mínimo (MSE) obtido pela equação (39).

$$MSE = \sum_{i=1}^A \sum_{j=1}^L (I_{i,j} - I'_{i,j}) / d \quad (39)$$

onde

$I_{i,j}$: pixels da imagem original;

$I'_{i,j}$: pixels da imagem modificada;

A e L : altura e largura das imagens, respectivamente;

d : dimensão da matriz que representa a imagem.

$$NC(W, W') = \sum_{m=1}^{N_w} (w_m w'_m) / \sqrt{\left(\sum_{m=1}^{N_w} w_m^2 \sum_{m=1}^{N_w} w'_m{}^2 \right) / N_w} \quad (40)$$

Na Equação 40, W é a marca d'água inserida e W' a extraída e N_w , o número de pixels da marca d'água.

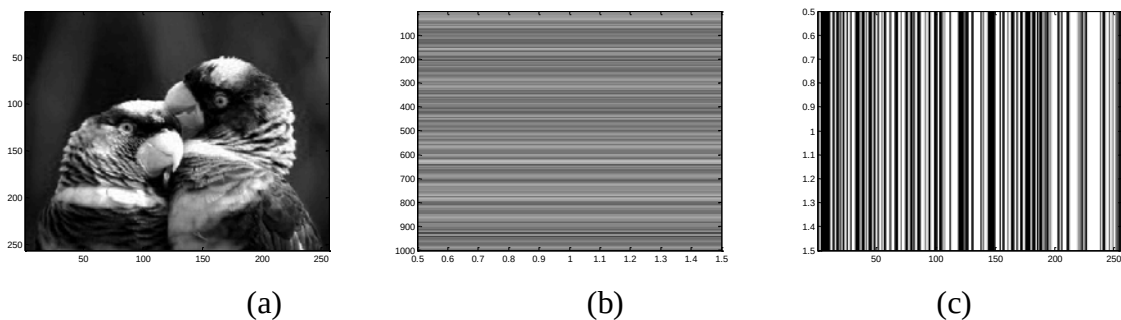
5.6 Testes com os métodos analisados

Os testes foram realizados com uma imagem de 256×256 pixels, sendo realizada como ataque a compressão usando o limiar *Hard* (DONOHO; JOHNSTNE, 1994). Tal operação se encaixa em um dos tipos de ataque que uma imagem contendo marca d'água pode sofrer e é caracterizada como uma compressão com perdas, um dos ataques mais fortes que uma imagem pode sofrer.

Para verificar o nível de compressão da imagem, em cada método, foi calculado a *PSNR* (HUANG et al., 2010) e a correlação normalizada, para verificar a similaridade entre as marcas d'água inserida e extraída.

A seguir são apresentas as marcas d'água extraídas de acordo com cada método analisado. Na Figura 48 são apresentadas (a) Imagem hospedeira 256×256 pixels; (b) Marca d'água pseudoaleatória $n=1000$; (c) Marca d'água aleatória; (d) Marca d'água binária 8×8 pixels.

Figura 48 - (a) Imagem hospedeira 256×256 pixels; (b) Marca d'água pseudoaleatória; (c) Marca d'água aleatória; (d) Marca d'água binária 8×8 pixels.

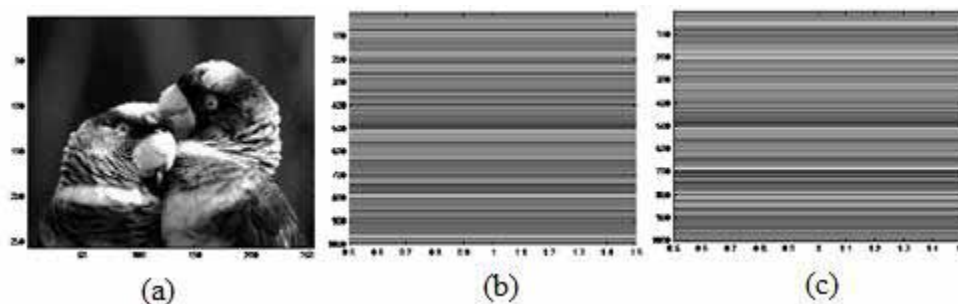


Fonte: Elaborada pela própria autora.

A Figura 49 apresenta a imagem marcada e as marcas, inserida e extraída pelo método de (COX et al., 1997). Na Figura 50 são apresentas, a imagem marcada, as marcas, inserida e

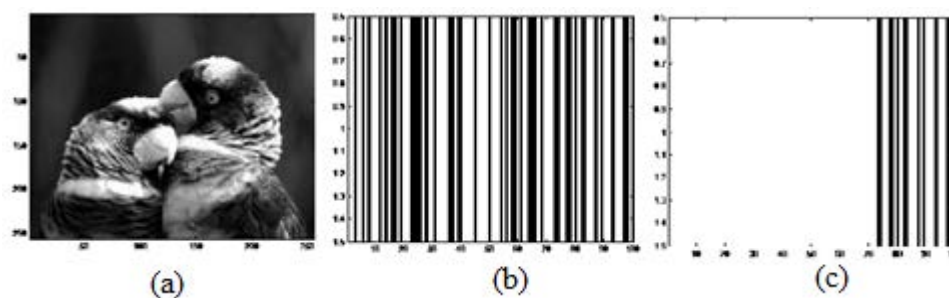
extraída pelo método de Sanghyn et al. (2002), e a Figura 51 apresenta a imagem marcada, as marcas, inserida e extraída pelo método de (HAJJARA; ABDALLAH; HUDAIB, 2009).

Figura 49 - (a) Imagem marcada pelo método de Cox et al. (1997); (b) Marca d'água inserida; (c) Marca d'água extraída.



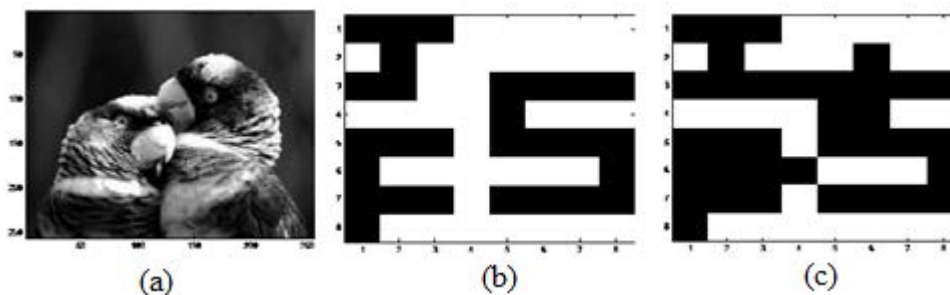
Fonte: Elaborada pela própria autora.

Figura 50 - (a) Imagem marcada pelo método de Sanghyn et al. (2002); (b) Marca d'água inserida; (c) Marca d'água extraída.



Fonte: Elaborada pela própria autora.

Figura 51 - (a) Imagem marcada pelo método de Hajjara, Abdallah e Hudaib (2009); (b) Marcas d'água inseridas; (c) Marca d'água extraída.



Fonte: Elaborada pela própria autora.

A Tabela 14 apresenta as métricas obtidas após a aplicação de cada uma dos métodos analisados na imagem pássaros.

Tabela 14- Métricas obtidas após aplicação dos métodos analisados

Ataques	PSNR (dB)	Correlação Normalizada (NC)
Método proposto por Cox et al. (1997)	36,53	1,000
Método proposto por Sanghy et al.(2002)	29,23	0,4543
Método proposto por Hajjara, Abdallah e Hudaib (2009)	30,96	0,8026

Fonte: Dados da pesquisa da própria autora.

Os métodos analisados buscam garantir a integridade da marca d'água inserida para uma futura verificação de integridade da imagem hospedeira ou simplesmente da própria marca d'água. Além disso, os mesmos garantem a qualidade visual da imagem hospedeira, inserindo marcas d'água robustas.

Na extração da marca d'água, após a compressão da imagem, o método de Cox et al. (1997) se mostrou mais eficiente, pois obteve uma marca idêntica à original. O método de Sanghyn et al. (2002) teve uma correlação baixa, isso se deve ao fato do mesmo trabalhar com marca d'água com pixels com valores -1 ou 1 e o processo aleatório deve ser aplicado também na extração.

O método de Hajjara, Abdallah e Hudaib (2009) apresenta um valor de correlação melhor que o de Sanghyn et al. (2002), muito em função do tipo de marca d'água usada. Este valor pode melhorar ainda mais se a marca usada tiver um número maior de pixels, pois numa imagem 8×8 pixels, como a usada nesse teste, a mudança de valor num pixel interfere bastante no resultado final da correlação.

Dos três métodos, o mais seguro é o de Hajjara, Abdallah e Hudaib (2009), pois a sequência PN usada na inserção da marca d'água funciona como uma chave de segurança para a preservação da integridade da marca, além do fato da marca ser uma imagem e não, simplesmente, uma sequência aleatória como nos outros dois métodos.

6 METODOLOGIA PROPOSTA

Após análise de alguns métodos baseados na inserção, extração e verificação de marca d'água pode-se constatar que, além dos resultados serem satisfatórios para a área de processamento de imagens, as técnicas em questão podem ser facilmente implementadas mantendo a integridade da imagem hospedeira com uma marca d'água robusta.

Em geral, os métodos são estruturados para manter a integridade da marca d'água após ataques num projetado processo de extração não se dando relevância significativa à imagem hospedeira no final de tal processo, sendo esta, em muitas aplicações, o principal material a ser manipulado, como é o caso de imagens médicas dispostas em bancos de dados. Ou seja, os métodos propostos são voltados a manter a integridade da imagem de modo comprobatório e não de modo visual, sendo este requisito mantido apenas no processo de inserção, já que é mais viável para fins tecnológicos a marca d'água imperceptível.

A partir destas constatações, foram realizadas implementações baseadas em operações matemáticas que se estendem desde a ferramenta de processamento, que é a transformada wavelet, até a técnica de criptografia proposta por Sanghyn et al. (2002) que é, basicamente, estruturada em operações matemáticas.

A ferramenta de processamento escolhida é a DWT bidimensional, pois tem apresentado resultados que garantem manter a integridade visual de imagens (MENDES, 2008). Desta forma, a questão de integridade visual da imagem hospedeira e da marca d'água pode ser garantida não se limitando à aplicação da técnica desenvolvida apenas em imagens que apresentam fins comerciais, mas principalmente as que apresentam finalidades científicas. Além disso, para questões que envolvem transmissão de arquivos, a transformada wavelet é eficiente em técnicas de compressão, sendo esta a finalidade da aplicação de marca d'água em imagens, já que não se pensa mais em transmissão de dados sem envolver sua compactação.

O método proposto, neste trabalho, divide-se em quatro etapas, que, por sua vez, podem se subdividir em outras. A primeira, consiste na preparação da imagem hospedeira. Nesta preparação, as possíveis regiões, onde a marca d'água poderá ser inserida, são dispostas em sub-bandas de frequências resultantes da aplicação da DWT bidimensional. Nesta mesma etapa, a marca d'água recebe o mesmo tratamento da imagem hospedeira, porém de modo separado, isto porque na marca d'água é aplicado apenas um nível de decomposição pela DWT bidimensional fornecendo quatro sub-bandas de frequências que futuramente receberão a criptografia. A transformada wavelet é aplicada nos dois casos visando um melhor

desempenho do método de inserção e garantindo um maior entrelaçamento entre os pixels da imagem hospedeira e da marca d'água.

A segunda etapa pode ser considerada uma subdivisão da primeira, mas para exemplificar de forma mais significativa o método proposto, esta etapa foi considerada isolada, representando apenas a manipulação da marca d'água. As sub-bandas de frequência, correspondentes à decomposição da marca d'água realizada na primeira etapa, são consideradas como blocos. Esses blocos são criptografados pela técnica ACM e receberão outra modificação. A técnica de criptografia ACM foi escolhida - entre outras descritas na literatura - devido a simplicidade de sua implementação, a qual aplica-se apenas processos sucessivos de desorganização dos pixels sem modificar seu valor espectral.

A terceira etapa consiste na inserção dos blocos criptografados resultantes da segunda etapa. Estes blocos serão alocados na sub-banda de frequência HL_2 resultante da decomposição da sub-banda HL_1 da imagem hospedeira realizada da primeira etapa. Os locais escolhidos para inserir esses blocos foram os quatro cantos da sub-banda HL_2 , escolha esta que visa não prejudicar a qualidade visual da imagem, porém não os impede de serem inseridos em outros locais, assim como podem ser inseridos do mesmo modo em outras sub-bandas.

A quarta etapa consiste em extrair a marca d'água e verificar a autenticidade diante da marca d'água inserida. Por esse motivo, o processo de extração é caracterizado como semicego (PORTILLA; SIMONCELLI, 2000). Neste processo de extração, primeiramente, procura-se apenas garantir a integridade da marca d'água inserida. Os cuidados com a imagem hospedeira são envolvidos apenas na primeira, segunda e terceira etapa, procurando agir de modo a não prejudicar visualmente a imagem hospedeira, por isso que na verificação é necessária apenas a marca d'água inserida.

A ferramenta utilizada para a inserção e extração da marca d'água, como mencionado anteriormente, é a DWTB o que possibilita que a marca d'água a ser inserida apresente características computacionais binárias e visualmente imperceptíveis ao HVS. Além disso, é uma marca d'água detectável e robusta. Os processos de inserção, extração e verificação são detalhados a seguir.

6.1 Primeira etapa

A primeira etapa se subdivide em outras duas etapas que envolvem a manipulação da imagem hospedeira e da marca d'água a ser inserida.

6.1.1 Preparação da imagem hospedeira

Nesta primeira sub-etapa, o foco de manipulação é a imagem hospedeira, mais precisamente a região que receberá a marca d'água. Inicialmente, é aplicada a DWTB com um nível de decomposição não-padrão na imagem hospedeira em seguida, é realizado o mesmo processo de decomposição, porém, diferente de outras decomposições usuais que aplicam o processo recursivamente na sub-banda LL .

A decomposição apenas será realizada em um nível na sub-banda de frequência HL_1 , como proposto por Hajjara, Abdallah e Hudaib (2009), resultando assim novas sub-bandas de frequências LL_2 , LH_2 , HL_2 e HH_2 . É nesta etapa que se escolhe, dentre LL_2 , LH_2 , HL_2 e HH_2 , qual é a melhor sub-banda de frequência para inserir a marca d'água.

A seguir são apresentados os passos do algoritmo que resulta nas quatro possíveis regiões que a imagem hospedeira poderá receber a marca d'água.

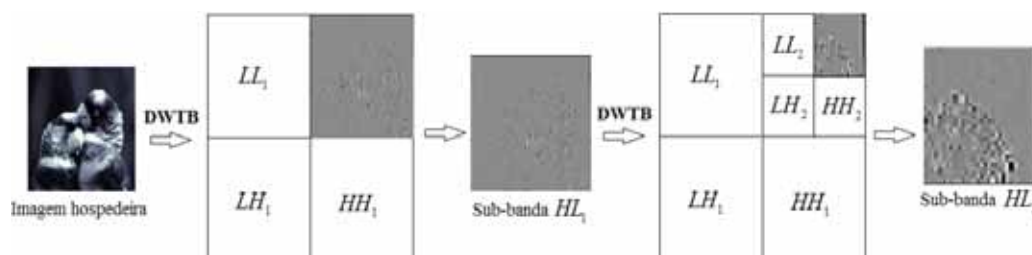
6.1.1.1 Algoritmo de preparação

Passo 1 : Aplica a DWT bidimensional na imagem hospedeira para obter a sub-banda HL_1 ;

Passo 2 : Aplica a DWT bidimensional na sub-banda HL_1 para obter uma segunda sub-banda, HL_2 que possui coeficientes de detalhes da imagem. Essa será a região onde a marca d'água será inserida.

O algoritmo de preparação da imagem hospedeira é ilustrado na Figura 52.

Figura 52 - Preparação da região hospedeira da marca d'água.



Fonte: Elaborada pela própria autora.

Foram feitos vários testes, que incluem a escolha da outras sub-bandas, tanto no primeiro nível de decomposição (LL_1 , LH_1 e HH_1), quanto no segundo nível, quando é aplicada a decomposição apenas na sub-banda escolhida no primeiro nível. Por exemplo, a sub-banda HL_1 resulta nas sub-bandas LL_2 , LH_2 e HH_2 .

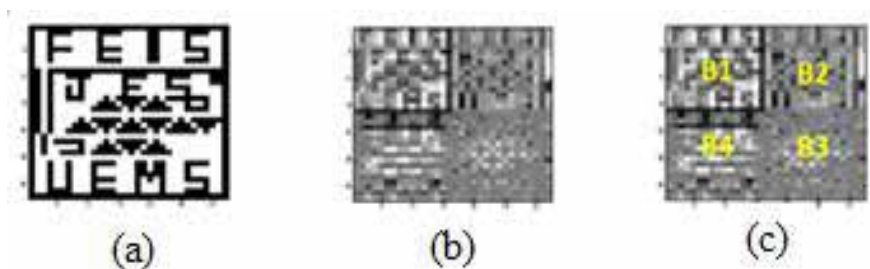
Os testes apontam que os melhores resultados são os obtidos da na sub-banda HL_2 de HL_1 , mesmo com formas de inserção e extração e criptografia da marca d'água totalmente diferentes da que será usada aqui.

Isto porque, a sub-banda LL_k contém os coeficientes mais significativos e, no caso de um ataque, esses coeficientes são os mais prejudicados. Se a marca d'água for inserida na sub-banda LH_k o efeito será o mesmo obtido na sub-banda HL_k . Já se a marca d'água for inserida na sub-banda HH_k , por conter os coeficientes menos significativos, diante do ataque de compressão com perda, os coeficientes da imagem hospedeira serão facilmente eliminados, incluindo os coeficientes da marca d'água.

6.1.2 Preparação da marca d'água

Assim como a imagem hospedeira recebeu processamento via DWT bidimensional, nesta sub-etapa a mesma aplicação será realizada na marca d'água de dimensão $N \times N$, porém ao invés de aplicar a decomposição em dois níveis, será aplicado apenas um nível de decomposição na marca d'água resultando em sub-bandas LL_1 , LH_1 , HL_1 e HH_1 . Essas quatro sub-bandas apresentam dimensões quadradas de ordem $\frac{N}{2}$. Pela característica das dimensões das sub-bandas, todas as quatro poderão corresponder a quatro blocos com as mesmas dimensões correspondentes a cada sub-banda. Com essa ideia a marca d'água no domínio wavelet é representada por quatro partes de dimensões $\frac{N}{2} \times \frac{N}{2}$, a partir do canto superior esquerdo no sentido horário. Essas partes são chamadas de blocos B_1 , B_2 , B_3 e B_4 como ilustra a Figura 53.

Figura 53 - (a) Marca d'água binária; (b) Sub-banda de frequência da marca d'água; (c) Blocos correspondentes as sub-bandas de frequência.



Fonte: Elaborada pela própria autora.

6.2 Segunda etapa

Diante das inúmeras aplicações o emprego da criptografia tem sido constantemente apresentadas em varias pesquisas, fundamentadas com resultados significantes para a área de processamento de imagens, inclusive no emprego em marca d'água (STALLING; HALL, 1998).

Talvez, essa seja a principal fase de qualquer técnica de inserção de marca d'água, inclusive do método proposto. É nesta fase que a marca d'água receberá todas as manipulações necessárias para torná-la robusta diante de possíveis ataques. Para isso, a criptografia empregada na marca d'água é baseada no algoritmo ACM. A técnica proposta por Arnold, Avez (1968) é uma transformação aplicada a uma imagem transformando os pixels da imagem como se fossem dispostos de forma aleatória. Porém, não modificando seu valor espectral. A operação é facilmente revertida, pois a transformação é periódica e depois de aplicada T vezes fornece novamente a imagem original, sendo T o período ACM da imagem.

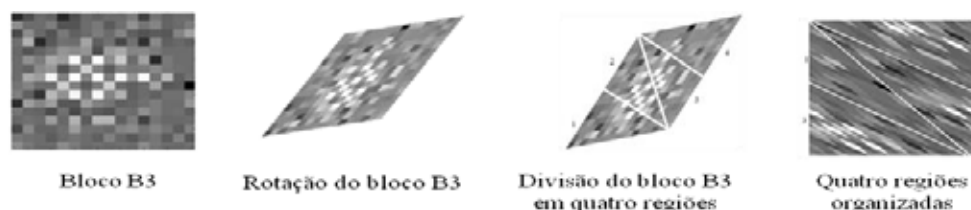
6.2.1 Criptografia da marca d'água

A criptografia empregada na marca d'água é baseada no algoritmo Arnold's Cat Map (ACM) descrito na seção 1.4, implementado no passo 2 do algoritmo descrito a seguir.

Passo 1: Após a obtenção dos quatro blocos B_1 , B_2 , B_3 e B_4 aplica-se $K = \left\lfloor \frac{T}{2} \right\rfloor$ vezes o

algoritmo proposto por Arnold separadamente em cada um dos quatro blocos da marca d'água decomposta, resultando em novos outros quatro blocos B_{1_crip} , B_{2_crip} , B_{3_crip} e B_{4_crip} . A Figura 54 ilustra a criptografia de um dos blocos com uma iteração.

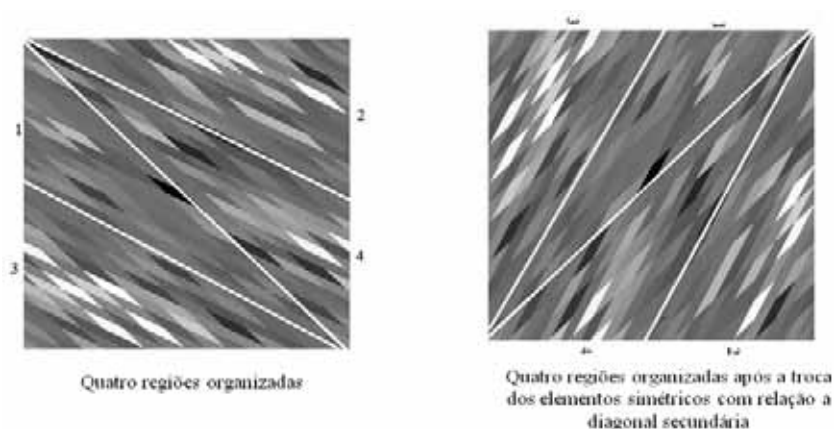
Figura 54 - Criptografia usando o algoritmo ACM.



Fonte: Elaborada pela própria autora.

Passo 2 : Em cada um dos blocos B_{1_crip} , B_{2_crip} , B_{3_crip} e B_{4_crip} será feita uma troca dos elementos que estão em posições simétricas em relação à diagonal secundária, gerando outros novos quatro blocos $B_{1_crip_diag}$, $B_{2_crip_diag}$, $B_{3_crip_diag}$ e $B_{4_crip_diag}$. Esta troca é ilustrada na Figura 55 realizada no bloco B_{3_crip} dando origem ao bloco $B_{3_crip_diag}$.

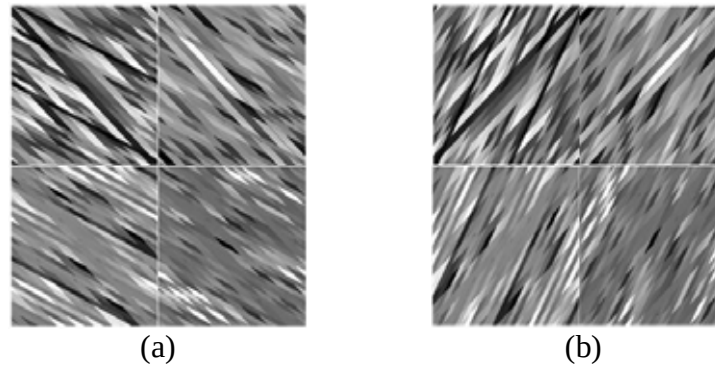
Figura 55 - Troca de posições dos elementos simétricos em relação à diagonal secundária em um bloco.



Fonte: Elaborada pela própria autora.

A troca de posições entre elementos simétricos em relação à diagonal secundária é uma implementação a mais na criptografia empregada buscando dar mais segurança ao processo. Além disso, assim como o algoritmo proposto por Arnold, esta implementação é uma operação facilmente aplicada em imagens de qualquer dimensão, especificamente as de dimensão quadrada, pelo fato de que computacionalmente as imagens são representadas por matrizes. A Figura 56 apresenta uma melhor comparação ao realizar esta implementação na criptografia.

Figura 56 - Troca de posições dos elementos simétricos em relação à diagonal secundária nos blocos criptografados pelo algoritmo ACM: (a) Blocos $B1_crip$, $B2_crip$, $B3_crip$ e $B4_crip$; (b) Blocos $B1_crip_diag$, $B2_crip_diag$, $B3_crip_diag$ e $B4_crip_diag$.



Fonte: Elaborada pela própria autora.

6.3 Terceira etapa

A terceira etapa se subdivide em mais duas que, em conjunto, representam a última etapa do processo de inserção, já que é nesta fase que os blocos $B1_crip_diag$, $B2_crip_diag$, $B3_crip_diag$ e $B4_crip_diag$ resultantes da criptografia empregada serão alocados na sub-banda HL_2 de HL_1 da imagem hospedeira processada na primeira etapa.

6.3.1 Inserção da marca d'água

Os blocos criptografados $B1_crip_diag$, $B2_crip_diag$, $B3_crip_diag$ e $B4_crip_diag$ da marca d'água são inseridos aleatoriamente por sobreposição nos quatro cantos da sub-banda HL_2 de HL_1 , da imagem hospedeira como ilustra a Figura 57.

Figura 57 - Inserção aleatória dos blocos nos quatro cantos da sub-banda HL_2 .

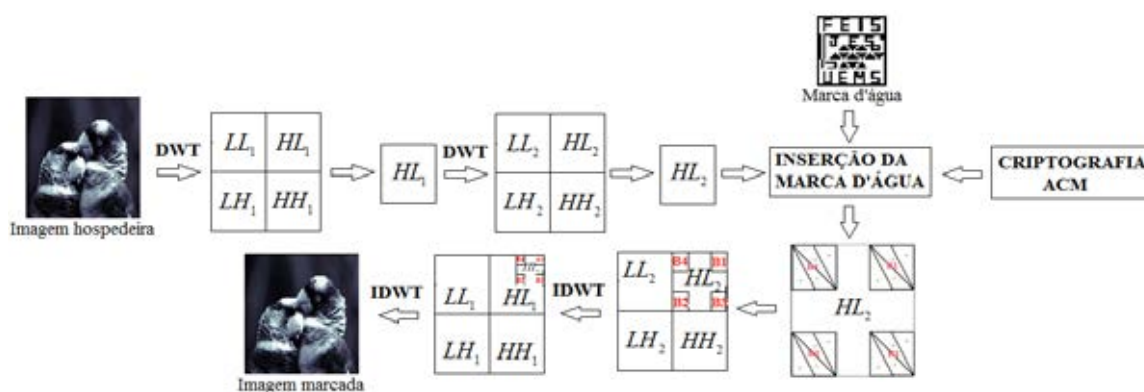


Fonte: Elaborada pela própria autora.

6.3.2 Aplicação da IDWT bidimensional para a reconstrução da imagem decomposta pela DWT bidimensional

Na primeira etapa as sub-bandas LL_2 , LH_2 e HH_2 da imagem hospedeira não são descartadas para que então após a inserção dos blocos $B_{1_crip_diag}$, $B_{2_crip_diag}$, $B_{3_crip_diag}$ e $B_{4_crip_diag}$ da sub-banda marcada HL_2 volte a compor o conjunto de sub-bandas de frequência. Para isso é aplicado primeiro uma vez a IDWTB resultando na primeira representação decomposta da imagem hospedeira, por fim, para obter a imagem hospedeira marcada basta aplicar mais uma vez a IDWTB. A Figura 58 ilustra todo o esquema de inserção da marca d'água, desde a preparação da imagem hospedeira, incluindo a criptografia, até a finalização da inserção.

Figura 58 - Finalização da etapa de inserção da marca d'água.



Fonte: Elaborada pela própria autora.

Como pode ser visto na Figura 58, o processo de inserção é baseado apenas numa dupla aplicação da IDWT bidimensional implementada por técnicas de criptografia.

6.4 Quarta etapa

Após a terceira etapa, a imagem está pronta para possivelmente ser enviada a terceiros em um canal de comunicação aberto e, portanto, está vulnerável a futuros ataques visando manipulações maldosas. É na quarta etapa que a integridade da marca d'água é verificada após o processo de extração. Portanto, pode-se dizer que a quarta etapa se subdivide em outras duas: uma envolvendo a extração da marca d'água e a outra envolvendo a verificação da

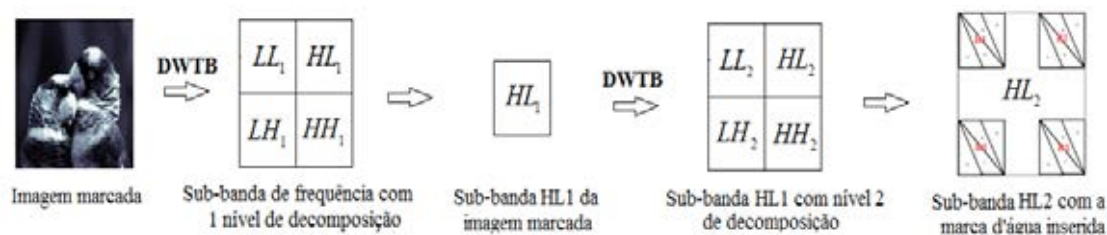
autenticidade da marca d'água extraída. Após as duas sub-etapas realizadas, será possível analisar o desempenho do método proposto.

6.4.1 Algoritmo de extração

O processo de extração segue sete passos. Trata-se de um método de extração semicego, ou seja, precisa apenas da imagem hospedeira e da marca d'água original para verificar a correlação existente.

Passo 1: Aplicar a DWTB na imagem marcada, este processo irá resultar nas quatro sub-bandas LL_2 , HL_2 , HH_2 e LH_2 que posteriormente será usada no passo 2 conforme a sub-banda escolhida no processo de inserção, que neste caso foi a HL_2 . A Figura 59 ilustra o processo descrito neste passo.

Figura 59 - Representação esquemática da extração da região onde a marca d'água foi inserida.



Fonte: Elaborada pela própria autora.

Passo 2: Como o método é semicego, a marca d'água inserida é disponibilizada para o receptor da imagem marcada. Porém, agora ela é usada apenas para a comparação com a marca d'água extraída, não precisando passar pelas transformações da etapa de inserção, como ilustrado na Figura 60.

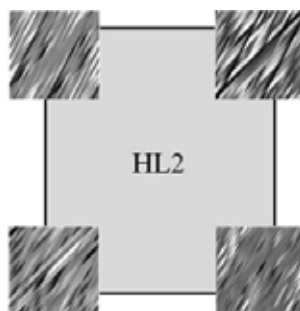
Figura 60 - Preparação da marca d'água inserida.



Fonte: Elaborada pela própria autora.

Passo 3: Junto com a marca d'água o proprietário pode fornecer o local onde a marca d'água foi inserida, portanto, basta ir aos quatro cantos da sub-banda HL_2 e retirar os quatro blocos inseridos. A Figura 61 ilustra o processo de inserção dos quatro blocos.

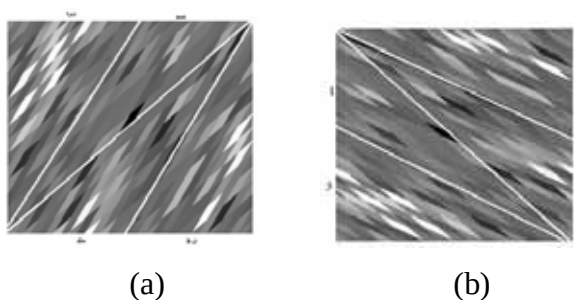
Figura 61 - Representação esquemática da extração dos blocos.



Fonte: Elaborada pela própria autora.

Passo 4: Após retirar os quatro blocos, é feita a troca em relação à diagonal secundária em cada uma dos quatro blocos retirados. A Figura 62 ilustra o processo descrito neste passo.

Figura 62 - Representação esquemática da troca de posições dos elementos simétricos em relação à diagonal secundária: (a) Quatro regiões organizadas após a troca dos elementos simétricos com relação à diagonal secundária no processo de criptografia; (b) Quatro regiões organizadas no processo inverso da troca dos elementos simétricos com relação à diagonal secundária no processo de criptografia.

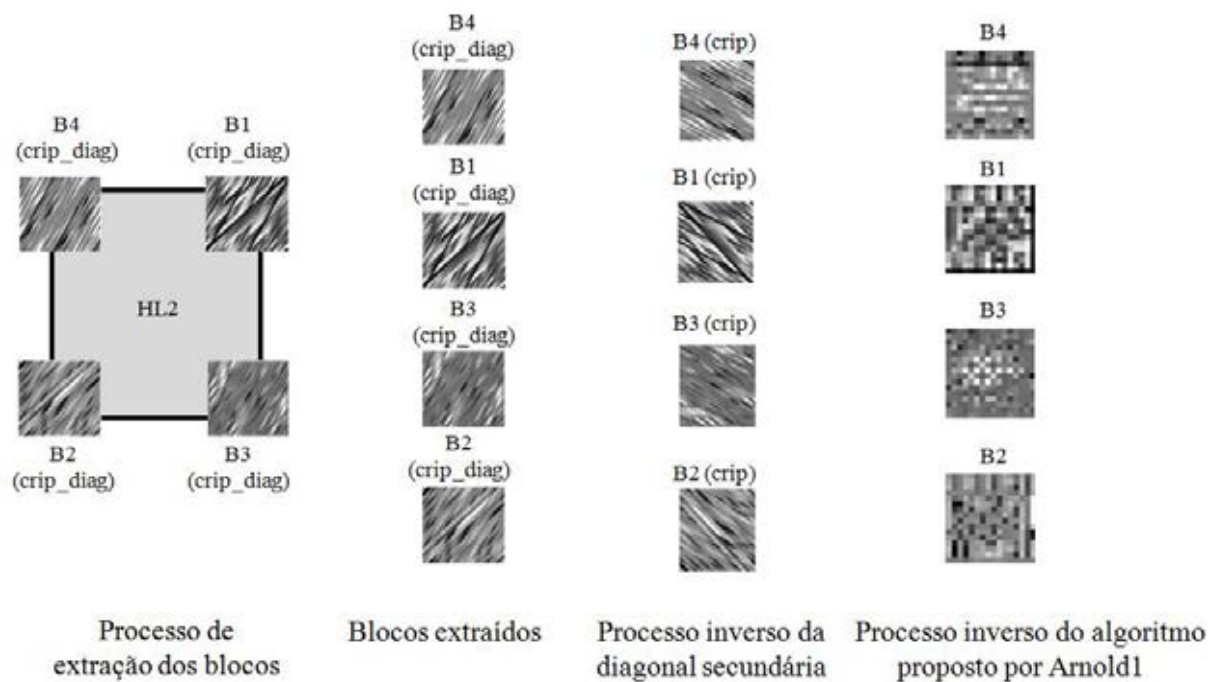


Fonte: Elaborada pela própria autora.

Passo 5: Aplicar o algoritmo Arnold K vezes, sendo, neste caso, $K = \left\lceil \frac{T}{2} \right\rceil$. Da mesma maneira como no processo de criptografar, o processo será repetido em cada bloco resultante do passo 4, já que após um número maior inteiro que $T/2$, sendo T o período de Arnold, cada bloco voltará a apresentar as mesmas características espectrais do início da iteração. A Figura 63 ilustra o resultado de todo o processo descrito neste passo.

Note que, a soma dos dois valores de K usados no passo 1 da inserção e no passo 5 da extração é igual a T , garantindo que na extração o bloco inserido seja recuperado.

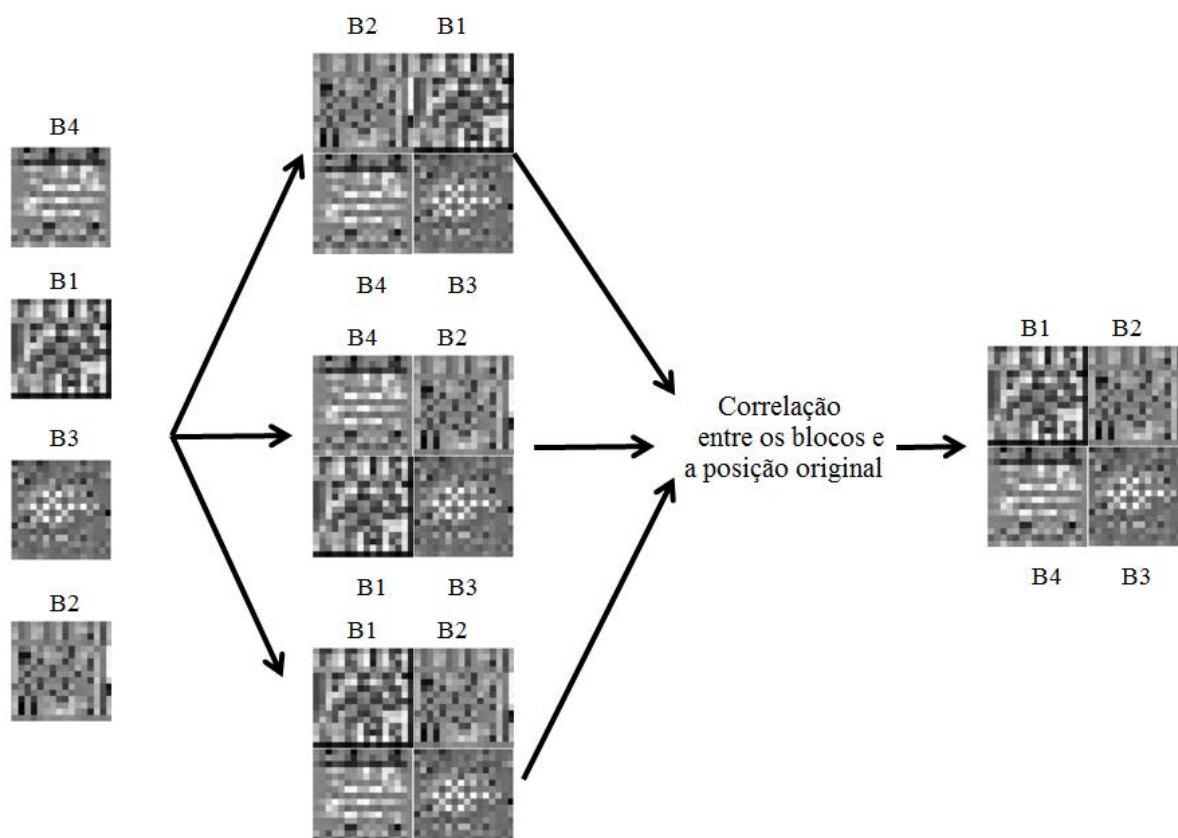
Figura 63 - Representação esquemática do passo 5.



Fonte: Elaborada pela própria autora.

Passo 6: Fazem-se as combinações possíveis dos blocos resultantes do passo 5, a combinação que apresentar correlação perfeita com a decomposição da marca adicionada é a escolhida. A Figura 64 ilustra o processo descrito neste passo.

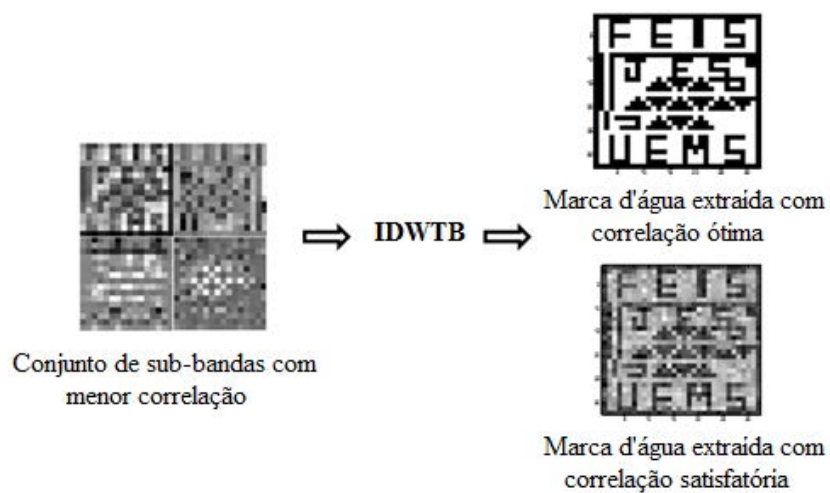
Figura 64 - Representação esquemática do cálculo da correlação.



Fonte: Elaborada pela própria autora.

Passo 7: Aplica-se a IDWT na combinação ótima para obter a marca d'água extraída. A Figura 65 ilustra o processo resultante do passo 7.

Figura 65 - Representação esquemática do resultado do passo 7.



Fonte: Elaborada pela própria autora.

Como se pode observar na Figura 65, uma das marcas d'água extraída apresenta correlação ótima ao contrário da outra. Porém, visualmente é considerada aceitável, pois é possível verificar que contém as mesmas características nos pixels mais escuros. Por isso, uma marca d'água com mais detalhes se torna mais robusta não sendo tão vulnerável a ataques.

Para comprovar a eficiência do método proposto são realizados ataques de compressão e adição de ruído, justamente porque o objetivo é fornecer uma marca d'água robusta diante a ataques naturalmente realizados no processo de transmissão, onde a imagem marcada poderá ser compactada e transmitida por um canal aberto de comunicação.

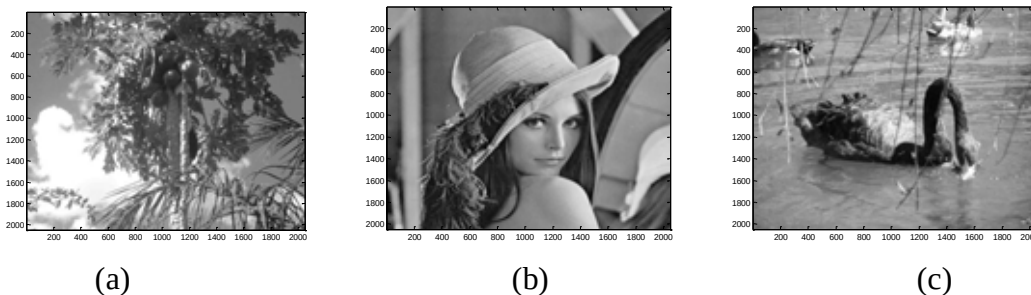
7 TESTES E RESULTADOS

Para testar a técnica de inserção, extração e verificação de marca d'água proposta no capítulo anterior foi usada a Transformada Wavelet Discreta Bidimensional, implementada com a função wavelet de Daubechies 6 (db6) (DAUBECHIES, 1992), escolhida após vários testes. A função wavelet db6 apresenta um número suficiente de momentos nulos para evidenciar detalhes da imagem e para propiciar uma boa reconstrução da mesma (DAUBECHIES, 1992). O processamento foi realizado usando o *Software* MATLAB[®].

Foram realizados um total de 6 experimentos, em cada um dos 6 experimentos foram aplicados quatro tipos de ataques, a compressão com perdas, um ataque ruidoso seguido de compressão e a compressão JPEG e a compressão proposta por Hajjara, Abdallah e Hudaib (2009). Diante dos vários outros tipos de ataques, esses são os ataques que naturalmente as imagens dispostas em banco de dados estão mais vulneráveis a sofrer.

Para testar a robustez da marca d'água, as imagens usadas compõem um conjunto de três imagens (Cass, Lenna e Cisne) como ilustra a Figura 66. Cada uma delas com duas dimensões diferentes, 2048×2048 e 1024×1024 pixels. Em cada variação da dimensão da imagem a marca d'água inserida também sofrerá variações. A variação da dimensão da marca d'água servirá para analisar em qual tipo de ataque a marca d'água se mantém mais robusta e se essa robustez depende ou não da sua dimensão em relação à dimensão da imagem hospedeira.

Figura 66 - Imagens: (a) Cass 2048×2048 pixels; (b) Lenna 2048×2048 pixels; (c) Cisne 2048×2048 pixels.

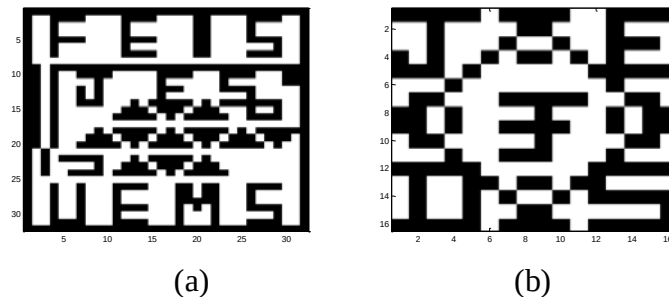


Fonte: Elaborada pela própria autora.

Como marcas d'água foram usadas duas imagens binárias de dimensão 32×32 pixels e 16×16 pixels, tamanho suficiente para se manter e verificar a robustez, principalmente nas imagens com dimensões maiores que 1024×1024 pixels. Pois, para o método proposto, a marca d'água não pode ter dimensão igual ou superior à dimensão da sub-banda HL_2 de HL_1 .

Caso contrário, toda a sub-banda seria substituída por ela, tornando-a alvo fácil de ataque. Essas marcas d'água são apresentadas na Figura 67.

Figura 67 - (a) Marca d'água 32×32 pixels; (b) Marca d'água 16×16 pixels.



Fonte: Elaborada pela própria autora.

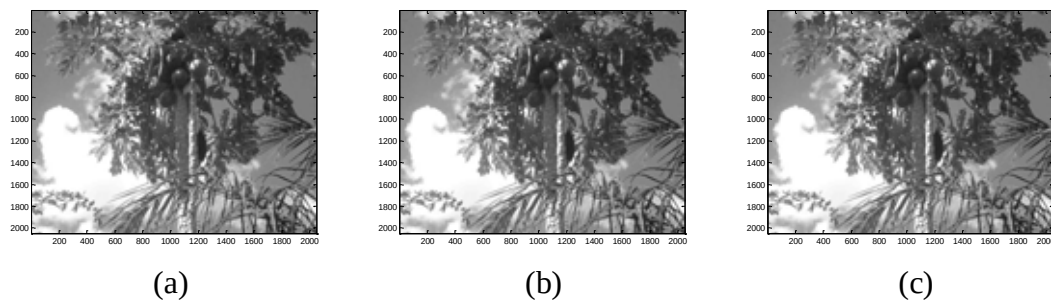
A robustez da marca d'água foi verificada pela seguinte sequência de ataques. Primeiro, a compressão, que foi aplicada em três níveis de taxa de compressão, 30%, 40% e 50%. O segundo ataque foi um conjunto da adição de 40% de ruído com posterior compressão, 30%, 40% e 50%, aplicando o limiar *Hard* (SILVA, 2008). O terceiro ataque foi a compressão JPEG, 30% e o quarto ataque foi a compressão com perda de 30% proposto pelo método de (HAJJARA; ABDALLAH; HUDAIB, 2009).

A eficiência do método proposto foi verificada de acordo com o valor das duas métricas especificadas na seção anterior, uma que mede o nível de distorção de uma imagem quando a mesma passa por alguma transformação chamada de PSNR e a outra a NC (correlação normalizada) (HUANG et. al., 2010). Os testes realizados foram analisados em especial com compressão com perda de 30% comparados com o método proposto por (HAJJARA; ABDALLAH; HUDAIB, 2009).

7.1 Experimento 1

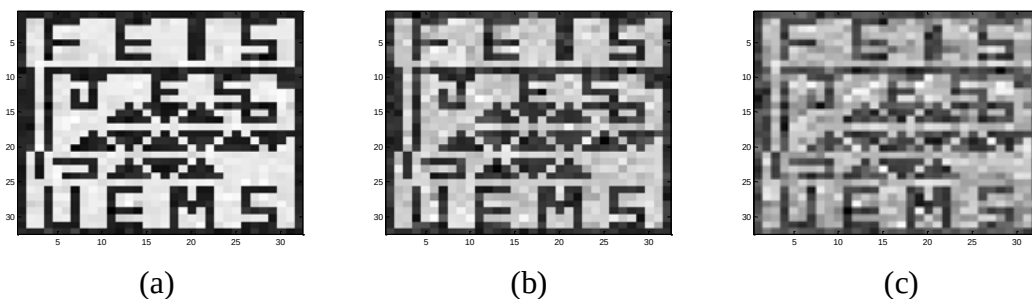
O primeiro teste teve como imagem hospedeira a imagem Cass (2048×2048 pixels), com PSNR 38,73 dB entre as imagens original e marcada com a marca d'água 32×32 pixels. Quando marcada com marca d'água 16×16 pixels a imagem hospedeira apresenta PSNR 41,79 dB em relação à imagem original. Na Figura 68 são apresentadas a imagem original, as marcas d'água e as imagens marcadas respectivamente. A análise visual das marcas d'água extraídas, após os respectivos ataques são apresentadas nas Figuras 69 a 71 e nas Figuras 72 e 73. Os valores de PSNR e NC, na Tabela 15.

Figura 68 - (a) Imagem original Cass 2048×2048 pixels; (b) Imagem marcada com a marca d'água 32×32 pixels e (c) Imagem marcada com a marca d'água 16×16 pixels.



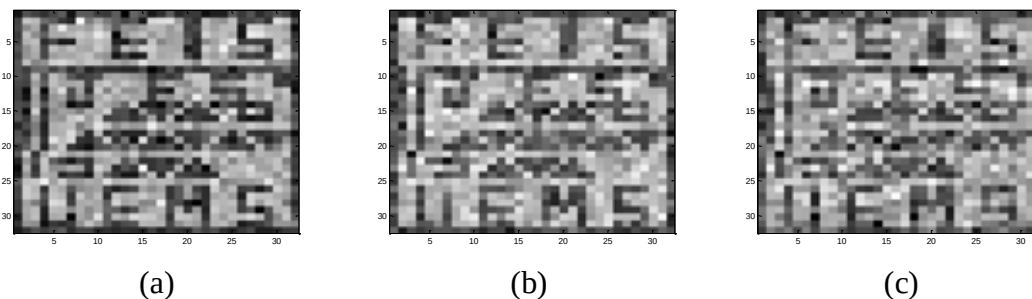
Fonte: Elaborada pela própria autora.

Figura 69 - Marcas d'água 32×32 pixels extraídas da imagem Cass 2048×2048 pixels, após ataque de compressão com TC de: (a) 30%; (b) 40% e (c) 50%.



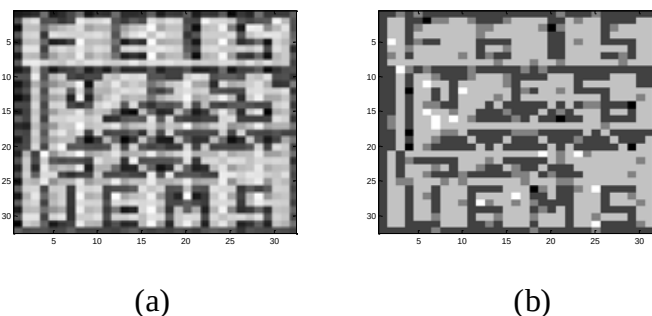
Fonte: Elaborada pela própria autora.

Figura 70 - Marcas d'água 32×32 pixels extraídas da imagem Cass 2048×2048 pixels após ataque ruidoso seguido de compressão com TC de: (a) 30%; (b) 40% e (c) 50%.



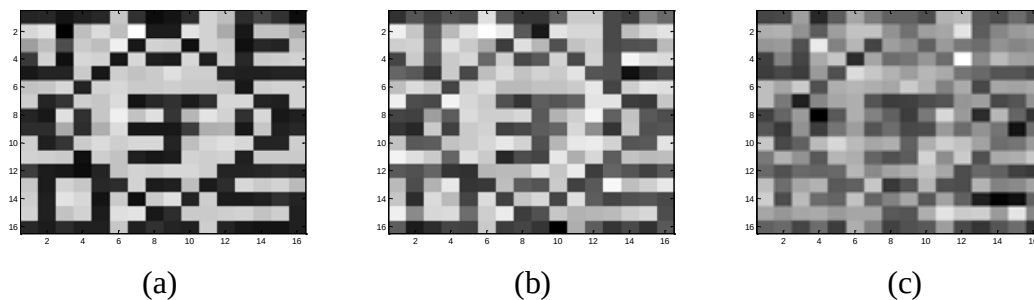
Fonte: Elaborada pela própria autora.

Figura 71 – Marcas d'água 32×32 pixels extraídas da imagem Cass 2048×2048 pixels após ataque de compressão JPEG (a) 30% e (b) Marca d'água extraída após inserção proposta pelo método Hajjara, Abdallah e Hudaib (2009) 30%.



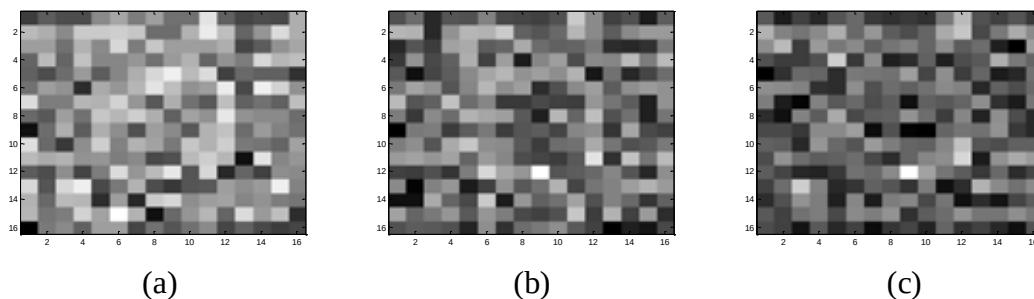
Fonte: Elaborada pela própria autora.

Figura 72 - Marcas d'água 16×16 pixels, extraídas da imagem Cass 2048×2048 pixels, após ataque de compressão com TC de: (a) 30%; (b) 40% e (c) 50%.



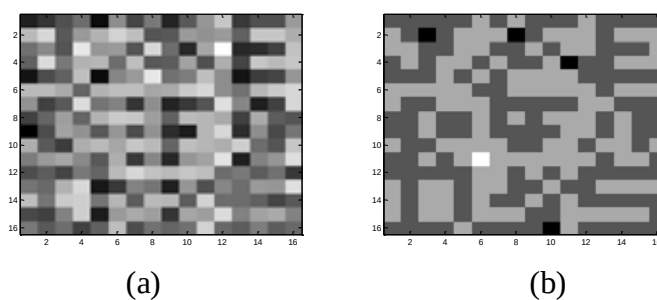
Fonte: Elaborada pela própria autora.

Figura 73 - Marcas d'água 16×16 pixels, extraídas da imagem Cass 2048×2048 pixels após ataque ruidoso seguido de compressão com TC de: (a) 30%; (b) 40% e (c) 50%.



Fonte: Elaborada pela própria autora.

Figura 74 - Marcas d'água 16×16 pixels, extraídas da imagem Cass 2048×2048 pixels após ataque de compressão JPEG (a) 30% e (b) Marca d'água extraída após inserção proposta pelo método Hajjara, Abdallah e Hudaib (2009) 30%.



Fonte: Elaborada pela própria autora.

Tabela 15 - Valores da PSNR e o nível de correlação após ataques de: Compressão com perda 30%; 40% e 50%; Ruidoso seguido de compressão 30%; 40% e 50%; Compressão JPEG 30% e Hajjara, Abdallah e Hudaib (2009) 30%, aplicados na imagem Cass 2048×2048 pixels.

Marca d'água 32×32 pixels			Marca d'água 16×16 pixels		
Ataques	PSNR (dB)	Correlação Normalizada (NC)	Ataques	PSNR (dB)	Correlação Normalizada (NC)
Compressão com perda 30%	37,4794	0,9953	Compressão com perda 30%	39,5769	0,9942
Compressão com perda 40%	35,3146	0,9772	Compressão com perda 40%	36,4107	0,9754
Compressão com perda 50%	32,2182	0,9084	Compressão com perda 50%	32,7510	0,8854
Ruidoso seguido de compressão 30%	31,9121	0,9180	Ruidoso seguido de compressão 30%	31,9121	0,8242
Ruidoso seguido de compressão 40%	31,4639	0,8960	Ruidoso seguido de compressão 40%	31,4640	0,8042
Ruidoso seguido de compressão 50%	30,2335	0,8403	Ruidoso seguido de compressão 50%	30,2341	0,7857
Compressão JPEG 30%	38,7073	0,9639	Compressão JPEG 30%	41,7930	0,9146
Hajjara, Abdallah e Hudaib (2009) 30%	33,2340	0,9376	Hajjara, Abdallah e Hudaib (2009) 30%	35,3679	0,7407

Fonte: Elaborada pela própria autora.

A Tabela 15 mostra que a marca d'água se apresentou mais robusta diante do ataque de compressão com perda de 30%, ocorrendo este fato em ambas as marcas, mesmo quando a dimensão da marca d'água é reduzida de 32×32 pixels para 16×16 pixels, ocorrendo uma redução na correlação de 0,11%.

Quando a marca d'água inserida é a de 32×32 pixels, no ataque ruidoso seguido de compressão pode-se observar que todas as métricas apresentam valores inferiores aos obtidos no ataque de (HAJJARA; ABDALLAH; HUDAIB, 2009). Quando o ataque é a compressão JPEG este fato não ocorre.

Quando a marca d'água inserida é a de 16×16 pixels, a métrica obtida em Hajjara, Abdallah e Hudaib (2009) não apresenta em nenhum dos níveis de ataque valor superior aos encontrados no método proposto nem mesmo quando a compressão é de 50% tanto na compressão com perda quando no ataque ruidoso seguido de compressão de 50% e no ataque de compressão JPEG.

Em geral pode-se dizer que, quando inserida a marca d'água na imagem Cass de 2048×2048 pixels, ambas as marcas d'água se apresentam robustas em até 40% de compressão e na compressão JPEG. Porém, a marca d'água de 32×32 pixels se apresenta frágil diante do ataque de compressão de 50% e em todos os níveis de ataque ruidoso, diferente da marca de dimensão 16×16 pixels, que não apresenta fragilidade diante dos demais ataques.

A Tabela 16 mostra a comparação das métricas obtidas quando é aplicado o método proposto por Hajjara, Abdallah e Hudaib (2009) com relação a compressão de 30%. É possível analisar que o método proposto neste trabalho apresenta uma correlação maior que do Hajjara, Abdallah e Hudaib (2009), independente da dimensão da marca d'água inserida. Apresentando uma melhora de 5,79% no valor da correção encontrada em Hajjara, Abdallah e Hudaib (2009) quando a marca d'água inserida é de 32×32 pixels e 25,49% quando a marca d'água é de 16×16 pixels. Diante dos demais ataques, Hajjara, Abdallah e Hudaib (2009) apresenta correlação superior apenas quando a marca d'água inserida é de 32×32 pixels para o ataque ruidoso seguido de compressão.

Tabela 16 - Valores do nível de correlação após ataque de compressão 30%; ataque ruidoso seguido de compressão 30%; ataque de compressão JPEG 30% e Hajjara, Abdallah e Hudaib (2009) 30%, aplicados na imagem Cass 2048×2048.

Marca d'água 32×32 pixels		Marca d'água 16×16 pixels	
Ataques	Correlação Normalizada (NC)	Ataques	Correlação Normalizada (NC)
Compressão com perda 30%	0,9953	Compressão com perda 30%	0,9942
Ruidoso seguido de compressão 30%	0,9180	Ruidoso seguido de compressão 30%	0,8242
Compressão JPEG 30%	0,9639	Compressão JPEG 30%	0,9146
Hajjara, Abdallah e Hudaib (2009) 30%	0,9376	Hajjara, Abdallah e Hudaib (2009) 30%	0,7407

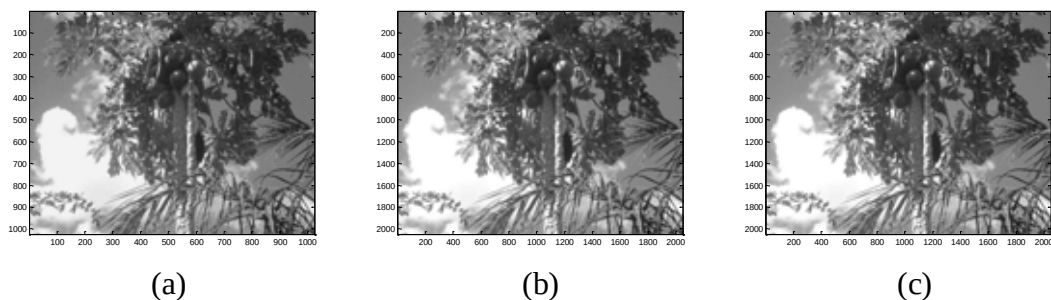
Fonte: Elaborada pela própria autora.

7.2 Experimento 2

O segundo teste teve como imagem hospedeira a imagem Cass, porém, com dimensão inferior a dimensão da imagem hospedeira no primeiro teste, sendo neste caso, de 1024×1024 pixels com PSNR de 31,67 dB entre as imagens original e marcada, quando usada a marca d'água de 32×32 pixels. Com a inserção da marca d'água de 16×16 pixels, a PSNR entre as

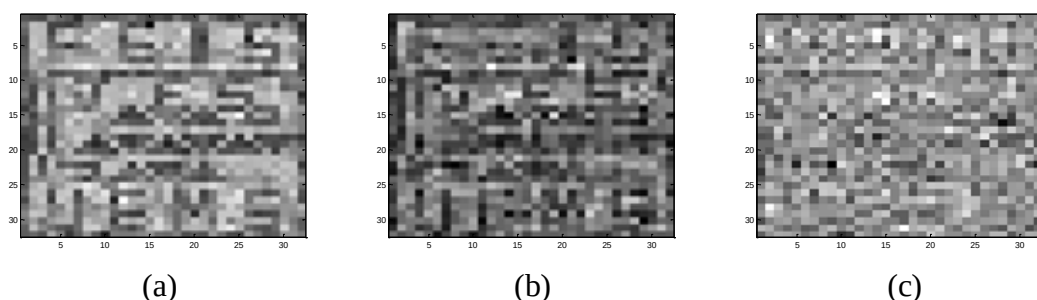
imagens original e marcada é de 35,66 dB. Na Figura 75, são apresentadas a imagem original, as marcas d'água e as imagens marcadas respectivamente. A análise visual das marcas d'água extraídas após os respectivos níveis de ataque são apresentadas nas Figuras 76 a 78 e nas Figuras 79 a 81, as métricas na Tabela 17.

Figura 75 - (a) Imagem original Cass 1024×1024 pixels; (b) Imagem (a) marcada com a marca d'água 32×32 pixels e (c) Imagem (a) marcada com a marca d'água 16×16 pixels.



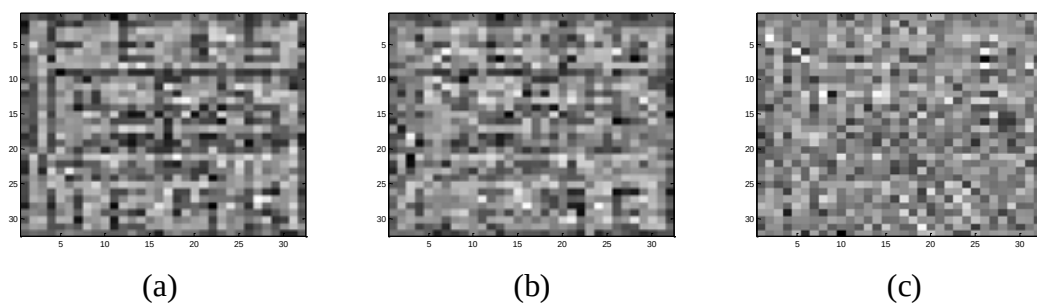
Fonte: Elaborada pela própria autora.

Figura 76 - Marcas d'água 32×32 pixels, extraídas da imagem Cass 1024×1024 pixels, após ataque de compressão com TC de: (a) 30%; (b) 40% e (c) 50%.



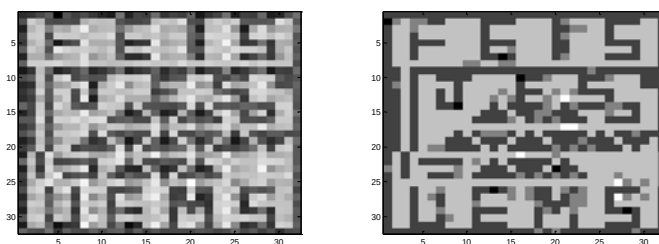
Fonte: Elaborada pela própria autora.

Figura 77 - Marcas d'água 32×32 pixels, extraídas da imagem Cass 1024×1024 pixels, após ataque ruidoso seguido de compressão com TC de: (a) 30%; (b) 40% e (c) 50%.



Fonte: Elaborada pela própria autora.

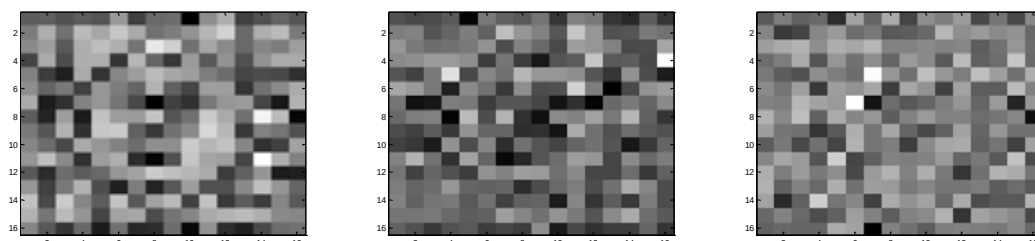
Figura 78 - Marcas d'água 32×32 pixels, extraídas da imagem Cass 1024×1024 pixels, após ataque de: compressão JPEG (a) 30% e (b) após inserção proposta pelo método Hajjara, Abdallah e Hudaib (2009) 30%.



(a) (b)

Fonte: Elaborada pela própria autora.

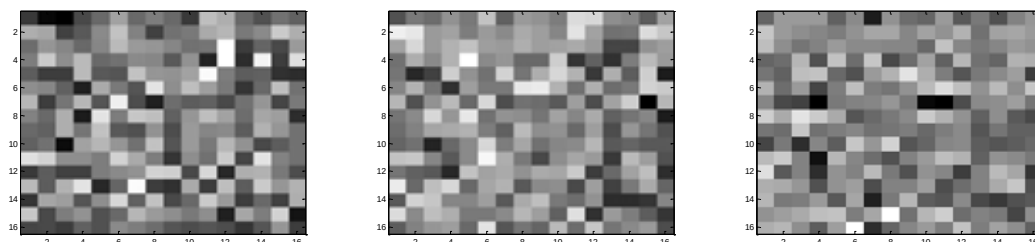
Figura 79 - Marcas d'água 16×16 pixels, extraídas da imagem Cass 1024×1024 pixels, após ataque de compressão com TC de: (a) 30%; (b) 40% e (c) 50%.



(a) (b) (c)

Fonte: Elaborada pela própria autora.

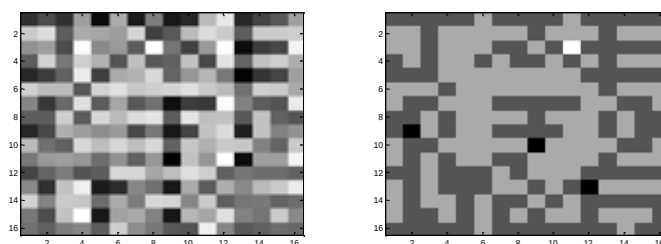
Figura 80 - Marcas d'água 16×16 pixels, extraídas da imagem Cass 1024×1024 pixels, após ataque ruidoso seguido de compressão com TC de: (a) 30%; (b) 40% e (c) 50%.



(a) (b) (c)

Fonte: Elaborada pela própria autora.

Figura 81 - Marcas d'água 16×16 pixels, extraídas da imagem Cass 1024×1024 pixels, após ataque de compressão JPEG (a) 30% e (b) após inserção proposta pelo método Hajjara, Abdallah e Hudaib (2009) 30%.



(a) (b)

Fonte: Elaborada pela própria autora.

Tabela 17 - Valores da PSNR e o nível de correlação após ataques de: Compressão com perda 30%; 40% e 50%; Ruidoso seguido de compressão 30%; 40% e 50%; Compressão JPEG 30% e Hajjara, Abdallah e Hudaib (2009) 30%, aplicados na imagem Cass 1024×1024 pixels.

Marca d'água 32×32 pixels			Marca d'água 16×16 pixels		
Ataques	PSNR (dB)	Correlação Normalizada (NC)	Ataques	PSNR (dB)	Correlação Normalizada (NC)
Compressão com perda 30%	29,4856	0,8523	Compressão com perda 30%	31,2761	0,8528
Compressão com perda 40%	26,8273	0,6859	Compressão com perda 40%	27,5996	0,6683
Compressão com perda 50%	23,5223	0,4482	Compressão com perda 50%	23,7304	0,4465
Ruidoso seguido de compressão 30%	29,6759	0,7925	Ruidoso seguido de compressão 30%	29,4496	0,7204
Ruidoso seguido de compressão 40%	27,0630	0,6900	Ruidoso seguido de compressão 40%	26,8555	0,5813
Ruidoso seguido de compressão 50%	23,9469	0,4123	Ruidoso seguido de compressão 50%	23,7288	0,3732
Compressão JPEG 30%	31,6673	0,9585	Compressão JPEG 30%	35,6527	0,9188
Hajjara, Abdallah e Hudaib (2009) 30%	31,9874	0,9514	Hajjara, Abdallah e Hudaib (2009) 30%	30,8659	0,8266

Fonte: Dados da pesquisa da autora.

Com a mudança da dimensão da imagem Cass de 2048×2048 pixels para 1024×1024 pixels, pode-se comprovar pela Tabela 17, que as marcas d'água inseridas, tanto a marca d'água de 32×32 pixels quanto a marca d'água de 16×16 pixels, se apresentam robustas diante do ataque de compressão JPEG com perda de 30%. Há uma redução no valor da correção encontrada quando a dimensão da marca d'água passa de 32×32 pixels para 16×16 pixels. Esta redução é maior do que quando a imagem hospedeira era de 2048×2048 pixels, sendo de 4,14%.

Quando a imagem é de 2048×2048 pixels o método proposto apresenta valores inferiores aos obtidos por Hajjara, Abdallah e Hudaib (2009), quando a marca d'água inserida é a de dimensão 32×32 pixels. Quando a marca d'água inserida é a de dimensão 16×16 pixels, o método proposto apresenta uma correlação superior a obtida por Hajjara, Abdallah e Hudaib (2009) no ataque de compressão com perda de 30%. Em todos os níveis de ataques, ambas as marcas d'água se apresentam robustas diante do ataque de compressão JPEG e diante do método proposto por (HAJJARA; ABDALLAH; HUDAIB, 2009). E ambas as marcas d'água

apresentam-se frágeis em todos os outros ataques. A Tabela 18 apresenta as métricas obtidas em todos os ataques de compressão de 30% comparadas com o método proposto por (HAJJARA; ABDALLAH; HUDAIB, 2009).

Tabela 18 - Valores do nível de correlação após ataque de compressão 30%; ataque ruidoso seguido de compressão 30%; ataque de compressão JPEG 30% e Hajjara, Abdallah e Hudaib (2009) 30%, aplicados na imagem Cass 1024×1024.

Marca d'água 32×32 pixels		Marca d'água 16×16 pixels	
Ataques	Correlação Normalizada (NC)	Ataques	Correlação Normalizada (NC)
Compressão com perda 30%	0,8523	Compressão com perda 30%	0,8528
Ruidoso seguido de compressão 30%	0,7925	Ruidoso seguido de compressão 30%	0,7204
Compressão JPEG 30%	0,9585	Compressão JPEG 30%	0,9188
Hajjara, Abdallah e Hudaib (2009) 30%	0,9514	Hajjara, Abdallah e Hudaib (2009) 30%	0,8266

Fonte: Elaborada pela própria autora.

Pode-ser observado que na situação de compressão JPEG com perda de 30%, o método proposto neste trabalho apresenta uma correlação maior que do método proposto por Hajjara, Abdallah e Hudaib (2009) em ambas marcas d'águas, apresentando uma melhora de 0,74% quando a marca inserida é de 32×32 pixels e 10,03% quando a marca d'água é de 16×16 pixels.

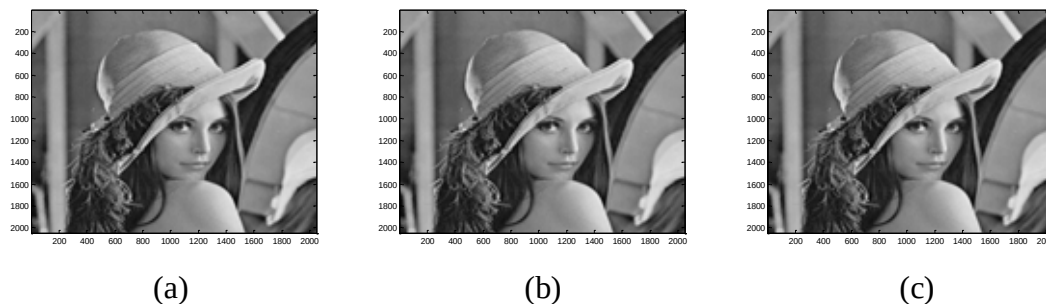
Diante dos demais ataques, quando a marca d'água inserida é a de dimensão 32×32 pixels, o método proposto por Hajjara, Abdallah e Hudaib (2009) apresenta correlação superior diante do ataque de compressão e ataque ruidoso seguido de compressão. Quando a marca d'água inserida é de 16×16 pixels Hajjara, Abdallah e Hudaib (2009) apresenta valores melhores apenas diante do ataque ruidoso seguido de compressão.

7.3 Experimento 3

O terceiro teste teve como imagem hospedeira a imagem Lenna de 2048×2048 pixels com PSNR 44,02 dB, entre as imagens original e marcada com a marca d'água 32×32 pixels. Quando marcada com marca d'água 16×16 pixels, a PSNR entre as imagens marcada e original foi de 48,95 dB. Na Figura 82 são apresentadas a imagem original, as marcas d'água e a imagem marcada. As marcas d'água extraídas após os respectivos níveis de ataque são

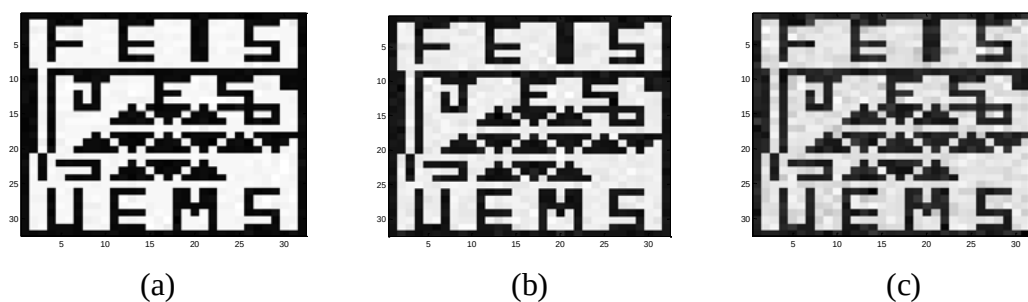
apresentadas nas Figuras 83 a 85 e nas Figuras 86 a 88 e os valores de PSNR e NC na Tabela 19.

Figura 82 - (a) Imagem original Lenna 2048×2048 pixels; (b) Imagem (a) marcada com marca d'água 32×32 pixels e (c) Imagem (a) marcada com marca d'água 16×16 pixels.



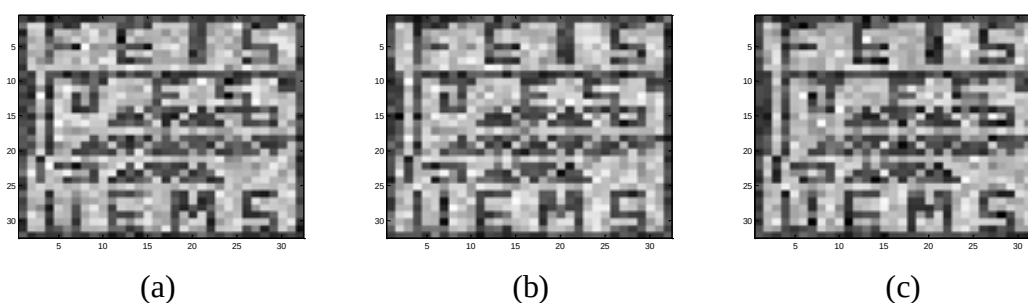
Fonte: Elaborada pela própria autora.

Figura 83 - Marcas d'água 32×32 pixels, extraídas da imagem Lenna 2048×2048 pixels, após ataque de compressão com TC de: (a) 30%; (b) 40% e (c) 50%.



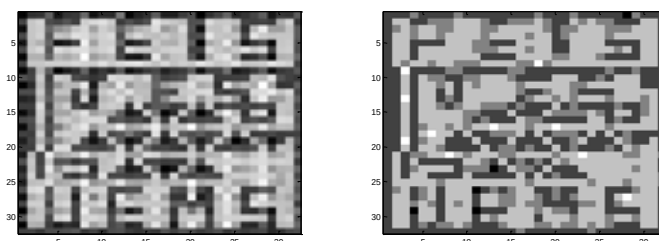
Fonte: Elaborada pela própria autora.

Figura 84 - Marcas d'água 32×32 pixels, extraídas da imagem Lenna 2048×2048 pixels, após ataque ruidoso seguido de compressão com TC de: (a) 30%; (b) 40% e (c) 50%.



Fonte: Elaborada pela própria autora.

Figura 85 - Marcas d'água 32×32 pixels, extraídas da imagem Lenna 2048×2048 pixels, após ataque de compressão JPEG (a) 30% e (b) após inserção proposta pelo método Hajjara, Abdallah e Hudaib (2009) 30%.



(a) (b)

Fonte: Elaborada pela própria autora.

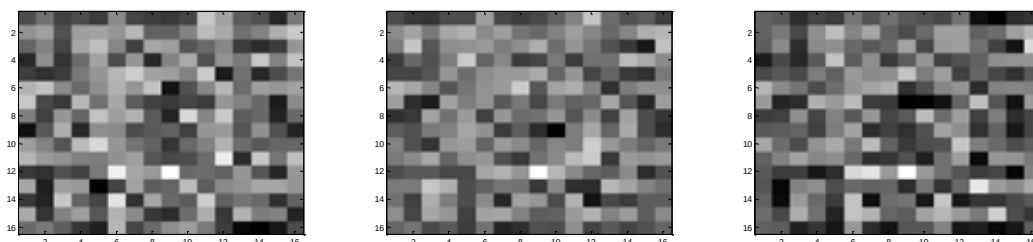
Figura 86 - Marcas d'água 16×16 pixels, extraídas da imagem Lenna 2048×2048 pixels, após ataque de compressão com TC de: (a) 30%; (b) 40% e (c) 50%.



(a) (b) (c)

Fonte: Elaborada pela própria autora.

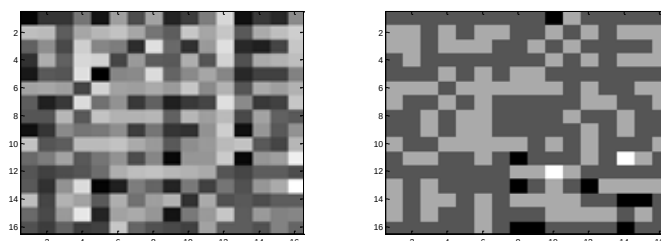
Figura 87 - Marcas d'água 16×16 pixels, extraídas da imagem Lenna 2048×2048 pixels, após ataque ruidoso seguido de compressão com TC de: (a) 30%; (b) 40% e (c) 50%.



(a) (b) (c)

Fonte: Elaborada pela própria autora.

Figura 88 - Marcas d'água 16×16 pixels, extraídas da imagem Lenna 2048×2048 pixels, após ataque de compressão JPEG (a) 30% e (b) após inserção proposta pelo método Hajjara, Abdallah e Hudaib (2009) 30%.



(a) (b)

Fonte: Elaborada pela própria autora.

Tabela 19 - Valores da PSNR e o nível de correlação após ataques de: Compressão com perda 30%, 40% e 50%; Ruidoso seguido de compressão 30%; 40% e 50%; Compressão JPEG 30% e Hajjara, Abdallah e Hudaib (2009) 30%, aplicados na imagem Lenna 2048×2048 pixels.

Marca d'água 32×32 pixels			Marca d'água 16×16 pixels		
Ataques	PSNR (dB)	Correlação Normalizada (NC)	Ataques	PSNR (dB)	Correlação Normalizada (NC)
Compressão com perda 30%	43,7090	0,9996	Compressão com perda 30%	47,9061	0,9992
Compressão com perda 40%	42,7035	0,9986	Compressão com perda 40%	45,5697	0,9967
Compressão com perda 50%	40,3940	0,9938	Compressão com perda 50%	41,8536	0,9886
Ruidoso seguido de compressão 30%	31,9077	0,9252	Ruidoso seguido de compressão 30%	31,9077	0,8420
Ruidoso seguido de compressão 40%	31,8901	0,9253	Ruidoso seguido de compressão 40%	31,8900	0,8626
Ruidoso seguido de compressão 50%	31,8277	0,9238	Ruidoso seguido de compressão 50%	31,8276	0,8397
Compressão JPEG 30%	44,077	0,9628	Compressão JPEG 30%	48,9523	0,9214
Hajjara, Abdallah e Hudaib (2009) 30%	30,8710	0,8934	Hajjara, Abdallah e Hudaib (2009) 30%	30,8754	0,7265

Fonte: Elaborada pela própria autora.

Os valores apresentados na Tabela 19 mostram que ambas marcas d'água se apresentam robustas diante do ataque de compressão de 30%. Houve uma redução de 0,04% no valor da correção obtida neste ataque, quando a marca d'água passa de 32×32 pixels para 16×16 pixels. Em todos os níveis de ataques, as métricas obtidas por Hajjara, Abdallah e Hudaib (2009) não apresentam valores superiores aos obtidos no método proposto. Nem mesmo quando a compressão é de 50%, tanto na compressão com perdas quanto no ataque ruidoso seguido de compressão de 50% e também a compressão JPEG.

Analisando todos os níveis de ataques, na imagem Lenna de 2048×2048 pixels, ambas as marcas d'água se apresentam robustas diante de todos os ataques de compressão com perda, ruidoso seguido de compressão e compressão JPEG. No caso em que a marca d'água é de 32×32 pixels essa robustez é mantida mesmo diante do ataque ruidoso seguido de compressão de 30%, 40% e 50%. Nenhuma das marcas, se apresentaram frágeis diante dos ataques.

Com os valores apresentados na Tabela 20 é possível comparar as métricas obtidas pelo método proposto nesta pesquisa com o método proposto por Hajjara, Abdallah e Hudaib (2009) diante do ataque de compressão com perda de 30%. Neste caso, o método proposto neste trabalho apresenta uma correlação maior que do método proposto por Hajjara, Abdallah e Hudaib (2009) em ambas marcas d'água, apresentando uma melhora de 10,62% quando inserida a marca d'água 32×32 pixels e 27,29% no caso da marca d'água de 16×16 pixels. Diante dos demais ataques Hajjara, Abdallah e Hudaib (2009) não apresenta correlação superior ao método proposto, como pode ser analisado na Tabela 20.

Tabela 20 - Valores médios do nível de correlação após ataque de compressão 30%; ataque ruidoso seguido de compressão 30%; ataque de compressão JPEG 30% e Hajjara, Abdallah e Hudaib (2009) 30%, aplicados na imagem Lenna 2048×2048 pixels.

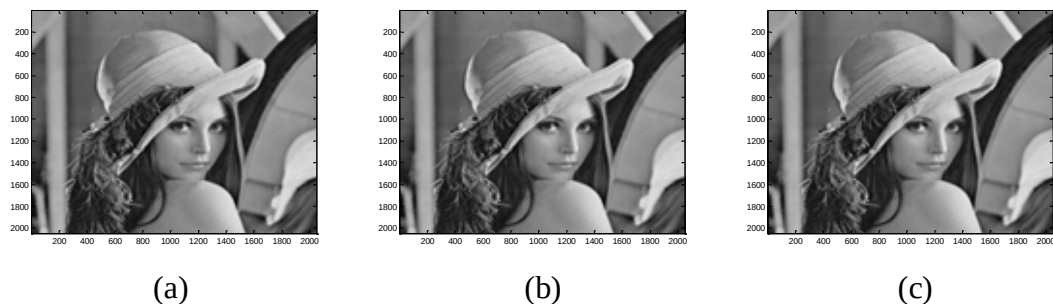
Marca d'água 32×32 pixels		Marca d'água 16×16 pixels	
Ataques	Correlação Normalizada (NC)	Ataques	Correlação Normalizada (NC)
Compressão com perda 30%	0,9996	Compressão com perda 30%	0,9992
Ruidoso seguido de compressão 30%	0,9252	Ruidoso seguido de compressão 30%	0,8420
Compressão JPEG 30%	0,9628	Compressão JPEG 30%	0,9214
Hajjara, Abdallah e Hudaib (2009) 30%	0,8934	Hajjara, Abdallah e Hudaib (2009) 30%	0,7265

Fonte: Elaborada pela própria autora.

7.4 Experimento 4

O quarto teste tem como imagem hospedeira a imagem Lenna de 1024×1024 pixels com PSNR 37,38 dB entre as imagens original e marcada quando usada a marca d'água 32×32 pixels e 41,10 dB com marca d'água 16×16 pixels. Na Figura 89 são apresentadas a imagem original, as marcas d'água e as imagens marcadas.

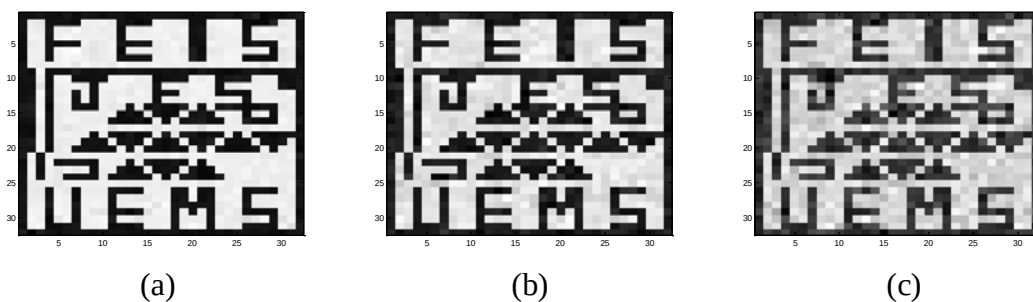
Figura 89 - (a) Imagem original 1024×1024 pixels; (b) Imagem (a) marcada com marca d'água 32×32 pixels e (c) Imagem (a) marcada com marca d'água 16×16 pixels.



Fonte: Elaborada pela própria autora.

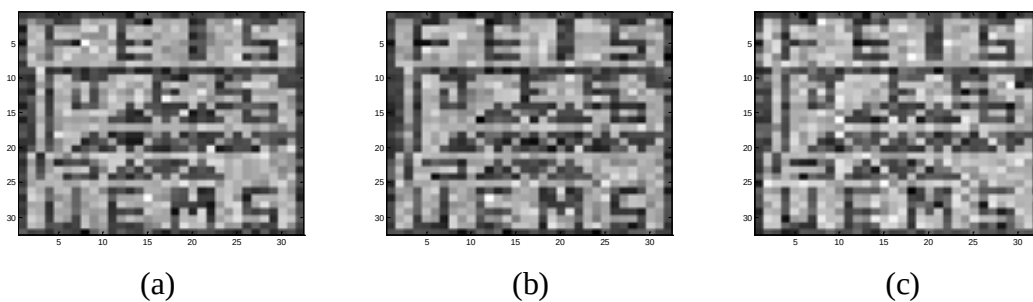
As marcas d'água extraídas de 32×32 pixels e 16×16 pixels são apresentadas nas Figuras 90 a 92 e nas Figuras 93 a 95, respectivamente.

Figura 90 - Marcas d'água 32×32 pixels, extraídas da imagem Lenna 1024×1024 pixels, após ataque de compressão com TC de: (a) 30%; (b) 40% e (c) 50%.



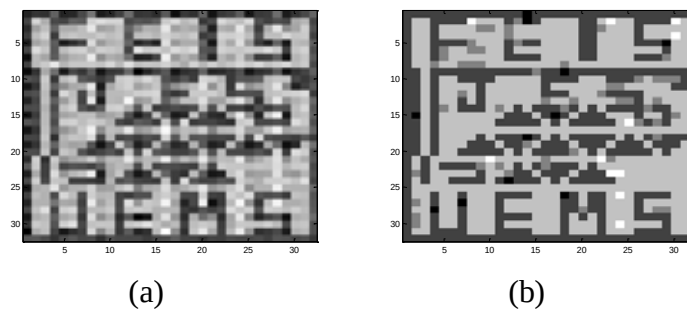
Fonte: Elaborada pela própria autora.

Figura 91 - Marcas d'água 32×32 pixels, extraídas da imagem Lenna 1024×1024 pixels, após ataque ruidoso seguido de compressão com TC de: (a) 30%; (b) 40% e (c) 50%.



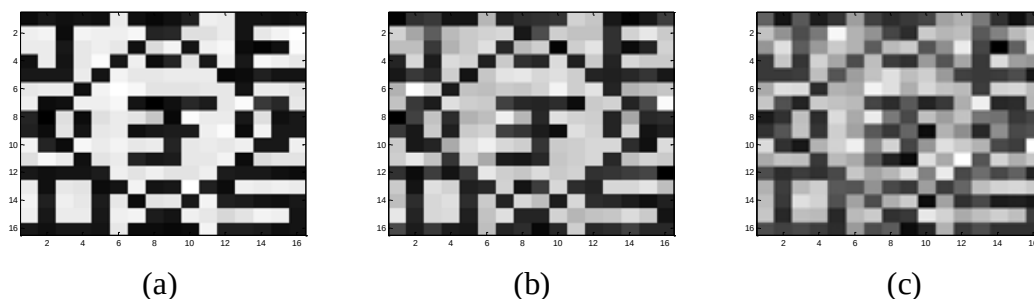
Fonte: Elaborada pela própria autora.

Figura 92 - Marcas d'água 32×32 pixels, extraídas da imagem Lenna 1024×1024 pixels, após ataque de compressão JPEG (a) 30% e (b) após inserção proposta pelo método Hajjara, Abdallah e Hudaib (2009) 30%.



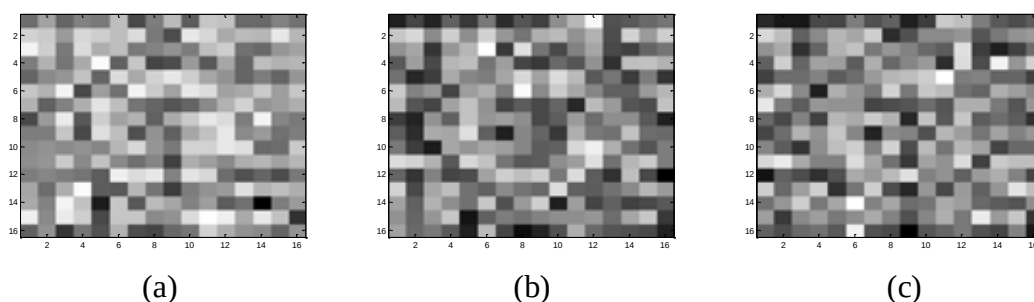
(a) (b)
Fonte: Elaborada pela própria autora.

Figura 93 - Marcas d'água 16×16 pixels, extraídas da imagem Lenna 1024×1024 pixels, após ataque de compressão com TC de: (a) 30%; (b) 40% e (c) 50%.



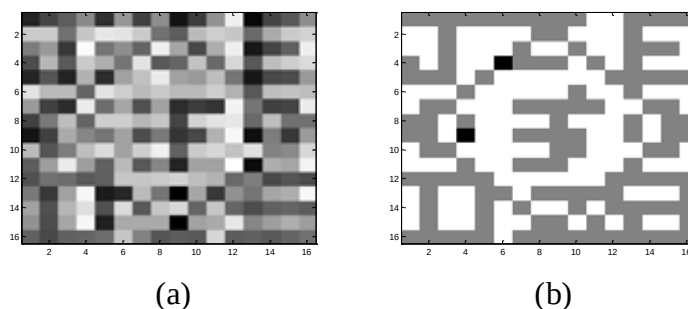
(a) (b) (c)
Fonte: Elaborada pela própria autora.

Figura 94 - Marcas d'água 16×16 pixels, extraídas da imagem Lenna 1024×1024 pixels, após ataque ruidoso seguido de compressão com TC de: (a) 30%; (b) 40% e (c) 50%.



(a) (b) (c)
Fonte: Elaborada pela própria autora.

Figura 95 - Marcas d'água 16×16 pixels, extraídas da imagem Lenna 1024×1024 pixels, após ataque de compressão JPEG (a) 30% e(b) após inserção proposta pelo método Hajjara, Abdallah e Hudaib (2009) 30%.



(a) (b)
Fonte: Elaborada pela própria autora.

Os valores de correlação e PSNR entre as imagens original e extraídas para os dois tipos de marcas d'água são exibidos na Tabela 21.

Tabela 21 - Valores da PSNR e o nível de correlação após ataques de: Compressão com perda 30%, 40% e 50%; Ruidoso seguido de compressão 30%; 40% e 50%; Compressão JPEG 30% e Hajjara, Abdallah e Hudaib (2009) 30%, aplicados na imagem Cass 1024×1024 pixels.

Marca d'água 32×32 pixels			Marca d'água 16×16 pixels		
Ataques	PSNR (dB)	Correlação Normalizada (NC)	Ataques	PSNR (dB)	Correlação Normalizada (NC)
Compressão com perda 30%	37,1698	0,9991	Compressão com perda 30%	40,4675	0,9983
Compressão com perda 40%	36,4651	0,9952	Compressão com perda 40%	39,0500	0,9905
Compressão com perda 50%	34,7916	0,9821	Compressão com perda 50%	36,3294	0,9593
Ruidoso seguido de compressão 30%	31,8211	0,9286	Ruidoso seguido de compressão 30%	31,9077	0,8512
Ruidoso seguido de compressão 40%	31,6590	0,9231	Ruidoso seguido de compressão 40%	31,8900	0,8572
Ruidoso seguido de compressão 50%	31,1961	0,9063	Ruidoso seguido de compressão 50%	31,8276	0,8271
Compressão JPEG 30%	37,5548	0,9609	Compressão JPEG 30%	41,3031	0,9244
Hajjara, Abdallah e Hudaib (2009) 30%	38,7761	0,9613	Hajjara, Abdallah e Hudaib (2009) 30%	41,2145	0,9205

Fonte: Elaborada pela própria autora.

Quando se muda a dimensão da imagem hospedeira Lenna de 2048×2048 pixels para 1024×1024 pixels, pode-se comprovar pela Tabela 21 que ambas as marcas d'água continuam se mantendo robustas diante do ataque de compressão com perda de 30% e que também houve uma redução no valor da correlação encontrado quando a dimensão da marca d'água passa de 32×32 pixels para 16×16 pixels, essa redução é de 0,08%.

Quando a imagem Lenna é de 2048×2048 pixels, o método proposto não apresentou valores inferiores aos de (HAJJARA; ABDALLAH; HUDAIB, 2009). Porém, com exceção da compressão JPEG para a marca d'água de 16×16 pixels e da compressão com perdas para as duas marcas d'água, o método proposto apresenta valores inferiores em todos os níveis, tornando ambas a marcas d'água frágeis. Analisando todos os níveis de ataques, na imagem Lenna 1024×1024 pixels, ambas as marcas d'água se apresentam robustas diante de todos os níveis de ataque de compressão com perdas e compressão JPEG, porém essa robustez já não é mantida diante dos níveis de ataque ruidoso seguido de compressão, tornando ambas as marcas frágeis.

A Tabela 22 apresenta a comparação entre o método proposto e o método Hajjara, Abdallah e Hudaib (2009) com compressão de 30%. Os valores exibidos atestam que o método proposto apresenta uma correlação maior do que o método de Hajjara, Abdallah e Hudaib (2009) em ambas marcas d'água. Apresentando uma melhora de 3,10% no caso da marca d'água de 32×32 pixels e 6,33% com a marca d'água de 16×16 pixels. Diante dos demais ataques com marca d'água de 32×32 pixels, Hajjara, Abdallah e Hudaib (2009) apresenta correlação superior as obtidas com o método proposto neste trabalho.

Tabela 22 - Valores médios do nível de correlação após ataque de compressão 30%, ataque ruidoso seguido de compressão 30%; ataque de compressão JPEG 30% e Hajjara, Abdallah e Hudaib (2009) 30%, aplicados na imagem Lenna 1024×1024 pixels.

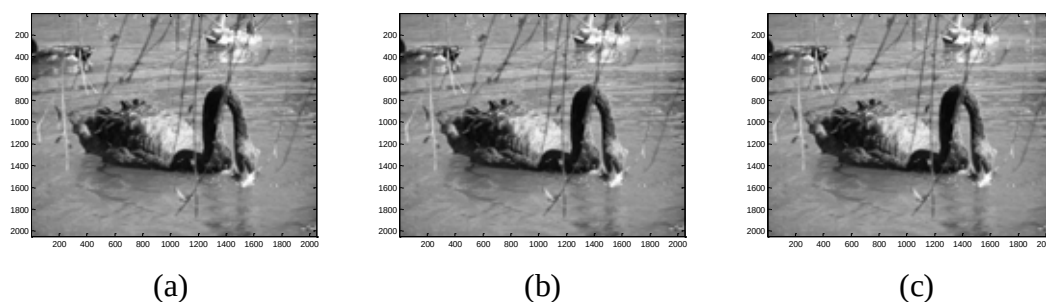
Marca d'água 32×32 pixels		Marca d'água 16×16 pixels	
Ataques	Correlação Normalizada (NC)	Ataques	Correlação Normalizada (NC)
Compressão com perda 30%	0,9921	Compressão com perda 30%	0,9827
Ruidoso seguido de compressão 30%	0,9193	Ruidoso seguido de compressão 30%	0,8451
Compressão JPEG 30%	0,9609	Compressão JPEG 30%	0,9244
Hajjara, Abdallah e Hudaib (2009) 30%	0,9613	Hajjara, Abdallah e Hudaib (2009) 30%	0,9205

Fonte: Elaborada pela própria autora.

7.5 Experimento 5

O quinto teste tem como imagem hospedeira a imagem Cisne de 2048×2048 pixels com PSNR 50,04 dB entre as imagens original e marcada quando usada a marca d'água 32×32 pixels e 55,93 dB com marca d'água 16×16 pixels. Na Figura 96 são apresentadas a imagem original, as marcas d'água e as imagens marcadas.

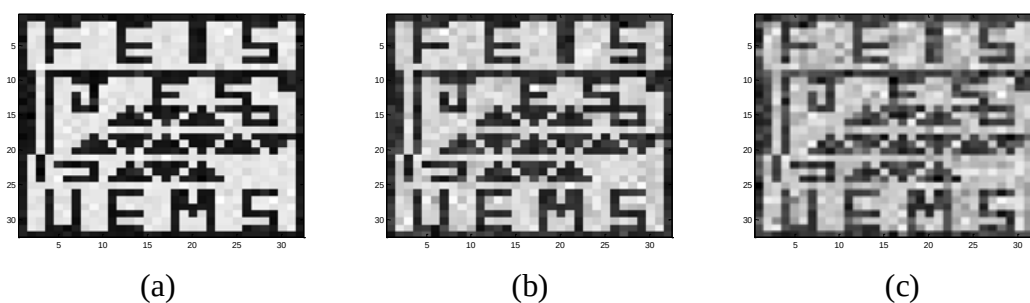
Figura 96 - (a) Imagem original Cisne 2048×2048 pixels; (b) Imagem marcada com a marca d'água 32×32 pixels e (c) Imagem marcada com a marca d'água 16×16 pixels.



Fonte: Elaborada pela própria autora.

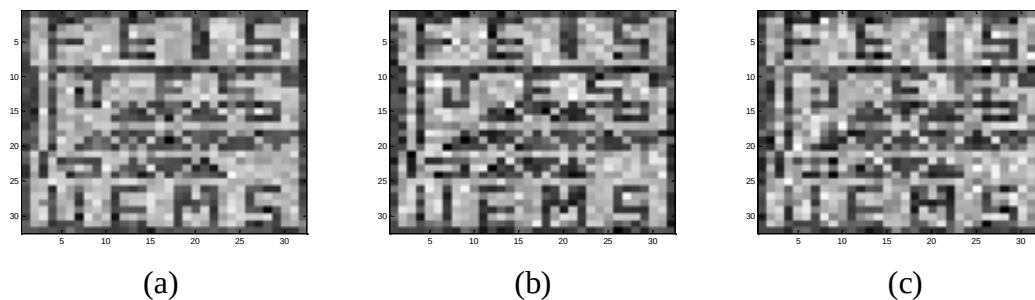
As marcas d'água de extraídas 32×32 pixels e 16×16 pixels são apresentadas nas Figuras 97 a 99 e nas Figuras 100 a 102, respectivamente.

Figura 97 - Marcas d'água 32×32 pixels, extraídas da imagem Cisne 2048×2048 pixels, após ataque de compressão com TC de: (a) 30%; (b) 40% e (c) 50%.



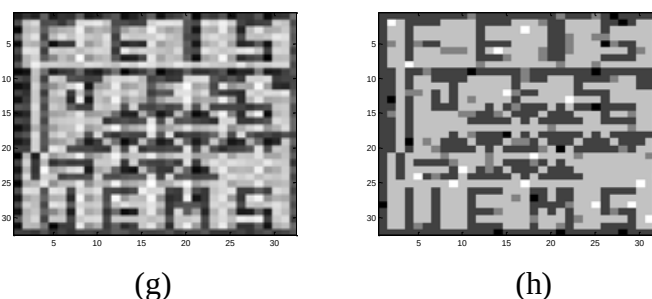
Fonte: Elaborada pela própria autora.

Figura 98 - Marcas d'água 32×32 pixels, extraídas da imagem Cisne 2048×2048 pixels, após ataque ruidoso seguido de compressão com TC de: (a) 30%; (b) 40% e (c) 50%.



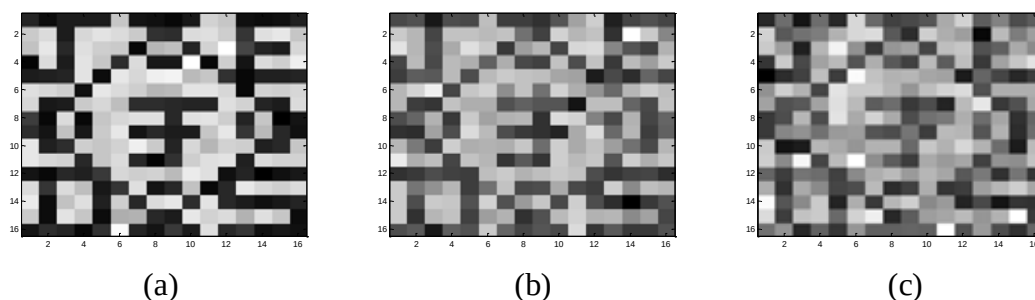
Fonte: Elaborada pela própria autora.

Figura 99 - Marcas d'água 32×32 pixels, extraídas da imagem Lenna Cisne 2048×2048 pixels, após ataque de compressão JPEG (a) 30% e (b) após inserção proposta pelo método Hajjara, Abdallah e Hudaib (2009) 30%.



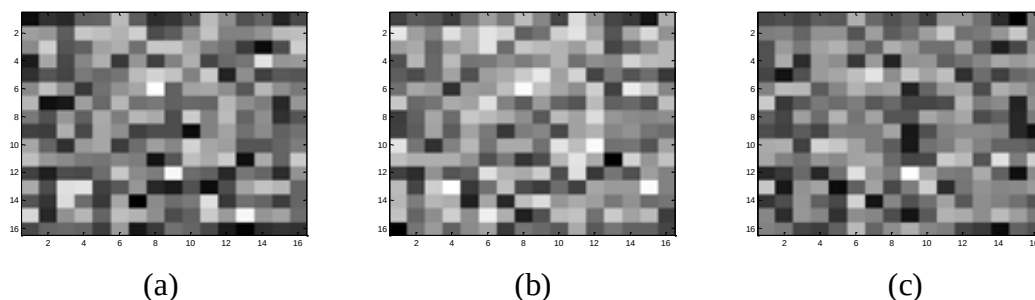
Fonte: Elaborada pela própria autora.

Figura 100 - Marcas d'água 16×16 pixels, extraídas da imagem Cisne 2048×2048 pixels, após ataque de compressão com TC de: (a) 30%; (b) 40% e (c) 50%.



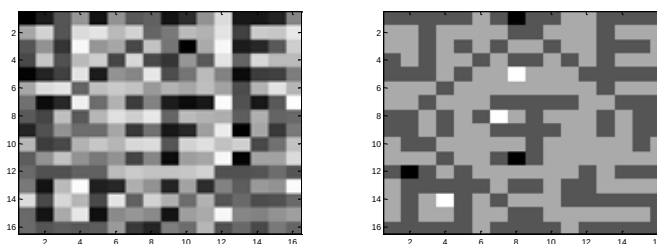
Fonte: Elaborada pela própria autora.

Figura 101 - Marcas d'água 16×16 pixels, extraídas da imagem Cisne 2048×2048 pixels, após ataque ruidoso seguido de compressão com TC de: (a) 30%; (b) 40% e (c) 50%.



Fonte: Elaborada pela própria autora.

Figura 102 - Marcas d'água 16×16 pixels, extraídas da imagem Lenna Cisne 2048×2048 pixels, após ataque de compressão JPEG (a) 30% e(b) após inserção proposta pelo método Hajjara, Abdallah e Hudaib (2009) 30%.



(a)

(b)

Fonte: Elaborada pela própria autora.

Os valores de correlação e PSNR entre as imagens original e extraídas para os dois tipos de marcas d'água são exibidos na Tabela 23.

Tabela 23 - Valores da PSNR e o nível de correlação após ataques de: Compressão com perda 30%, 40% e 50%; Ruidoso seguido de compressão 30%; 40% e 50%; Compressão JPEG 30% e Hajjara, Abdallah e Hudaib (2009) 30%, aplicados na imagem Cisne 2048×2048 pixels.

Marca d'água 32×32 pixels			Marca d'água 16×16 pixels		
Ataques	PSNR (dB)	Correlação Normalizada (NC)	Ataques	PSNR (dB)	Correlação Normalizada (NC)
Compressão com perda 30%	43,8338	0,9965	Compressão com perda 30%	44,6085	0,9928
Compressão com perda 40%	38,2093	0,9848	Compressão com perda 40%	38,2117	0,9633
Compressão com perda 50%	33,7424	0,9459	Compressão com perda 50%	33,7455	0,9205
Ruidoso seguido de compressão 30%	31,9034	0,9255	Ruidoso seguido de compressão 30%	31,8234	0,8342
Ruidoso seguido de compressão 40%	31,4471	0,9124	Ruidoso seguido de compressão 40%	31,3717	0,8351
Ruidoso seguido de compressão 50%	43,8338	0,9965	Ruidoso seguido de compressão 50%	30,3030	0,7771
Compressão JPEG 30%	38,2093	0,9848	Compressão JPEG 30%	56,0850	0,9193
Hajjara, Abdallah e Hudaib (2009) 30%	35,8721	0,9529	Hajjara, Abdallah e Hudaib (2009) 30%	32,8763	0,8744

Fonte: Elaborada pela própria autora.

A Tabela 23 mostra que na imagem Cisne de 2048×2048 pixels ambas marcas d'água se apresentaram robustas diante do ataque de compressão de 30%. Houve uma redução de 0,37% no valor da correção quando a marca d'água passa de 32×32 pixels para 16×16 pixels.

Em todos os níveis do ataque ruidoso seguido de compressão as métricas obtidas foram inferiores as métricas encontradas em Hajjara, Abdallah e Hudaib (2009) o qual apresenta valores superiores aos obtidos pelo método proposto em ambas as marcas d'água inseridas.

Analisando todos os níveis de ataques, as marcas d'água se apresentam robustas diante da maioria dos níveis de ataque de compressão com perda e compressão JPEG e se apresentaram frágeis diante dos níveis de ataque ruidoso seguido de compressão e também quando a compressão é de 50% quando inserida a marca d'água 32×32 pixels.

Na Tabela 24, para fins de comparação, são apresentados os valores de correlação obtidos com o método proposto e o método de Hajjara, Abdallah e Hudaib (2009) apenas para o caso de compressão de 30% para ambas marcas d'água. O método proposto apresenta um desempenho melhor que Hajjara, Abdallah e Hudaib (2009) em ambas marcas d'água. Apresentando uma melhora de 4,37% quando a marca d'água inserida é de 32×32 pixels e 11,92% com a de 16×16 pixels. E para os demais ataques Hajjara, Abdallah e Hudaib (2009) apresenta correlação superior as obtidas em ambas marcas d'água diante do ataque ruidoso seguido de compressão. Com o ataque de compressão JPEG, em ambas as marcas Hajjara, Abdallah e Hudaib (2009) apresenta valores inferiores.

Tabela 24 - Valores médios do nível de correlação após ataque de compressão 30%, ataque ruidoso seguido de compressão 30%; ataque de compressão JPEG 30% e Hajjara, Abdallah e Hudaib (2009) 30%, aplicados na imagem Cisne 2048×2048 pixels.

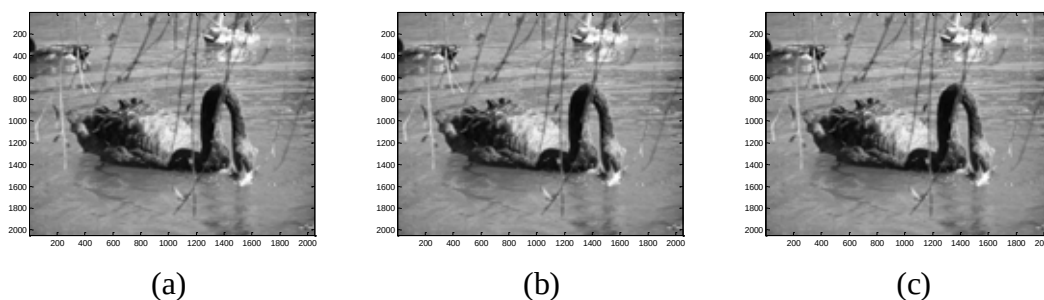
Marca d'água 32×32 pixels		Marca d'água 16×16 pixels	
Ataques	Correlação Normalizada (NC)	Ataques	Correlação Normalizada (NC)
Compressão com perda 30%	0,9965	Compressão com perda 30%	0,9928
Ruidoso seguido de compressão 30%	0,9255	Ruidoso seguido de compressão 30%	0,8342
Compressão JPEG 30%	0,9602	Compressão JPEG 30%	0,9193
Hajjara, Abdallah e Hudaib (2009) 30%	0,9529	Hajjara, Abdallah e Hudaib (2009) 30%	0,8744

Fonte: Elaboração da própria autora.

7.6 Experimento 6

O sexto teste tem como imagem hospedeira a imagem Cisne de 1024×1024 pixels com PSNR 41,32 dB entre as imagens original e marcada quando usada a marca d'água 32×32 pixels e 45,01 dB com marca d'água 16×16 pixels. Na Figura 103 são apresentadas a imagem original, as marcas d'água e as imagens marcadas.

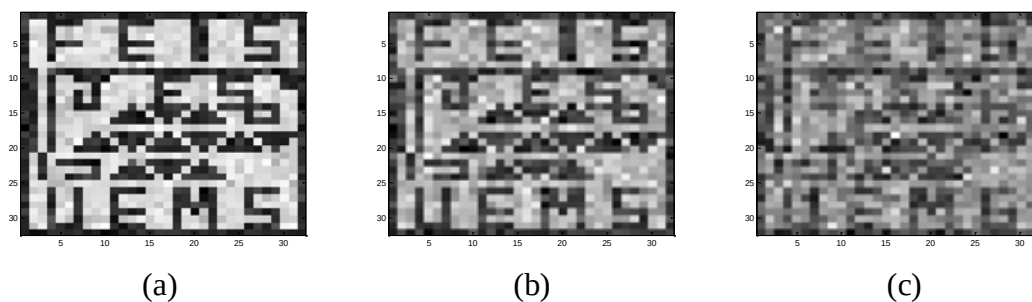
Figura 103 - (a) Imagem original Cisne 1024×1024 pixels; (b) Imagem marcada com a marca d'água 32×32 pixels e (c) Imagem marcada com a marca d'água 16×16 pixels.



Fonte: Elaborada pela própria autora.

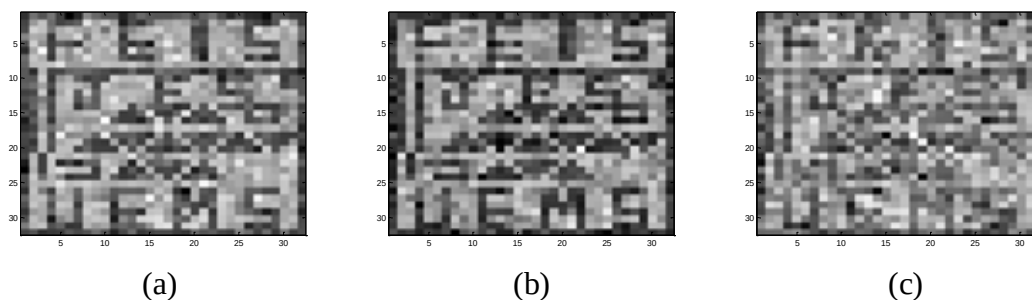
As marcas d'água extraídas de 32×32 pixels e 16×16 pixels são apresentadas nas Figuras 104 a 106 e nas Figuras 107 a 109, respectivamente.

Figura 104 - Marcas d'água 32×32 pixels, extraídas da imagem Cisne 1024×1024 após ataque de compressão com TC de: (a) 30%; (b) 40% e (c) 50%.



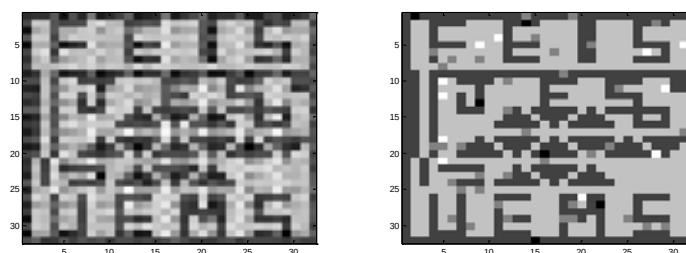
Fonte: Elaborada pela própria autora.

Figura 105 - Marcas d'água 32×32 pixels, extraídas da imagem Cisne 1024×1024 pixels, após ataque ruidoso seguido de compressão com TC de: (a) 30%; (b) 40% e (c) 50%.



Fonte: Elaborada pela própria autora.

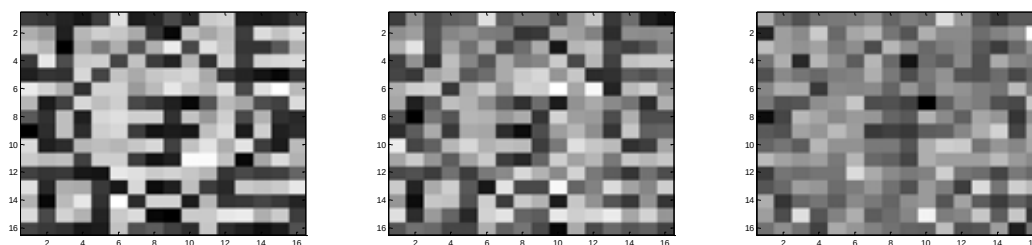
Figura 106 - Marcas d'água 32×32 pixels, extraídas da imagem Lenna Cisne 1024×1024 pixels, após ataque de compressão JPEG (a) 30% e (b) após inserção proposta pelo método Hajjara, Abdallah e Hudaib (2009) 30%.



(a) (b)

Fonte: Elaborada pela própria autora.

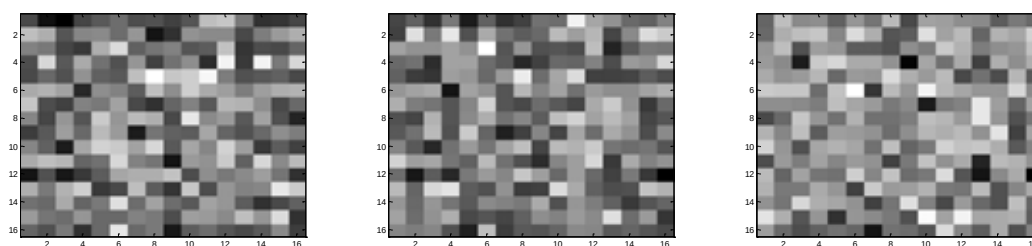
Figura 107 - Marcas d'água 16×16 pixels, extraídas da imagem Cisne 1024×1024 após ataque de compressão com TC de: (a) 30%; (b) 40% e (c) 50%.



(a) (b) (c)

Fonte: Elaborada pela própria autora.

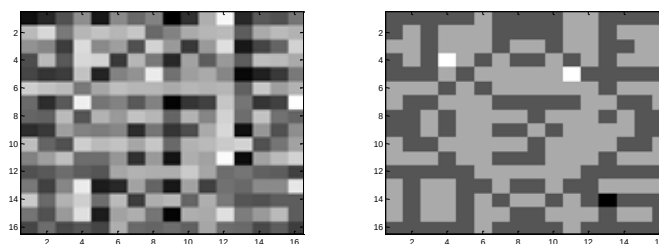
Figura 108 - Marcas d'água 16×16 pixels, extraídas da imagem Cisne 1024×1024 pixels, após ataque ruidoso seguido de compressão com TC de: (a) 30%; (b) 40% e (c) 50%.



(a) (b) (c)

Fonte: Elaborada pela própria autora.

Figura 109 - Marcas d'água 16×16 pixels, extraídas da imagem Lenna Cisne 1024×1024 pixels, após ataque de compressão JPEG (a) 30% e(b) após inserção proposta pelo método Hajjara, Abdallah e Hudaib (2009) 30%.



(g)

(h)

Fonte: Elaborada pela própria autora.

Os valores de correlação e PSNR entre as imagens original e extraídas para os dois tipos de marcas d'água são exibidos na Tabela 25 no qual mostra que ambas as marcas d'água se mantêm robustas quando inseridas na imagem Cisne de 1024×1024 pixels diante do ataque de compressão de 30%, havendo uma redução de 0,42% no valor da correção quando a marca d'água passa de 32×32 pixels para 16×16 pixels. Em todos os níveis de ataque ruidoso seguido de compressão, os valores obtidos por Hajjara, Abdallah e Hudaib (2009) apresentam-se superiores aos obtidos pelo método proposto em ambas as marcas d'água. Quando a marca inserida é a de 32×32 pixels até mesmo o ataque de compressão JPEG apresenta métrica inferior ao obtido por (HAJJARA; ABDALLAH; HUDAIB, 2009). Isso não acontece quando a marca d'água passa a ser a de 16×16 pixels diante do mesmo ataque.

Tabela 25 - Valores da PSNR e o nível de correlação após ataques de: Compressão com perda 30%, 40% e 50%; Ruidoso seguido de compressão 30%; 40% e 50%; Compressão JPEG 30% e Hajjara, Abdallah e Hudaib (2009) 30%, aplicados na imagem Cisne 1024×1024 pixels.

Marca d'água 32×32 pixels			Marca d'água 16×16 pixels		
Ataques	PSNR (dB)	Correlação Normalizada (NC)	Ataques	PSNR (dB)	Correlação Normalizada (NC)
Compressão com perda 30%	37,3175	0,9833	Compressão com perda 30%	38,4179	0,9791
Compressão com perda 40%	33,0065	0,9327	Compressão com perda 40%	33,3695	0,9024
Compressão com perda 50%	28,6309	0,7996	Compressão com perda 50%	28,7473	0,7087
Ruidoso seguido de compressão 30%	31,0875	0,9036	Ruidoso seguido de compressão 30%	31,0695	0,8311
Ruidoso seguido de compressão 40%	29,5713	0,8554	Ruidoso seguido de compressão 40%	29,5493	0,7596
Ruidoso seguido de compressão 50%	27,0748	0,7482	Ruidoso seguido de compressão 50%	27,0662	0,6461
Compressão JPEG 30%	41,3961	0,9615	Compressão JPEG 30%	45,0207	0,9222
Hajjara, Abdallah e Hudaib (2009) 30%	41,4578	0,9731	Hajjara, Abdallah e Hudaib (2009) 30%	41,6790	0,9197

Fonte: Elaborada pela própria autora.

Analizando todos os níveis de ataques, na imagem Cisne 1024×1024 pixels ambas as marcas d'água se apresentaram robustas diante do ataque de compressão com perda de 30% e frágeis diante dos demais níveis de compressão, tanto de compressão com perda quanto ruidoso seguido de compressão.

Na Tabela 26 apresentam-se os valores da correlação obtidos no ataque de compressão de 30% para comparação entre com o método de Hajjara, Abdallah e Hudaib (2009) e o método proposto. Neste caso o método proposto neste trabalho apresenta correlação maior que o método proposto por Hajjara, Abdallah e Hudaib (2009) em ambas marcas d'água apresentando uma melhora de 0,43% e 5,48% quando a marca d'água é de 16×16 pixels. Diante dos demais ataques Hajjara, Abdallah e Hudaib (2009) apresenta correlação superior aos obtidos em ambas marca d'água diante do ataque ruidoso seguido de compressão e diante do ataque de compressão JPEG com marca 16×16 pixels Hajjara, Abdallah e Hudaib (2009) apresenta valor inferior.

Tabela 26 - Valores médios do nível de correlação após ataque de compressão 30%; ataque ruidoso seguido de compressão 30%; ataque de compressão JPEG 30% e Hajjara, Abdallah e Hudaib (2009) 30%, aplicados na imagem Cisne 1024×1024 pixels.

Marca d'água 32×32 pixels		Marca d'água 16×16 pixels	
Ataques	Correlação Normalizada (NC)	Ataques	Correlação Normalizada (NC)
Compressão com perda 30%	0,9833	Compressão com perda 30%	0,9791
Ruidoso seguido de compressão 30%	0,9036	Ruidoso seguido de compressão 30%	0,8311
Compressão JPEG 30%	0,9615	Compressão JPEG 30%	0,9222
Hajjara, Abdallah e Hudaib (2009) 30%	0,9731	Hajjara, Abdallah e Hudaib (2009) 30%	0,9197

Fonte: Elaborada pela própria autora.

Ao longo de todos os experimentos, pode-se dizer que o método proposto é mais robusto aos ataques de compressão com perdas de 30% e compressão JPEG.

Os resultados mostram que há um decréscimo na correlação quando a dimensão da marca d'água passa de 32×32 pixels para 16×16 pixels. Visualmente, também se pode observar que conforme a taxa de correlação aumenta, a qualidade da marca d'água extraída diminui.

Na imagem Cass a marca mais robusta é a 32×32 pixels diante da maioria dos ataques, exceto na compressão com perdas quando a imagem é de 1024×1024 pixels.

Na imagem Lenna, a marca mais robusta é a 32×32 pixels diante de todos os ataques com as duas dimensões da imagem hospedeira, acontecendo o mesmo com a imagem Cisne. Podendo-se assim dizer que a marca d'água mais robusta foi a de 32×32 pixels.

Em geral, a análise de todos os resultados apresentados mostra que o método proposto torna as marcas d'água robustas diante da maioria dos ataques. Ataques esses que são os mais comuns nos atuais meios de transmissão de dados.

8 CONSIDERAÇÕES FINAIS

Com o aumento do uso da tecnologia digital, aumentou-se, também, a necessidade de garantir os direitos autorais sobre arquivos disponíveis nos meios de comunicação, como é o caso das imagens. A marca d'água digital é uma forma simples e barata de garantir a segurança e o direito autoral em imagens. Assim, é constante o surgimento de várias técnicas voltadas para essa finalidade.

Dentre as diversas técnicas, cada qual com sua aplicação e pelos estudos realizados neste trabalho, foi possível propor uma melhoria na técnica de Hajjara, Abdallah e Hudaib (2009), possibilitando testar as sub-bandas de frequência para determinar qual a melhor para a inserção da marca d'água.

A ferramenta de processamento aplicada no método proposto foi a transformada wavelet que facilita o processamento da imagem hospedeira, além de torná-la robusta a ataques como compressão e adição de ruído gaussiano.

A preparação da imagem hospedeira foi feita usando o mesmo processo do método de Hajjara, Abdallah e Hudaib (2009). Porém, a preparação e a inserção da marca d'água foram mais complexas e eficazes, de forma a torná-la robusta aos ataques testados. Além disso, os experimentos realizados variaram com relação às dimensões das imagens hospedeiras e das marcas d'água inseridas, abrangendo as possibilidades de verificar qual dimensão é mais viável para a inserção da d'água binária pelo método proposto e até mesmo pelo método proposto por Hajjara, Abdallah e Hudaib (2009), diante dos ataques que naturalmente as imagens estão vulneráveis a sofrer.

Os resultados dos testes numéricos mostraram que o método proposto foi eficiente no que diz respeito à preservação da marca d'água após ataques realizados, apresentando médias de correlação, entre a marca d'água inserida e a extraída, próximas à correlação perfeita.

Com isso, pode-se dizer que o método proposto apresentou uma marca d'água robusta diante dos ataques mencionados, principalmente, quando o ataque se refere apenas a compressão. Apesar de não apresentar resultados numéricos com correlação ótima, o método proposto pode ser considerado de caráter significativo para assuntos envolvendo a autenticação de imagens por marca d'água no domínio wavelet. Principalmente, quando comparado com outros métodos que serviram de base para a implementação da técnica apresentada neste trabalho.

Como principal contribuição do método proposto para a pesquisa de inserção e extração de marcas d'água em imagens digitais, pode-se citar o tratamento da marca d'água antes da sua inserção da imagem hospedeira. Esse tratamento impossibilita a detecção da marca d'água por alguém que não conhece o seu método de inserção.

Uma deficiência do método proposto está no fato de que a dimensão da marca d'água é dependente da dimensão da sub-banda escolhida para a inserção, não podendo ser maior. Porém, isso é uma deficiência da maioria dos métodos wavelet que fazem a inserção da marca d'água em uma única sub-banda de frequência.

A continuação deste trabalho consistiria em explorar outras maneiras de inserção como o método proposto por Wong, mediante realização de outros tipos de ataques, usando o método proposto e, ainda, utilizando um fator de ganho para a marca d'água baseado em propriedades da imagem hospedeira.

REFERÊNCIAS

ADDISON, P. S. **The illustrated wavelet transform handbook introductory theory and applications in science, engineering, medicine and finance**. [S.1.]: Institute of Physics Publishing Bristol and Philadelphia, 2002.

AL-HUNAITY, M. F.; NAJIN, S. A.; EL-EMARY, I. M. Colored image watermarking using wavelet technique. **American Journal of Applied Science**, New York, v. 4, n. 9, p. 658-662, 2007.

ANTON, H.; RORRES, C. **Elementary linear algebra: applications vrsion**. 7th ed. New York: John Wiley & Sons, 1994.

ARNOLD, V. I.; AVEZ, A. **Ergodic problems of classical mechanics**. New York: [s.n.], 1968.

BARRETO, P. S. L. M. **Criptografia robusta e marcas d'água frágeis: construção e análise de algoritmos para localizar alterações em imagens digitais**. 2003. 150 f. Tese (Doutorado em Engenharia de Sistemas Eletrônicos)- Escola Politécnica, Universidade de São Paulo - USP, São Paulo, 2003.

BARRETO, P. S. L. M.; KIM, H. Y.; RIJMEN, V. Toward a secure public-key blockwise fragile authentication watermarking. **IEE Proceedings - Vision, Image and Signal Processing**, Stevenage, v. 149, n. 2, p. 57-62, 2002.

BARNI, M.; BARTOLINI, F. **Watermarking systems engineering enabling digital assets security and other applications**. New York: Marcel Dekker, 2004. (Signal Processing and Communications Series).

CHIRIGATI, F. S.; KIKUCHI, R. S. A.; GOMES, T. L. **Esteganografia**. Rio de Janeiro: Universidade Federal do Rio de Janeiro, 2009. Disponível em: <http://www.gta.ufrj.br/grad/09_1/versao-final/stegano/index.html>. Acesso em: 18 ago. 2011.

CHEMAK, C.; LAPAYRE, J. C.; BOUHLEU, M. S. A new scheme of image watermarking on 5/3 wavelet decomposition and turbo-code. **WSEAS Transactions on Biology and Biomedicine**, Zographou, v. 4, n. 4, p. 45-52, 2007.

COX, I. J; KILIAN, J; LEIGHTON, F.T.; SHAMOON, T. Secure spread spectrum watermark for multimedia. In: INTERNATIONAL CONFERENCE ON IMAGE PROCESSING, 1997, Piscataway. **Proceedings...** Piscataway: [s. n.], 1997. p. 1673-1687.

COX, I. J; MILLER, M. L; BLOOM, J. A. Watermarking applications and their properties. In: INTERNATIONAL CONFERENCE ON INFORMATION TECHNOLOGY, 2000, Las Vegas. **Proceedings...** Las Vegas: [s. n.], 2000.

DAUBECHIES, I. **Ten lectures on wavelets**. Philadelphia: SIAM, 1992.

D'IPPÓLITO, K. M. **Estudo de métodos numéricos para eliminação de ruídos em**

imagens digitais. 2005. 73 f. Dissertação (Mestrado em Matemática Aplicada) - Instituto de Biociências, Letras e Ciências Exatas, Universidade Estadual Paulista - UNESP, São José do Rio Preto, 2005.

DONOHU, D. L.; JOHNSTONE, I. M. Ideal spatial adaptation via wavelet shrinkage. **Biometrika**, Oxford, v. 81, n. 3, p. 425-455, 1994.

DOU, Y., SHAIK, M. S. A robust watermarking method for copyright protection of digital images using wavelet transformation. **IEEE Transactions on Systems, Man, and Cybernetics**, Tokyo, v. 123, n. 2, p. 262-266, 2003.

DUARTE, M. A. Q.; SILVA, J. F.; VILLARREAL, F. Análise de métodos de inserção e extração de marca d'água no domínio wavelet. In: CONFERÊNCIA BRASILEIRA DE DINÂMICA, CONTROLE E APLICAÇÕES – DINCON, 10., 2011, Águas de Lindóia. **Anais...** Águas de Lindóia: DINCON, 2011.

FARID, H. **Detecting steganographic messages in digital images**. Hanover: Dartmouth College, 2001. (Technical Report, TR2001-412).

FRAUDE no comércio: exemplo de notas e moedas brasileiras falsas. [S. l]: Monitor das Fraudes, 2013. Disponível em: <<http://www.fraudes.org/showpage2.asp?pg=114>>. Acesso em: 4 abr. 2014.

FREDERES, T. A. **Digital watermarking**: autenticação de imagens com o uso de marca d'água digital. 2007. 54 f. Trabalho de Conclusão de Curso (Graduação em Ciência da Computação) – Faculdade de Ciências da Computação, Universidade Federal do Rio Grande do Sul, Porto Alegre, 2007.

GONZÁLES, R. C.; WOODS, R. E. **Processamento de imagens digitais**. São Paulo: Edgard Blucher, 2000.

GONZÁLES, R. C.; WOODS, R. E.; EDDINS, S. L. **Digital image processing using MATLAB**. 2. ed. Knoxville: Gatesmark Publishing, 2009.

HAJJARA, S.; ABDALLAH, M.; HUDAIB, A. Digital image watermarking using localized biorthogonal wavelets. **European Journal of Scientific Research**, Orion Mall, v. 26, n. 4, p. 594-608, 2009.

HSIEH, C. T.; WU, Y. J. Digital image multiresolution watermark based on human visual system using error correcting code. **Tamkang Journal of Science and Engineering**, Taiwan, v. 4, n. 3, p. 201-208, 2001.

HUANG, W. T.; TAN, S. Y.; CHANG, Y. J.; CHEN, C. H. A robust watermarking for copyright protection using discrete wavelet transform. **WSEAS Transactions on Computers**, Zographou, v. 9, n. 5, p. 485-495, 2010.

JAYAWARDENA, A.; LENDERS, P.; Embedding multiresolution binary images into wavelet domain multiresolution binary watermark channels for copyright enforcement. In: IEEE INTERNATIONAL CONFERENCE ON ACOUSTICS, SPEECH AND SIGNAL PROCESSING, 6., 2000, Piscataway. **Proceedings...** Piscataway: [s.n], 2000. p. 1983–1986.

JOHNSON, N. F.; An introduction to watermark recovery from images. In: SANS INTRUSION DETECTION AND RESPONSE CONFERENCE, 1999, San Diego. **Proceedings...** San Diego: [s.n.], 1999. p. 1-6.

KATZENBEISSER, S.; PETITCOLAS, F. A. P. **Information hiding techniques for steganography and digital watermarking**. [S. l.]: Artech House, 2000.

KAWAGUCHI, E.; EASON, R. O. Principle and applications of BPCS-Steganography. **SPIE Proceedings Series**, Boston, v. 3528, p. 464-473, 1999.

KESSLER, G. C. **An overview of steganography for the computer forensics examiner: computer and digital**. Burlington: Champlain College, 2004.

LOPES, I. O.; SILVA, A. F.; BARCELOS, A. Z.; BATISTA, M. A. Introdução à marca d'água digital. In: SIMPÓSIO DE MATEMÁTICA. JORNADA DE MATEMÁTICA DE CATALÃO, 15., 2004, Catalão. **Anais...** Catalão: [s. n.], 2004.

MALLAT, S. A theory for multiresolution representation signal decomposition: the wavelet representation. **IEEE Transactions on Pattern Analysis and Machine Intelligence**, Piscataway, v. 11, n. 7, p. 674-693, 1989.

MALLAT, S.; HWANG, W. I. Singularity detection and processing with wavelets. **IEEE Transactions on Information Theory**, Piscataway, v. 38, p. 617-643, 1992.

MARQUES FILHO, O.; VIEIRA NETO, H. **Processamento digital de imagens**. Rio de Janeiro: Brasport, 1999.

MARTÍNEZ, G. D. F.; VIOLA, G. V. A. **Inserción de marcas de agua em imágenes digitales: projeto de Taller V**. Montevideo: Instituto de Computación, Faculdade de Ingeniería, 2000.

MENDES, F. B. C. **Uma proposta de assinatura digital para imagens por meio de marca d'água**. 2008. 134 f. Dissertação (Mestrado em Ciência da Computação) – Faculdade de Computação, Universidade Federal de Uberlândia - UFU, Uberlândia, 2008.

MOHANTY, S. P. **Digital watermarking: a tutorial review**. Tampa: Dept of Comp Sc and Eng. University of South Florida, 1999.

ÖZER, H.; AVCIBAS, I.; SANKUR, B.; MEMON, N. Steganalysis of audio based on audio quality metrics. **Proceedings of the SPIE**, Bellingham, v. 5020, p. 55-66, 2003.

PAMBOUKIAN, S. V. D. **Marcas d'água de autenticação para imagens binárias: marcas reversíveis e marcas para o padrão JBIG2** 2007. 2007. 154 f. Tese (Doutorado Engenharia de Sistemas Eletrônicos)- Escola Politécnica, Universidade de São Paulo - USP, São Paulo, 2007.

PETERSON, G. **Linear algebra, arnold's cat map**. [S. l.: s. n.], 1997.

PORTILLA, J.; SIMONCELLI, E. P. A parametric texture model based on joint statistics of

complex wavelet coefficients. **Int'l Journal of Computer Vision**, New York, v. 40, n. 1, p. 49-71, 2000.

RIOL, O.; VETTERLI, M. Wavelets and signal processing. **IEEE Signal Processing Magazine**, Piscataway, v. 8, n. 4, p. 14-38, 1991.

ROCHA, R. S.; RODRIGUES, M. A. F.; TADDEO, L. S. Performance evaluation of a hybrid algorithm for collision detection in crowded interactive environments. In: BRAZILIAN SYMPOSIUM ON COMPUTER GRAPHICS AND IMAGE PROCESSING- SIBGRAPI, 19., 2006, Manaus. **Proceedings...** Manaus: IEEE CS Press, 2006. P. 86--93,

SANGHYUN, J.; YOUNGHO, S.; JAEHO, S.; HISAKAZU, K. A new robust watermarking embedding into wavelet DC components. **ETRI Journal**, Daejeon, v. 24, n. 5, p. 401-404, 2002.

SANS, D. R. **Identificação de propriedade em imagens com marcas d'água no domínio da transformada wavelet**. 2008. 127 f. Dissertação (Mestrado em Informática) - Faculdade de Ciências da Computação, Universidade Federal do Paraná, Curitiba, 2008.

SANS, D. R.; PEDRINI, H. Inserção e recuperação de marcas d'águas em imagens pela transformada wavelet. WORKSHOP DE VISÃO COMPUTACIONAL, 4., 2008, Bauru. **Anais...** Bauru: [s. n.], 2008. p. 63-68.

SILVA, J. F. **Sistema de armazenamento de imagens comprimidas através da transformada wavelet**. 2008. 99 f. Dissertação (Mestrado em Engenharia Elétrica) - Faculdade de Engenharia, Universidade Estadual Paulista - UNESP, Ilha Solteira, 2008.

SILVA, J. F.; DUARTE, M. A. Q.; VILLARREAL, F. Inserção e extração de marca d'água em imagens digitais no domínio wavelet. In: CONFERÊNCIA BRASILEIRA DE DINÂMICA, CONTROLE E APLICAÇÕES – DINCON, 2013, Fortaleza. **Anais...** Fortaleza: DINCON, 2013.

SIMON, M. **Marca d'água: hora de sujar suas fotos**. [S.l.: s.n., 200-]. Disponível em: <<http://www.fotografia-dg.com/marca-de-agua-fotos/>>. Acesso em: 13 out. 2013.

SOARES, W. C. **Um método não-limiar para redução de ruído em sinais de voz no domínio wavelet**. 2009. 205 f. Tese (Doutorado em Engenharia Elétrica) - Faculdade de Engenharia, Universidade Estadual Paulista, Ilha Solteira, 2009.

STALLINGS, W. **Cryptography and network security: principles and practice**. 2. ed. [S.l.]: Prentice Hall, 1999.

STOLLNITS, E. J.; DEROSE, T. D.; SALESIN, D. H. **Wavelets for computer graphics theory and applications**. San Francisco: Morgan Kaufmann , 1996.

TAY, P.; HAVILCEK, J. V. **Image watermarking using wavelets**. Norman: University of Oklahoma, 2002. Disponível em: <hotnsour.ou.edu/joejob/PdfPubs/MWSCAS2002Peter.pdf>. Acesso em: 21 abr. 2009.

THE LENA story. Boston: Lena, 1997. Disponível em:

<<http://www.cs.cmu.edu/~chuck/lennapg/>>. Acesso em: 4 abr. 2014.

VALENS, C. **EZW encoding**. [S. l.: s. n], 2004. Disponível em: <<http://perso.orange.fr/polyvalens/clemesn/ezw.html>>. Acesso em: 26 set. 2011.

VOLPI, M. M. **Assinatura digital**: aspectos técnicos, práticos e legais. Rio de Janeiro: Axcel Books do Brasil, 2001.

WAYNER, P. **Disappearing cryptography**: information hiding: steganography and watermarking. 2. ed. Maryland Heights: Morgan Kaufmann, 2002.

WONG, P. W. A public key watermark for image verification and authentication. **IEEE Int. Conf. on Image Processing**, Piscataway, v. 1, p. 455-459, 1998.

WONG, P. W. A watermark for image integrity and ownership verification. In: IS & T PIC CONFERENCE, 1998, Portland. **Proceedings...** Portland: Society for Imaging Science and Thecnology, 1998.

WONG, P. W.; MEMON, N. Secret and public key image watermarking schemes for image authentication and ownership verification. **IEEE Trans. Image Processing**, Piscataway, v. 10, n. 10, p. 1593-1601, 2001.

WANG, H. J.; KUO, C. C. J. An integrated progressive image coding and watermark system. In: IEEE INTERNATIONAL CONFERENCE ON ACOUSTICS SPEECH, AND SIGNAL PROCESSING – ICASSP, 6., 1998. **Proceedings...** [S. l]: IEEE explore, 1998. p. 3721–3724.

WANG, J. Z.; WIEDERHOLD, G. Wavemark: digital image watermarking using daubechies wavelets and error correcting coding. **Conference of Multimedia Systems and Applications**, Boston, v. 3528, p. 432-439, 1998.