



UNIVERSIDADE FEDERAL DE PERNAMBUCO
CENTRO DE INFORMÁTICA
GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO



MATHEUS CABRAL DE ARAÚJO GOIS
(mc@cin.ufpe.br)

UMA ARQUITETURA PARA APLICAÇÕES DE MASCARAMENTO DE INFORMAÇÕES EM IMAGENS

**Trabalho de conclusão de curso em Ciência
da Computação, Centro de Informática,
Universidade Federal de Pernambuco.**

Orientador: Prof. Dr. Alejandro C. Frery
(frery@cin.ufpe.br)

RECIFE, 3 DE FEVEREIRO DE 2003



UNIVERSIDADE FEDERAL DE PERNAMBUCO
CENTRO DE INFORMÁTICA
GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO



TERMO DE APROVAÇÃO

UMA ARQUITETURA PARA APLICAÇÕES DE MASCARAMENTO DE INFORMAÇÕES EM IMAGENS

Trabalho aprovado como requisito parcial para conclusão da disciplina de Trabalho de Graduação em Computação Visual, disciplina essa do Centro de Informática da Universidade Federal de Pernambuco.

Autor:

**Matheus Cabral de Araújo Gois
Centro de Informática – UFPE**

Banca Examinadora:

**Prof. Dr. Alejandro C. Frery
Centro de Informática – UFPE**

**Prof. Dr. Ruy J. Guerra B. de Queiroz
Centro de Informática – UFPE**

RECIFE, 3 DE FEVEREIRO DE 2003

DEDICATÓRIA

Gostaria de dedicar este trabalho a minha família: meus “pais” (Enio, Arabela e Elda), meus “irmãos” (Thiago, Pinho e Pinico), minhas “cunhadas” (Claudinha, Ju e Silvinha) e meus papagaios Tabaco e Que-qué. Vocês foram a fonte de toda minha energia e, mesmo fisicamente distantes, estarão sempre em meu coração.

Dedico esse trabalho também a quatro grandes amigos que estiveram sempre ao meu lado durante toda minha graduação: Carlos Eduardo Bezerra Galvão (*in memoriam*), Giordano Ribeiro Eulálio Cabral, Hedlena Maria de Almeida Bezerra e Paulo Gonçalves de Barros.

AGRADECIMENTOS

Agradeço primeiro a minha família pelo incentivo, suporte e confiança que sempre me deram em todos os momentos de minha vida.

Agradeço especialmente a meu orientador e amigo Alejandro por todo conhecimento passado, pela sua dedicação, paciência, apoio, boa vontade e alto nível de exigência no desenvolvimento desse trabalho. Seu inesgotável conhecimento, demonstrado durante nossas reuniões semanais, tem me servido como constante fonte de aprendizagem e inspiração.

Gostaria de agradecer também a Verônica Teichrieb e Babi por suas amizades e detalhadas revisões do presente documento. Suas críticas e sugestões foram de fundamental importância para minha aprendizagem.

Agradeço a todos os meus amigos. Em especial, gostaria de agradecer a Adeline, Angela, Bah (Mariano), Carlinha, Erika e Hedlena pela ajuda, ora em revisões desse documento ora em discussões sobre o projeto.

Agradeço também aos autores de livros e artigos aqui mencionados, sendo de primordial importância para o desenvolvimento deste trabalho. Gostaria também de agradecer aos compositores e músicos que me acompanharam por horas no decorrer deste trabalho.

Minha gratidão a todos que contribuíram para a formação da minha pessoa.

SUMÁRIO

LISTA DE FIGURAS	VI
RESUMO	VIII
ABSTRACT	VIII
1. INTRODUÇÃO	1
2. ASPECTOS HISTÓRICOS E ANTECEDENTES	7
2.1. Esteganografia	7
2.1.1. Tempos Antigos	8
2.1.2. Tempos Modernos	9
2.2. Marcação Digital	11
2.3. Ferramentas Existentes	13
2.3.1. Invisible Secrets 2002	13
2.3.2. Steganos Security Suite	14
3. TERMINOLOGIA E CLASSIFICAÇÕES	17
3.1. Terminologia	17
3.2. Classificação	18
3.2.1. Classificação por categoria do estego-objeto	18
3.2.2. Classificação por visibilidade	19
3.2.2.1. Marcação digital visível	19
3.2.2.2. Marcação digital invisível	19
3.2.3. Classificação pelo tipo da marca	19
3.2.3.1. Marca digital em formato de ruído	19
3.2.3.2. Marca digital em formato de imagem	20
3.2.4. Classificação pelo método de processamento	20
3.2.4.1. Métodos do domínio espacial	20
3.2.4.2. Métodos do domínio transformado	20
3.2.5. Classificação pela detecção/extração da marca	21

3.2.5.1.	Por necessidade do objeto original _____	21
	Marcação digital obscura _____	21
	Marcação digital não obscura _____	21
3.2.5.2.	Pela natureza da marca _____	21
	Marcação digital aberta _____	21
	Marcação digital fechada _____	22
3.2.5.3.	Por reconhecimento da marca _____	22
	Marcação digital legível _____	22
	Marcação digital detectável _____	22
3.2.5.4.	Pela entrada/saída do algoritmo de extração _____	22
	Marcação digital privada _____	23
	Marcação digital semi-privada _____	24
	Marcação digital pública _____	24
	Marcação digital semi-pública _____	24
	Marcação digital assimétrica _____	24
3.2.6.	Classificação pela persistência da marca _____	25
3.2.6.1.	Marcação digital frágil _____	25
3.2.6.2.	Marcação digital robusta _____	25
3.2.6.3.	Marcação digital semi-frágil _____	26
4.	<u>APLICAÇÕES</u>	27
4.1.	Comunicação Encoberta _____	27
4.2.	Proteção de Direitos Autorais _____	28
4.3.	Seriação (<i>Fingerprinting</i>) _____	28
4.4.	Certificação e Controle de Acesso _____	29
4.5.	Legendas em Imagens e Vídeos _____	30
4.6.	Controle de Cópias _____	30
4.7.	Autenticação e Verificação da Integridade _____	30
5.	<u>REQUISITOS E ATAQUES</u>	32
5.1.	Requisitos _____	32
5.1.1.	Invisibilidade (Transparência perceptual) _____	32
5.1.2.	Custo computacional _____	33

5.1.3.	Capacidade _____	33
5.1.4.	Robustez _____	34
5.1.4.1.	Compressão/Descompressão JPEG _____	34
5.1.4.2.	Transformações _____	34
	Espelhamento horizontal _____	35
	Recorte (Cropping) _____	35
	Rotação _____	36
	Ajustes de escala _____	36
	Remoção de linhas e/ou colunas _____	37
	Combinações de transformações _____	37
	Distorções aleatórias _____	37
5.1.4.3.	Conversões digital/analógico e analógico/digital _____	37
5.1.4.4.	Adição de ruídos _____	37
5.1.4.5.	Filtros passa-baixa _____	38
5.1.4.6.	Quantização de cores _____	38
5.1.5.	Segurança _____	38
5.1.6.	Falsos positivos _____	39
5.2.	Ataques _____	40
5.2.1.	Ataques de robustez _____	40
5.2.1.1.	Ataques de robustez baseados em operações de processamento _____	40
5.2.1.2.	Ataques de robustez analíticos _____	40
5.2.2.	Ataques de apresentação _____	41
5.2.3.	Ataques de interpretação _____	42
5.2.4.	Ataques legais _____	43
6.	<u>ARQUITETURA PROPOSTA</u> _____	44
6.1.	Modelagem da Imagem _____	45
6.2.	Modelagem do Acesso à Imagem _____	49
6.3.	Modelagem do Mascaramento de Informações _____	50
6.4.	Modelagem de Componentes Complementares _____	53
6.4.1.	Exceções _____	53
6.4.2.	ObjectFactory e NativeFactory _____	54
6.4.3.	Fachada e Interface Gráfica (GUI) _____	55

6.5.	Arquitetura Final	56
7.	CONCLUSÕES E TRABALHOS FUTUROS	58
7.1.	Objetivos Alcançados	58
7.2.	Dificuldades Encontradas	59
7.3.	Trabalhos Futuros	59
7.4.	Linhas de Pesquisa	60
	REFERÊNCIAS BIBLIOGRÁFICAS	62
	ANEXO A	68
	ANEXO B	70

LISTA DE FIGURAS

FIGURA 1: CLASSIFICAÇÃO DE MASCARAMENTO DE INFORMAÇÕES SEGUNDO [PFITZMANN, 1996].	2
FIGURA 2: EXEMPLO DE ESTEGANOGRAFIA. (A) REPRESENTA A IMAGEM ORIGINAL. (B) REPRESENTA A ESTEGO-IMAGEM COM O TEXTO “MINHA SENHA DO UNIX É: 123456” ESCONDIDO NOS BITS MENOS SIGNIFICATIVOS DA IMAGEM (A).	3
FIGURA 3: EXEMPLO DE MARCAÇÃO DIGITAL. AS IMAGENS (A) E (B) MOSTRAM MARCAÇÕES DIGITAIS ESTEGANOGRÁFICAS. AS IMAGENS (C) E (D) APRESENTAM MARCAÇÕES DIGITAIS NÃO ESTEGANOGRÁFICAS (OBSERVE O LOGOTIPO CORBIS NO CENTRO DA IMAGEM (C) E O LOGOTIPO DO VATICANO NO CENTRO DA IMAGEM (D)). FONTES: [CRAVER, 1998], [PETITCOLAS, 2002], [CORBIS, 2002] E [MINTZER, 1996].	4
FIGURA 4: EXEMPLO DE ESTEGANOGRAFIA BASEADO NO MAPEAMENTO LETRA – NOTA MUSICAL. (A) APRESENTA O MAPEAMENTO. (B) REPRESENTA UMA COMPOSIÇÃO BASEADA EM UMA FRASE. FONTE: [SCHOTTI, 1665].	10
FIGURA 5: TELA PRINCIPAL DO INVISIBLE SECRETS.	14
FIGURA 6: TELA PRINCIPAL DO STEGANOS SECURITY SUITE.	15
FIGURA 7: PROCESSOS DE INSERÇÃO E DETECÇÃO/ EXTRAÇÃO DE MARCAÇÃO DIGITAL. EM (A), O PROCESSO DE INSERÇÃO. OS PROCESSOS DE EXTRAÇÃO E DETECÇÃO DA MARCAÇÃO DIGITAL PRIVADA SÃO ILUSTRADOS, RESPECTIVAMENTE, EM (B) E (C). O PROCESSO DE DETECÇÃO DA MARCAÇÃO DIGITAL SEMI-PRIVADA É APRESENTADO EM (D). OS PROCESSOS DE EXTRAÇÃO DA MARCAÇÃO DIGITAL SEMI- PÚBLICA E PÚBLICA SÃO ILUSTRADOS EM (E) E (F).	23
FIGURA 8: EXEMPLO DE UM CARTÃO DE IDENTIFICAÇÃO MARCADO. O NÚMERO DE IDENTIFICAÇÃO "123456789" ESTÁ ESCRITO EM FORMA DE TEXTO E TAMBÉM ESCONDIDO COMO UMA MARCA NA FOTO. FONTE: [KUTTER, 2001].	29
FIGURA 9: USO DE MARCAÇÃO DIGITAL PARA VERIFICAÇÃO DA INTEGRIDADE DE IMAGENS. À ESQUERDA, A IMAGEM PROTEGIDA. AO CENTRO, A IMAGEM ALTERADA. À DIREITA, AS ÁREAS MODIFICADAS DESCOBERTAS. FONTE: [KUTTER, 2001].	31
FIGURA 10: EXEMPLO DE ESPELHAMENTO HORIZONTAL. À ESQUERDA, A IMAGEM ORIGINAL E À DIREITA A IMAGEM TRANSFORMADA.	35

FIGURA 11: EXEMPLO DE RECORTE. À ESQUERDA, A IMAGEM ORIGINAL. À DIREITA, UM RECORTE DA IMAGEM ORIGINAL. _____	35
FIGURA 12: EXEMPLO DE ROTAÇÃO E RECORTE. À ESQUERDA, A IMAGEM ORIGINAL. À DIREITA, A IMAGEM ORIGINADA A PARTIR DA ROTAÇÃO (0.3 GRAUS HORÁRIOS) E RECORTE DA IMAGEM ORIGINAL. _____	36
FIGURA 13: EXEMPLO DE AJUSTE DE ESCALA. À ESQUERDA, A IMAGEM ORIGINAL. À DIREITA, A IMAGEM OBTIDA ATRAVÉS DE UM AJUSTE UNIFORME DE ESCALA (75%). _____	36
FIGURA 14: EXEMPLO DE ADIÇÃO DE RUÍDO. À ESQUERDA, A IMAGEM ORIGINAL. À DIREITA, A IMAGEM ADICIONADA DE UM RUÍDO SEGUNDO UMA DISTRIBUIÇÃO UNIFORME. _____	38
FIGURA 15: EXEMPLO DE ATAQUE DE COLISÃO. À ESQUERDA E AO CENTRO, IMAGENS VISUALMENTE IDÊNTICAS COM IDENTIFICADORES DIFERENTES. À DIREITA, IMAGEM GERADA DETERMINANDO ÁREAS DE DIFERENÇAS ENTRE AS IMAGENS. FONTE: [PETITCOLAS, 2001]. _____	41
FIGURA 16: EXEMPLO DE ATAQUE MOSAICO. AS SEIS PORÇÕES À ESQUERDA FORMAM À FIGURA A DIREITA (O MOSAICO). FONTE: [PETITCOLAS, 2002]. _____	42
FIGURA 17: OPERAÇÕES DA INTERFACE PIXELINTERFACE. _____	45
FIGURA 18: OPERAÇÕES DA INTERFACE IMAGEINTERFACE. _____	46
FIGURA 19: OPERAÇÕES DA INTERFACE IMAGEINTERFACE. _____	47
FIGURA 20: CLASSES ABSTRATAS IMAGE E IMAGE TYPE. _____	48
FIGURA 21: ESTUDO DE CASO DA MODELAGEM DO FORMATO DE IMAGEM TONS DE CINZA. _____	49
FIGURA 22: MODELAGEM DO ACESSO A ARQUIVOS DE IMAGENS. _____	50
FIGURA 23: CLASSES INFOHIDINGKEY (CHAVE) E INFOHIDINGMESSAGE (MENSAGEM). _____	51
FIGURA 24: MODELAGEM DAS TÉCNICAS DE MASCARAMENTO DE INFORMAÇÕES. _____	52
FIGURA 25: CLASSES OBJECTFACTORY (A) E NATIVEFACTORY (B). _____	55
FIGURA 26: ARQUITETURA FINAL. _____	57

RESUMO

Mascaramento de Informações pode ser definido como o conjunto de técnicas e protocolos cujo objetivo é esconder uma informação em algum objeto. Essa informação pode ser uma simples mensagem textual, uma marca representando uma empresa, um número de série ou qualquer outro tipo de informação. Esse trabalho tem como principal objetivo a modelagem de uma arquitetura de um *framework* que facilite a criação e testes de novas técnicas de mascaramento de informações em imagens. O planejamento dessa arquitetura é de fundamental importância para a área, uma vez que irá permitir que pesquisadores possam desenvolver e testar novas técnicas de mascaramento de informações para imagens sem necessidade de despendere esforços implementando cada uma delas de forma estanque.

ABSTRACT

Information Hiding can be defined as a set of techniques and protocols whose purpose is to conceal information within a given object. Such information can be a simple text message, a logo mark representing some company, a serial number and so on. This work main goal is modeling a framework architecture that lessens the creation and testing of new techniques of information hiding in digital images. The planning of this architecture is of utmost importance for the area since it will allow researchers to focus on both the development and testing new techniques of information hiding in images, regardless of the basic implementation of each one alone.

1. INTRODUÇÃO

What you've got they can't steal it

No they can't even feel it

(Bono Vox)

A evolução da comunicação digital possibilitou a troca de informações em diversos formatos como, por exemplo, e-mails, imagens, músicas e até vídeos. Entretanto, esse tipo de comunicação também possibilitou a invasão de privacidade uma vez que essas mensagens circulavam pela Internet e terceiros (*hackers*) passaram a ter acesso às mesmas. Dessa forma, as áreas de segurança de sistemas e, mais especificamente criptografia exerceram grande impacto na tentativa do desenvolvimento de aplicações e protocolos capazes de possibilitar uma comunicação com boas características. Essas “boas características” são, segundo [Schneier, 1996], o sigilo, a integridade, a autenticidade e a não-repudição (a impossibilidade do remetente negar a autoria de uma mídia enviada).

Entretanto, a criptografia tem como princípio a troca de mensagens que, por si só, são “embaralhadas” e ilegíveis aos olhos de possíveis atacantes. Para algumas aplicações é importante garantir que não exista vestígio da troca dessas mensagens, fato esse que a criptografia convencional e de chave pública não foram projetadas para satisfazer. Outro problema persistente na criptografia é que muitos governos fazem restrições à exportação de técnicas, métodos, algoritmos e chaves de criptografia forte, levando instituições e pesquisadores a procurarem outras técnicas que garantam a segurança das suas comunicações e sistemas.

Além disso, outro fator importante que as áreas de segurança de sistemas e criptografia não conseguem garantir satisfatoriamente é a proteção dos direitos autorais. Uma vez que as informações tornam-se cada vez mais digitais, a facilidade de fazer cópias perfeitas sem a autorização do criador do objeto digital leva a um alto índice de violações dos direitos autorais. Ferramentas como [Kazaa, 2002] e [Morpheus, 2002] permitem ainda a fácil troca de objetos digitais entre milhões de usuários sem respeitar os direitos autorais de seus autores.

Pelo acima exposto, indivíduos, indústrias e instituições estão investindo na pesquisa de tecnologias que dificultem a violação dos direitos autorais de seus produtos. Fabricantes de CDs, software e até mesmo a própria indústria literária são exemplos de instituições que possuem grande interesse na solução desses problemas.

Os exemplos acima citados são algumas possíveis aplicações de uma área de pesquisa bastante antiga, mas só recentemente incorporada ao contexto digital: o Mascaramento de Informações (*Information Hiding*).

Mascaramento de Informações pode ser definido como o conjunto de técnicas e protocolos que tentam esconder algum tipo de informação em algum objeto. O objeto onde a informação será inserida é denominado no que segue como “objeto guardada”. Essa informação pode ser uma simples mensagem textual, uma marca representando a empresa que fabricou o objeto guardada, o número de série do objeto (*fingerprinting*) ou qualquer outro tipo de informação. Além disso, é importante mencionar que a natureza do objeto guardada pode variar de acordo com a aplicação, podendo ser uma imagem, uma arquivo de música digital, um vídeo ou até mesmo um texto.

Segundo [Pfitzmann, 1996], as técnicas de mascaramento de informações podem ser classificadas segundo a taxonomia apresentada na Figura 1. Nesse trabalho daremos ênfase às aplicações que se encaixam nas áreas de Esteganografia e Marcação Digital (*Digital Watermarking*).

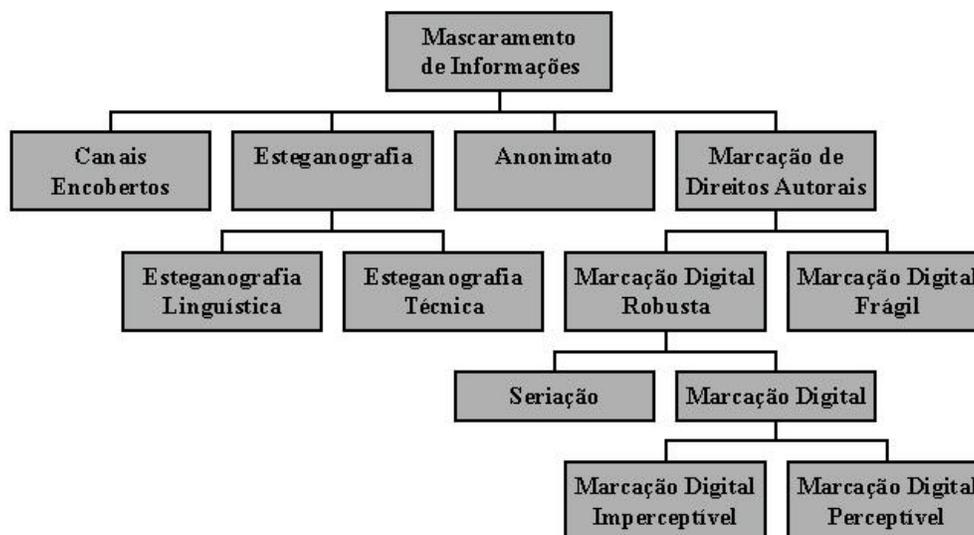


Figura 1: Classificação de Mascaramento de Informações segundo [Pfitzmann, 1996].

A Esteganografia é a principal e mais antiga sub-área de mascaramento de informações. A ciência da esteganografia visa a troca de mensagens e é mais antiga do que a própria criptografia. Esteganografia pode ser definida como a arte de esconder informações de forma que a presença das mesmas não seja detectada. O termo “esteganografia” deriva do grego $\sigma\tau\epsilon\gamma\alpha\nu\omicron\prime\text{-}\zeta, \gamma\rho\alpha\phi\text{-}\epsilon\iota\nu$ e significa “escrita encoberta” [Kahn, 1996].

Um exemplo de aplicação de esteganografia pode ser visto na Figura 2. Nesta, a imagem (a) representa a imagem original. A imagem (b) representa a estego-imagem, gerada a partir de (a), mas que contém uma determinada informação escondida, nos bits menos significativos de cada pixel. Neste exemplo, a informação escondida é a frase “Minha senha do UNIX é: 123456”. Dessa forma, a imagem (b) poderia ser transmitida para outro usuário sem levantar suspeita (a um possível atacante) de que uma informação secreta estava sendo transmitida.

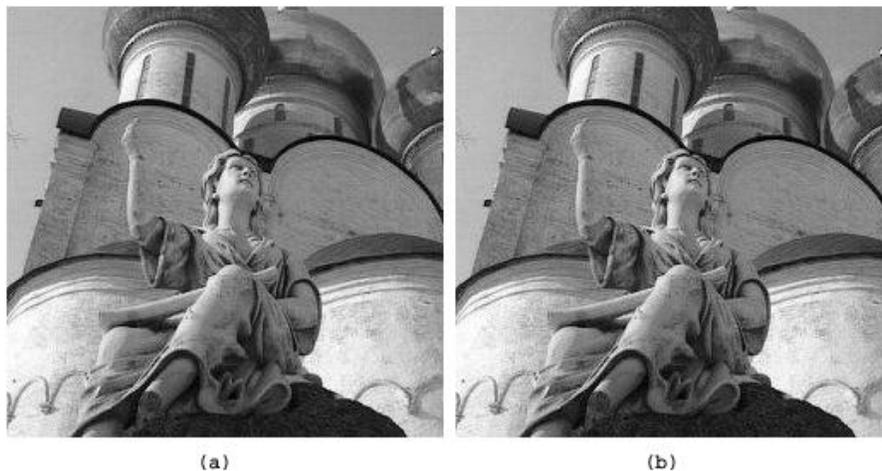


Figura 2: Exemplo de esteganografia. (a) representa a imagem original. (b) representa a estego-imagem com o texto “Minha senha do UNIX é: 123456” escondido nos bits menos significativos da imagem (a).

Outra sub-área bastante importante de mascaramento de informações é denominada *Digital Watermarking* (referida nesse trabalho como “Marcação Digital”) e pode ser definida como o conjunto de técnicas esteganográficas ou não¹ que permitem identificar o dono de determinado objeto digital. Além disso, algumas técnicas de marcação digital permitem não só fazer a proteção de direitos autorais bem como descobrir cópias não autorizadas, validar a

¹ Algumas técnicas de marcação digital empregam marcas que, por serem visíveis, não são consideradas técnicas de esteganografia. Para obter exemplos desse tipo de marca, o leitor pode consultar [Corbis, 2002] e [Mintzer, 1996].

identificação, verificar a integridade do objeto e fazer controle de acesso do mesmo [Memom, 1998]. É importante mencionar que as marcações digitais não esteganográficas ou marcações digitais perceptíveis fogem à definição de mascaramento de informações acima apresentada.

A Figura 3 ilustra os dois tipos de marcação digital. O leitor pode observar exemplos de técnicas de marcação digital esteganográficas nas imagens (a) e (b) e exemplos de técnicas de marcação digital não esteganográficas nas imagens (c) e (d). Neste último caso, os logotipos da *Corbis* e do Vaticano podem ser vistos no centro das imagens (c) e (d), respectivamente.



Figura 3: Exemplo de marcação digital. As imagens (a) e (b) mostram marcações digitais esteganográficas. As imagens (c) e (d) apresentam marcações digitais não esteganográficas (observe o logotipo CORBIS no centro da imagem (c) e o logotipo do Vaticano no centro da imagem (d)).

Fontes: [Craver, 1998], [Petitcolas, 2002], [Corbis, 2002] e [Mintzer, 1996].

É importante discernir claramente os conceitos de esteganografia e marcação digital, pois são bastante próximos. Como citado em [Petitcolas, 1999], o propósito principal da esteganografia é possibilitar a comunicação encoberta entre duas entidades sem que um

possível intruso tenha conhecimento da existência dessa troca de informações. Nesse caso, um ataque bem sucedido consiste na detecção da existência dessa comunicação. Por outro lado, a marcação digital possui o requisito adicional de exibir robustez contra possíveis ataques. No último caso, um ataque bem sucedido seria processar o objeto marcado de tal forma que ele não seja alterado significativamente, mas que redunde na destruição ou inutilização da marca. Em termos de imagens, um filtro passa-baixa seria um exemplo de processamento que poderia destruir a marca sem alterar substancialmente a imagem.

É importante também discernir as diferenças entre esteganografia e criptografia. Enquanto o propósito principal da criptografia é esconder o conteúdo das mensagens, o propósito da esteganografia é esconder a existência das mesmas. No que diz respeito à segurança de sistemas, é importante deixar claro que a esteganografia é um suplemento à criptografia, portanto, uma nunca deve substituir a outra.

Esse trabalho tem como principal objetivo a modelagem de uma arquitetura de um *framework* que facilite a criação e testes de novas técnicas de mascaramento de informações em imagens. O planejamento e possível implementação desse *framework* é de fundamental importância para a área de mascaramento de informações, uma vez que irá permitir que pesquisadores possam desenvolver e testar novas técnicas de mascaramento de informações para imagens sem necessidade de despender esforços implementando cada uma delas de forma estanque. Além disso, é importante também que essa modelagem possibilite a utilização do *framework* na criação de diferentes tipos de aplicações.

A modelagem dessa arquitetura será realizada em UML (*Unified Modeling Language*) [Booch, 1998] empregando a metodologia de desenvolvimento de software RUP (*Rational Unified Process*). Esta escolha está motivada pelo fato dessa metodologia permitir descrever de forma interativa e incremental a construção de software. Para aferir os modelos propostos, pelo menos uma técnica de mascaramento de informações será desenvolvida.

Outra meta deste trabalho é estudar formas de integrar a arquitetura aqui proposta com *benchmarks* já existentes para testes de robustez de técnicas de mascaramento de informações, como por exemplo o StirMark [Petitcolas, 2001] e o Checkmark [Checkmark, 2003].

Dado que não há consenso na língua portuguesa a respeito da terminologia a ser empregada para as diversas técnicas e metodologias abordadas neste documento, uma terceira contribuição deste trabalho consiste na discussão e proposta de termos para elas. Esta contribuição será realizada após a apresentação dos principais aspectos históricos da área.

O presente documento está organizado da seguinte forma: o capítulo 2 apresenta os aspectos históricos das técnicas de esteganografia e marcação digital em imagens e os principais antecedentes referentes às ferramentas relacionadas com a área de mascaramento de informações. O capítulo 3 apresenta uma sugestão de terminologia para na língua portuguesa. Nesse capítulo também é apresentada uma unificação das possíveis classificações das técnicas de mascaramento de informações. O capítulo 4 ilustra algumas, porém não únicas, aplicações da área. Os principais requisitos e ataques que envolvem as técnicas de mascaramento de informações são apresentados no capítulo 5. O capítulo 6 apresenta a arquitetura para aplicações de mascaramento de informações em imagens, principal objetivo desse trabalho. Finalmente, o capítulo 7 apresenta as principais conclusões e perspectivas de trabalhos futuros.

2. ASPECTOS HISTÓRICOS E ANTECEDENTES

*A journey of a thousand miles must
begin with a single step.*

(Lao-zi)

O capítulo anterior apresentou, rapidamente, os principais conceitos e exemplos referentes a área de mascaramento de informações. Além disso, foram apresentados os principais objetivos dessa pesquisa.

Nesse capítulo serão apresentados os principais aspectos históricos das duas principais sub-áreas do mascaramento de informações: esteganografia e marcação digital. Devido a sua vasta história, muitos exemplos de técnicas de mascaramento de informações não se referem a suas aplicações em imagens, mas foram aqui ilustrados uma vez que esses formam a base da história dessa área.

Por fim, serão apresentados os principais antecedentes em termos de ferramentas existentes de mascaramento de informações. Nessa seção, será dado o enfoque a aplicações que tratam imagens, mas também serão ilustrados exemplos que tratam de outros tipos de mídias (música, vídeo, texto etc.).

2.1. ESTEGANOGRAFIA

O mascaramento de informações tem como sub-área mais antiga a esteganografia. Fatos comprovam que essa ciência vem sendo praticada desde os tempos antigos principalmente por espões, governos e exércitos e, devido a uma série de aplicações, ela tem sido praticada pela própria indústria.

Ao longo da história muitas informações vêm sendo escondidas em desenhos, livros, pinturas, jornais, discursos, textos escritos e, até mesmo, em logotipos. Nas próximas subseções serão apresentados, de forma sucinta, os aspectos históricos da esteganografia desde os tempos antigos até os tempos modernos.

2.1.1. TEMPOS ANTIGOS

Segundo [Kobayashi, 1997], a primeira referência sobre uso de esteganografia² é a história sobre Belerofonte, narrada em *Ilíada* [Homero, 2002]. Belerofonte era um guerreiro famoso e amado por todas as mulheres da sua terra. Por rejeitar seus pedidos, a rainha Antéia disse ao seu marido Próito que Belerofonte tentou estuprá-la e ordenou que o Próito matasse Belerofonte. Não tendo coragem para tal ato, o rei Próito enviou Belerofonte ao rei de Lícia (sogro de Próito) dando a ele tabuinhas (*tablets*) que continham uma mensagem escondida contando o desejo do rei Próito.

Inúmeras histórias de Heródoto [Herodotus, 1972] tratam especificamente de métodos esteganográficos. Em uma delas relata-se que uma mensagem de Harpagus foi colocada no interior de um animal. Dessa forma, a mensagem conseguiu ultrapassar a guarda do rei de Medes e conseguiu chegar a Ciro, rei da Pérsia. A mensagem ajudou Ciro a destruir o rei de Medes.

Em uma segunda história, Heródoto conta como Histiaeus queria enviar uma mensagem a seu genro Aristagoras na tentativa de acertar uma rebelião contra os Persas. Sabendo que as estradas encontravam-se vigiadas, Histiaeus raspou a cabeça do seu escravo mais confiável, tatuou a mensagem nela, esperou o cabelo crescer e o enviou a Aristagoras. Chegando a seu destino, o escravo pediu para Aristagoras raspar seu cabelo e ler a mensagem [Kahn, 1996].

O grego “Aeneas – o tático” (*Aeneas - the Tactician*) [Aeneas, 1997] escreveu um capítulo inteiro de segurança em comunicações em um dos seus trabalhos sobre ciência militar. Nele, ele lista uma série de sistemas esteganográficos. Um exemplo de tais técnicas consistia em fazer buracos em discos. Tais buracos representavam letras do alfabeto grego. Outro exemplo que é utilizado ainda hoje consistia em pintar pequenos pontos acima ou abaixo das letras de um texto.

A evolução da esteganografia segue o mesmo caminho na Ásia. A Índia possui uma literatura repleta de referências a técnicas para escrita encoberta. Artha-sátra, Lalita-Vistara e Kama-sutra são exemplos de trabalhos que possuem referências a diferentes técnicas de

² A primeira aparição de esteganografia pode ser vista em [Kahn, 1996] onde são desvendadas as origens da escrita encoberta desde 4000 anos atrás até o Nilo, quando substituições de símbolos hieroglíficos foram usadas para inscrever informações na tumba do nobre Khnimhotep II. Entretanto, uma vez que o uso dessas substituições é ambíguo, não seria prudente considerar essa a primeira aparição evidente do uso de esteganografia.

esteganografia [Kobayashi, 1997]. O Kama-sutra de Vātsyāyana, por exemplo, lista a escrita encoberta como um dos sessenta e quatro iogas que as mulheres deveriam saber e praticar. O ioga é chamado “mlecchita-vikalpā” e consiste em substituições de letras baseada no relacionamento fonético entre as mesmas [Kahn, 1996].

Outro exemplo de técnica primitiva de esteganografia foi utilizado na China antiga, e consistia em escrever a mensagem num papel, esconder esse papel em qualquer objeto, por exemplo, uma pedra ou madeira e esconder esse objeto no próprio corpo, na maioria dos casos, engolindo-o. É importante lembrar que, apesar de primitiva, uma técnica similar a esta ainda é usada por traficantes de drogas que tentam atravessar fronteiras.

Alguns dos textos discutidos nesta seção estão apresentados no Anexo A, na página 68 deste documento.

2.1.2. TEMPOS MODERNOS

Apesar de existirem inúmeras histórias de usos de esteganografia datadas dos tempos antigos, resumidamente descritas acima, o termo “esteganografia” só ficou conhecido no século XV, depois da aparição do livro de Trithemius, intitulado *Steganographia* [Trithemius, 1500]. Nesse livro, o monge Trithemius detalhava várias técnicas para passar mensagens despercebidas. Para maiores detalhes das técnicas descritas por Trithemius, o leitor pode consultar [Davern, 1995] e [Trithemius, 1500].

Outro grande pesquisador da área de esteganografia foi Gaspari Schotti, que também apresentava inúmeras técnicas esteganográficas em seu livro *Schola Steganographica* [Schotti, 1665]. Nesse livro, por exemplo, Gaspari Schotti explica como esconder mensagens em notas musicais, onde cada nota corresponde a uma letra, como ilustrado na Figura 4. Nesta, (a) representa o mapeamento entre letras e notas musicais e (b) representa a “composição” baseada em uma frase. É importante mencionar que a música composta não deveria ser tocada uma vez que ela não seria necessariamente agradável aos ouvidos. Mesmo assim, o exemplo ilustrado constitui uma técnica de esteganografia uma vez que as composições passariam despercebidamente por todos que não entendessem de música.



(a)



(b)

Figura 4: Exemplo de esteganografia baseado no mapeamento letra – nota musical. (a) apresenta o mapeamento. (b) representa uma composição baseada em uma frase. Fonte: [Schotti, 1665].

Outros exemplos de inserções de mensagens em obras musicais são atribuídos ao brilhantismo de Johann Sebastian Bach. Trabalhos recentes de Helga Thoene [Bach, 2001] comprovam a inserção de informações escondidas em seis peças para solo de violino (BWV 1001-1006). Esta obra foi escrita por Bach em 1720, após a morte de sua primeira esposa Maria Bárbara Bach e ficou conhecida como “epitáfio em música” (à sua esposa) e é repleta de menções à morte e indicações para interpretá-la não como solo de violino senão com acompanhamento de corais. Alguns trechos dessa obra são apresentados no Anexo B e podem ser melhor estudados em [Bach, 2001] e [Bach, 2002].

Até a segunda guerra mundial, os métodos esteganográficos se baseavam quase que exclusivamente em tintas invisíveis. Com essas tintas, as entrelinhas de uma carta aparentemente inocente poderiam conter uma mensagem secreta. Durante as duas guerras mundiais, o uso de tintas invisíveis foi aprimorado para tornar mais difícil a detecção das mensagens atreladas. Esta prática só foi abandonada pelos alemães depois do desenvolvimento da microfilmagem de informações.

Além de tintas invisíveis, durante a Primeira Guerra Mundial documentos textuais eram usados para esconder informações. Um exemplo desse uso pode ser visto em uma mensagem enviada por um espião alemão na primeira guerra mundial [Kahn, 1996]:

*“Apparently neutral’s protest is thoroughly
discounted and ignored. Isman hard hit.
Blockade issue affects pretext for embargo
on by-products, ejecting suets and vegetable oils.”*

Trecho 1: Mensagem esteganográfica transmitida durante a I guerra mundial. Fonte: [Kahn, 1996].

Extraíndo a segunda letra de cada palavra da mensagem acima, revela-se a seguinte mensagem escondida:

“Pershing sails from NY June 1”

Trecho 2: Mensagem atrelada, referente as segundas letras de cada palavra da mensagem do Trecho 1. Fonte: [Kahn, 1996].

O conteúdo da mensagem se referia ao comandante das forças aliadas John J. Pershing. Entretanto, a mensagem foi inútil uma vez que o comandante saiu de Nova York no dia 28 de maio [Kahn, 1996].

Atualmente, várias metodologias podem ser usadas para esconder informações em documentos textuais [Barán, 2001], [Bender, 1996] e [Kobayashi, 1997]. Nesses métodos, não só são usadas algumas das técnicas acima citadas, mas também métodos que utilizam espaços em branco após cada linha para codificar mensagens, métodos sintáticos e semânticos (uso de sinônimos, por exemplo), entre outros.

Para um maior estudo sobre outras técnicas antigas de esteganografia, o leitor pode consultar [Katzenbeisser, 2000], [Petitcolas, 1999], [Davern, 1995], [Anderson, 1998] e [Kobayashi, 1997]. Outras metodologias utilizadas na segunda guerra mundial podem ser vistas em [Kahn, 1996] e [Kobayashi, 1997].

2.2. MARCAÇÃO DIGITAL

A proteção dos direitos autorais possui um passado nebuloso. Até os anos vinte do século passado, o único esquema de marcação digital amplamente conhecido consistia da inserção de símbolos e logotipos da editora e/ ou do autor em seus respectivos livros. Além disso, uma vez que a área de marcação digital está intrinsecamente relacionada com a área de esteganografia,

muitos autores da literatura aqui consultada apresentam os aspectos históricos de esteganografia como sendo também os aspectos históricos de marcação digital.

Uma vez que os aspectos históricos de esteganografia já foram cobertos, serão apresentados exemplos complementares que envolveram não apenas esteganografia, mas que, de alguma forma, tentaram garantir a proteção dos direitos autorais.

Um dos exemplos mais famosos de inserção de direitos autorais envolve o famoso livro *Hypnerotomachia Poliphili* (traduzido para o inglês “The Strife of Love in a Dream”), escrito anonimamente e publicado por Aldus Manutius em 1499. Em 1512, vários leitores descobriram que a junção das primeiras letras dos 38 capítulos do livro formava a frase “Poliam frater Franciscus Columna peramavit”, a qual possui a seguinte tradução para o português: “Irmão Francisco Colonna ama passionadamente Polia”. Colonna era um monge dominicano ainda vivo quando o livro foi publicado, justificando assim o motivo do anonimato. A identidade de Polia ainda é um mistério até a presente data [Kobayashi, 1997].

Outro exemplo da utilização de técnicas esteganográficas para a proteção é relacionado com o livro intitulado “The Testament of Love”, atribuído a Chaucer em 1532. Em 1897, Walter W. Skeat estava editando esse livro, quando descobriu que as letras iniciais de seus vários capítulos sugeriam uma mensagem. Com algumas junções, a mensagem dizia: “Margarete of Vitruw, have merci on thin[e] – Usk –”, indicando que o verdadeiro autor do livro era Thomas Usk e não Chaucer [Kahn, 1996], como algumas pessoas já suspeitavam.

O exemplo mais conflitante de proteção de direitos autorais é conhecido como a controvérsia Bacon/ Shakespeare. Kahn [Kahn, 1996] ilustra como um grupo de criptanalistas dogmáticos chamado *Baconians* citam inúmeros exemplos de códigos e técnicas esteganográficas que tentam atribuir a Sir Francis Bacon a verdadeira autoria de vários trabalhos atribuídos a William Shakespeare. Não existe nenhuma comprovação de que Sir Francis Bacon seja o real autor desses trabalhos. Para uma maior discussão sobre essa controvérsia, o leitor pode consultar o capítulo 24 de [Kahn, 1996].

A proteção de direitos autorais não se restringia à autoria de livros e trabalhos textuais, mas também composições. Bach desenvolveu diferentes técnicas para inserir o código “BACH” em suas composições. Em uma dessas técnicas, a contagem do número de ocorrências de uma nota representava uma determinada letra (uma ocorrência representava a letra A; duas ocorrências para a letra B, três para a letra C e oito ocorrências para a letra H). Como exemplo, seu coral para órgão intitulado *Vor deinem Thron* é repleto desse tipo de

inserção [Kobayashi, 1997]. Outro exemplo desse tipo de inserção também pode ser visto em [Bach, 2001].

2.3. FERRAMENTAS EXISTENTES

Esta seção apresenta as principais ferramentas existentes no que diz respeito a área de mascaramento de informações. Devido ao grande número de ferramentas relacionadas com a área de mascaramento de informações, os exemplos aqui apresentados formam apenas uma amostra deste universo. Exemplos comercialmente bem sucedidos foram preferencialmente incluídos uma vez que sua qualidade já foi verificada pelo usuário final. Além disso, é importante mencionar que softwares para aplicações de marcação digital são mais difíceis de serem encontrados e, por isso, os dois exemplos apresentados nessa seção se referem a sub-área de esteganografia.

É importante deixar claro ao leitor que os exemplos aqui apresentados podem estar defasados em relação a data que esse documento está sendo acessado. Novas buscas nos melhores engenhos de busca (como o Google [Google, 2002]) podem trazer exemplos de ferramentas mais atuais.

Além disso, é importante mencionar também que, no decorrer da pesquisa relacionada a esse trabalho, não foi encontrado nenhum *framework* para o desenvolvimento de aplicações de mascaramento de informações em imagens. Entretanto, muitos *benchmarks* para testes de resistência a ataques (ver seção 5.2) foram encontrados, como por exemplo o StirMark [Petitcolas, 2001], o Checkmark [Checkmark, 2003] e o Optimark [Optimark, 2003]. Como o objetivo principal desse trabalho não é o desenvolvimento de um *benchmark*, esses não serão detalhados nesse capítulo.

2.3.1. *INVISIBLE SECRETS 2002*

O Invisible Secrets 2002 [Neobyte, 2002] é uma ferramenta própria para a aplicação de comunicação encoberta através de esteganografia. Na presente data (fevereiro de 2003) essa ferramenta pode ser gratuitamente obtida para avaliação num período de trinta dias.

Essa ferramenta permite esconder informações em diferentes formatos de mídias. Entretanto, não fica especificado que técnicas são utilizadas no processo esteganográfico nem a possibilidade do usuário escolher alguma técnica esteganográfica.

Além disso, a ferramenta suporta a cifragem dos dados antes do mascaramento dos mesmos. Várias técnicas de criptografia podem ser utilizadas, como AES – Rijndael, Twofish, RC4, Cast 128, GOST, Diamond 2, Sapphire II e Blowfish, e outras podem ser adicionadas. Para maiores informações sobre algumas dessas técnicas, o leitor pode consultar [Schneier, 1996].

Em termos de esteganografia, a ferramenta consegue esconder informações em diferentes formatos de mídias. Em imagens, arquivos JPEG, BMP e PNG são aceitos. Para textos e arquivos de áudio, são aceitos como entrada arquivos de formato HTML e WAV, respectivamente. Além disso, a ferramenta possui como funcionalidade adicional a capacidade de compactar as informações antes da inserção. Testes iniciais comprovam a eficácia dessa ferramenta em termos do mascaramento de informações em imagens, deixando as imagens produzidas (estego-imagens) bem próximas da imagem original (imagem guardada).

A Figura 5 apresenta a tela principal dessa ferramenta. É possível observar as opções de cifrar/ decifrar uma informação, escondendo ou não esta em algum objeto guardado (*carrier file*).



Figura 5: Tela principal do Invisible Secrets.

2.3.2. STEGANOS SECURITY SUITE

O Steganos Security Suite [Steganos, 2003] é uma ferramenta que possui várias funcionalidades em relação a alguns aspectos da segurança de sistemas. Na presente data (fevereiro de 2003)

essa ferramenta pode ser gratuitamente obtida para avaliação num período de trinta dias. Algumas dessas funcionalidades são listadas a seguir.

- Steganos Safe – possibilita a criação de um drive seguro no computador, onde todos os dados enviados para esse drive são automaticamente cifrados;
- Email Encryption – possibilita cifrar/ decifrar mensagens eletrônicas;
- Steganos File Manager – permite que arquivos e pastas sejam cifrados e escondidos em objetos guardadas (opcionalmente). Essa funcionalidade será detalhada mais adiante nessa seção;
- Steganos Shredder – possibilita a exclusão segura de arquivos, eliminando inclusive possíveis rastros dos mesmos no disco rígido do computador;
- Password Manager – permite a armazenagem segura de várias senhas em um único lugar.

Essas e outras funcionalidades podem ser vistas na tela principal da ferramenta, apresentada na Figura 6.



Figura 6: Tela principal do Steganos Security Suite.

Em termos de criptografia, essa ferramenta não fornece (para nenhuma de suas funcionalidades) a opção de escolher que técnica de criptografia é desejada pelo usuário. Além disso, não é dito também que técnica é utilizada pela própria ferramenta.

Em termos esteganográficos, o Steganos File Manager permite que arquivos ou pastas do computador sejam cifrados e escondidos em algum objeto guardado. Infelizmente, não é fornecido ao usuário nem a opção de escolher uma nova técnica de esteganografia nem a informação de que técnica é utilizada. Além disso, não é dito também que tipos de objetos guardados a ferramenta suporta. Entretanto, testes preliminares também comprovam que a eficácia no mascaramento de informações em imagens, deixando a estego-imagem bastante próxima da imagem guardada.

3. TERMINOLOGIA E CLASSIFICAÇÕES

*É preciso estudar muito
para saber um pouco.
(Montesquieu)*

O capítulo anterior apresentou os principais aspectos históricos da área de mascaramento de informações. Além disso, exemplos de ferramentas existentes para a área também foram apresentados.

Nesse capítulo será apresentada uma proposta de terminologia para a língua portuguesa empregada para as diversas técnicas e metodologias da área de mascaramento de informações, uma vez que não existe um consenso dos termos adotados nessa língua.

Além disso, uma vez que não existe um consenso também referente às possíveis classificações de técnicas de mascaramento de informações, será apresentada uma proposta de classificação para as técnicas de mascaramento de informações (dando ênfase as técnicas de marcação digital).

3.1. TERMINOLOGIA

Nessa seção será apresentada a terminologia que será usada nesse trabalho, em acordo com [Pfitzmann, 1996].

Na literatura em português consultada até o momento de preparação deste trabalho (fevereiro de 2003), não foi encontrada nenhuma convenção aceita para os termos usuais em mascaramento de informações. Assim sendo, no decorrer desta seção, iremos propor alguns termos e/ou traduções para o português para os principais conceitos que irão aparecer no decorrer deste trabalho. Esta proposta é provisional, e pode vir a ser modificada conforme surjam outras evidências ou melhores alternativas.

O problema geral, isto é, *information hiding*, será denominado mascaramento de informações. O *embedded data* (a mensagem atrelada) é a mensagem que determinada pessoa deseja mandar secretamente. Ela é normalmente escondida em uma mensagem normal

referenciada como *cover-text* (texto guardada), ou *cover-audio* (áudio guardada) ou *cover-image* (imagem guardada) dependendo do caso, produzindo assim o *stego-text* (estego-texto), *stego-audio* (estego-áudio) ou o *stego-image* (estego-imagem). Genericamente, uma técnica de estenografia produz um *stego-object* (estego-objeto). Normalmente, uma *stego-key* (estego-chave) é usada para controlar o processo de esconder (ou detectar, respectivamente) a informação no objeto-guardada (estego-objeto, resp.) No contexto de *digital marking* ou *digital watermarking* (marcação digital, no nosso vocábulo), o estego-objeto é usualmente referenciado como “objeto marcado”.

É importante mencionar para referências futuras que, no contexto de criptografia, a mensagem original é denominada “mensagem pura”, “mensagem simples” ou ainda “mensagem plana” (do inglês *plaintext*), e a mensagem que possui informações, mas que não pode ser lida pois está codificada, é denominada mensagem embaralhada (*ciphertext*). O processo de transformação da mensagem plana em uma mensagem embaralhada é chamado de “cifragem”. O processo contrário é conhecido como “decifragem” [Schneier, 1996].

Como notação nesse trabalho e até que se diga o contrário, a imagem guardada será referenciada como I , a estego-chave como K , a marca digital como W e a estego-imagem como I' .

3.2. CLASSIFICAÇÃO

Não há consenso sobre as classificações para mascaramento de informações. Apesar disso, nessa seção tentaremos apresentar algumas possíveis classificações baseadas na Figura 1 e em [Pfitzmann, 1996], [Petitcolas, 1999], [Kutter, 1999], [Park, 2001] e [Lee, 2001].

Uma vez que a sub-área de marcação digital é conhecida como a sub-área mais complexa do mascaramento de informações, as classificações aqui apresentadas serão direcionadas para ela. Entretanto, algumas classificações também podem ser levadas para o contexto de esteganografia, como por exemplo as classificações 3.2.1 e 3.2.4.

3.2.1. CLASSIFICAÇÃO POR CATEGORIA DO ESTEGO-OBJETO

Essa classificação já foi mencionada na seção Terminologia. Usualmente, utilizam-se mídias como: texto, imagem, áudio e vídeo para servirem como receptáculos das mensagens a serem encobertas.

3.2.2. CLASSIFICAÇÃO POR VISIBILIDADE

Outra classificação possível é no que diz respeito à visibilidade da marca digital. Pode ser dividida em marcação digital visível e invisível, como descrito a seguir.

3.2.2.1. MARCAÇÃO DIGITAL VISÍVEL

Alguns esquemas de marcação digital inserem visualmente uma marca no objeto digital. Marcação digital visível está fortemente ligada a marcas em papéis que apareceram no final do século XIII para diferenciar fabricantes de papel daquela época [Rudin, 1990]. Mais modernamente podemos mencionar as imagens oferecidas pela Corbis [Corbis, 2002] e pelo Vaticano [Mintzer, 1996], já apresentados na Figura 3.

3.2.2.2. MARCAÇÃO DIGITAL INVISÍVEL

O estudo de marcação digital se concentra quase que totalmente ao estudo de técnicas de marcação digital invisível. Tal fato deve-se à gama de aplicações para tal método, que podem ser vistas no capítulo 4 deste documento.

3.2.3. CLASSIFICAÇÃO PELO TIPO DA MARCA

Como discutido em [Lee, 2001], a marca pode ser classificada em formato de ruído ou em formato de imagem, descritos a seguir.

3.2.3.1. MARCA DIGITAL EM FORMATO DE RUÍDO

Neste caso, a marca é formada por uma seqüência aleatória ou pseudo-aleatória de números que são incluídos no estego-objeto. Tais seqüências são mais usadas do que quaisquer outros tipos de marca, são mais robustas a ataques criptográficos além de serem mais fáceis de serem geradas [Lee, 2001].

3.2.3.2. MARCA DIGITAL EM FORMATO DE IMAGEM

Imagens digitais de logotipos, por exemplo, podem ser incluídas nessa categoria de marca digital. Esse tipo de marca pode ser distinguido visualmente após a extração, o que não aconteceria no caso anterior. Em alguns casos, a inserção de uma marca pseudo-aleatória pode ser obtida através de funções de *hash* [Schneier, 1996] da marca original, ou seja, da imagem.

3.2.4. CLASSIFICAÇÃO PELO MÉTODO DE PROCESSAMENTO

Os métodos de processamento de marcas digitais podem ser classificados em dois conjuntos: métodos que trabalham no domínio espacial e métodos que trabalham no domínio transformado.

3.2.4.1. MÉTODOS DO DOMÍNIO ESPACIAL

As técnicas de mascaramento de informações que trabalham no domínio espacial inserem a marca ou mensagem atrelada na própria imagem, sem fazer nenhum processamento prévio dos dados. Inserção LSB e Patchwork são exemplos desse tipo de processamento. [Bender, 1996], [Hartung, 1999], [Lee, 2001] e [Swanson, 1998] apresentam outros exemplos de técnicas que utilizam o domínio espacial para o mascaramento de informações.

3.2.4.2. MÉTODOS DO DOMÍNIO TRANSFORMADO

Por outro lado, técnicas de mascaramento de informações que trabalham no domínio transformado inserem a marca ou mensagem atrelada não diretamente na imagem, mas em uma transformada dela. Uma vez inserida a informação, a transformada inversa é aplicada para gerar uma estego-imagem, idealmente próxima da imagem original (imagem guardada). Técnicas que utilizam o domínio transformado são mais robustas e resistentes a possíveis ataques do que as que atuam no domínio dos dados [Hartung, 1999], [Lee, 2001], [Swanson, 1998], [Lee, 2001]. Além disso, o recente trabalho de Ramkumar e outros [Rankumar, 2001] afirma que a capacidade de informações que podem ser atreladas no domínio transformado é superior à capacidade de informações que podem ser atreladas no domínio espacial, sem que se cause uma perda perceptível da estego-imagem em relação à imagem guardada.

3.2.5. CLASSIFICAÇÃO PELA DETECÇÃO/EXTRAÇÃO DA MARCA

No contexto de mascaramento de informações, um processo de marcação digital pode ser classificado pelos diferentes processos de detecção/ extração da marca. Dentre esses processos, podemos citar a necessidade ou não do objeto original, a natureza da marca, a maneira de reconhecimento da marca e as várias entradas/saídas dos algoritmos de mascaramento de informações, como descritos a seguir.

3.2.5.1. POR NECESSIDADE DO OBJETO ORIGINAL

Apesar de sua intrínseca relação com a seção 3.2.5.4, alguns autores preferem enfatizar essa classificação a parte, dividindo-a em marcação digital obscura e marcação digital não obscura.

MARCAÇÃO DIGITAL OBSCURA

Nesse caso, a marca pode ser extraída sem a necessidade do objeto original. É equivalente a qualquer tipo de marcação digital diferente da privada e da semi-pública (ver seção 3.2.5.4).

MARCAÇÃO DIGITAL NÃO OBSCURA

Nesse tipo de marcação digital, a extração da marca necessita do objeto original. É equivalente às marcações digitais privada ou semi-pública, descritas na seção 3.2.5.4.

3.2.5.2. PELA NATUREZA DA MARCA

Essa classificação refere-se ao acesso da informação por parte do usuário, podendo ser dividida em marcação digital aberta e marcação digital fechada.

MARCAÇÃO DIGITAL ABERTA

Esquemas de marcação digital desse tipo permitem que qualquer pessoa possa ler a marca. Dessa forma, a chance de um ataque ser bem sucedido cresce, uma vez que qualquer pessoa

tem acesso ao algoritmo de extração. Logo, a segurança de sistemas de marcação digital desse tipo deve ser questionada.

MARCAÇÃO DIGITAL FECHADA

Nesse caso, a marca só pode ser extraída por uma pessoa autorizada (com sua chave secreta). A segurança desses sistemas depende quase que exclusivamente da chave, assemelhando-se assim a algoritmos criptográficos. Apesar disso, se o método de inserção da marca não satisfizer alguns requisitos de robustez (ver seção 5.1.4), a segurança do sistema poderá estar comprometida.

3.2.5.3. POR RECONHECIMENTO DA MARCA

Esta classificação refere-se ao modo de acesso à informação escondida, podendo ser dividida em marcação digital legível e marcação digital detectável.

MARCAÇÃO DIGITAL LEGÍVEL

Em esquemas desse tipo, a marca pode ser lida pela extração da mesma. Dessa forma, esses sistemas são tipicamente mais frágeis no que diz respeito à segurança e, portanto, mais susceptíveis a ataques.

MARCAÇÃO DIGITAL DETECTÁVEL

O conteúdo da marca não pode ser lido em esquemas desse tipo. Entretanto, a existência de determinada marca no estego-objeto pode ser verificada. Sistemas detectáveis tendem a ser mais resistentes a ataques.

3.2.5.4. PELA ENTRADA/SAÍDA DO ALGORITMO DE EXTRAÇÃO

Como citado em [Petitcolas, 1999], [Kutter, 1999] e [Park, 2001], os sistemas de marcação digital podem ser divididos em cinco categorias baseadas nas suas entradas/saídas da detecção/ extração da marca. Antes de tudo, é importante definir o processo de inserção da

marca em uma imagem. Tal processo pode ser definido como uma função do tipo $I \times K \times W \rightarrow I'$, observado na Figura 7 (a).

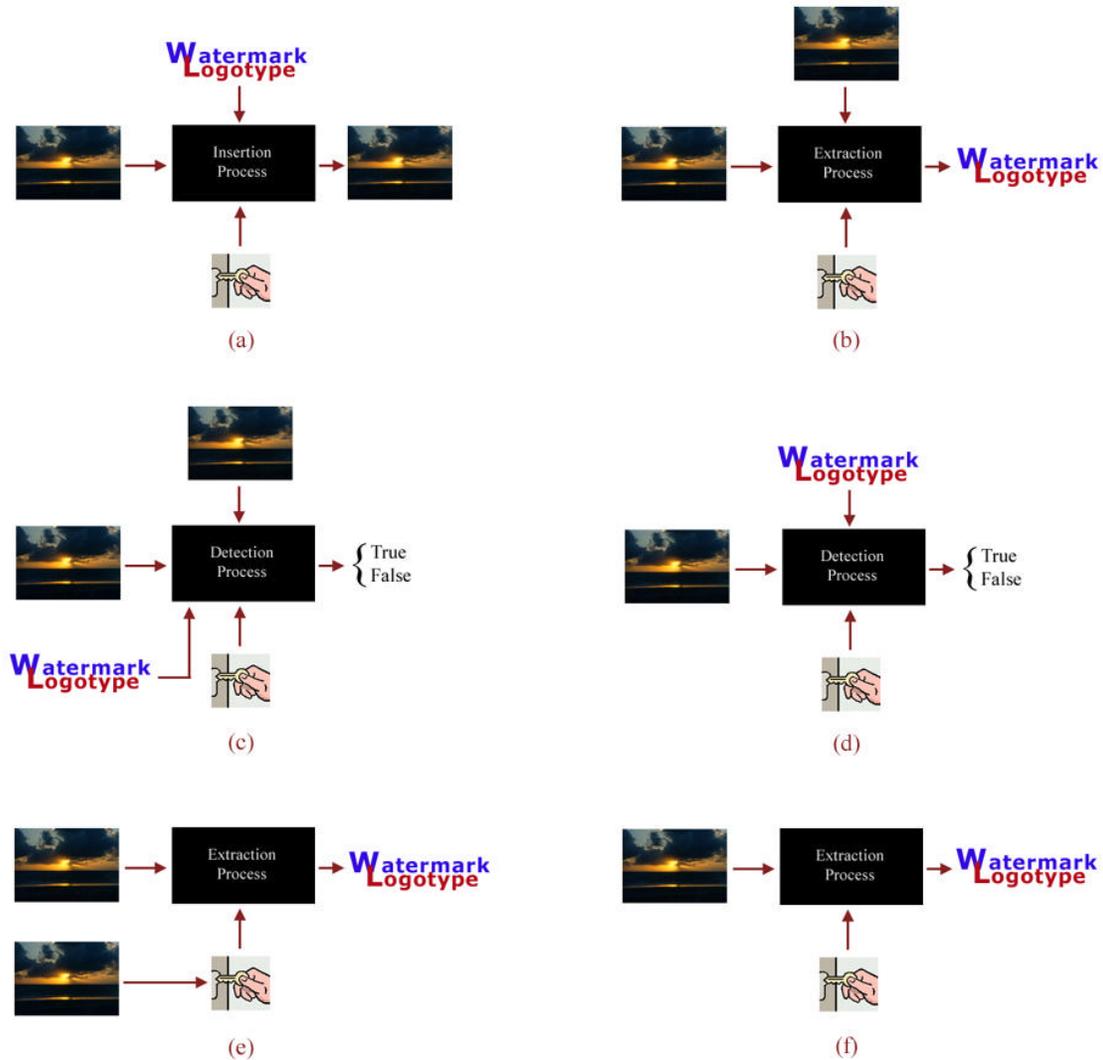


Figura 7: Processos de inserção e detecção/extração de marcação digital. Em (a), o processo de inserção. Os processos de extração e detecção da marcação digital privada são ilustrados, respectivamente, em (b) e (c). O processo de detecção da marcação digital semi-privada é apresentado em (d). Os processos de extração da marcação digital semi-pública e pública são ilustrados em (e) e (f).

MARCAÇÃO DIGITAL PRIVADA

Sistemas de marcação digital privada necessitam, ao menos, da imagem original e podem ser divididos nos sistemas do Tipo 1 e do Tipo 2. Sistemas do Tipo 1 extraem a marca W da estego-imagem I' com a estego-chave K e usam a imagem original I (imagem guardada) como

uma dica para descobrir onde a marca poderia estar em I' . Ou seja, são funções do tipo $I' \times I \times K \rightarrow W$. Sistemas do Tipo 2 necessitam de uma cópia da marca W para a extração de um campo booleano (sim/ não) para responder a seguinte pergunta: a estego-imagem I' contém a marca W ? Nesse caso, são funções do tipo: $I' \times I \times K \times W \rightarrow \{0,1\}$. Esses dois tipos de marcação digital privada são ilustrados na Figura 7 (b) e Figura 7 (c), respectivamente.

MARCAÇÃO DIGITAL SEMI-PRIVADA

Sistemas de marcação semi-privada não necessitam do uso da imagem original, mas são somente utilizados para responder a perguntas do Tipo 2 dos sistemas privados. Podem ser definidos como funções $I' \times K \times W \rightarrow \{0,1\}$. Esse processo é ilustrado na Figura 7 (d).

MARCAÇÃO DIGITAL PÚBLICA

Em sistemas de marcação digital pública, ilustrado na Figura 7 (f), a extração da marca necessita exclusivamente da estego-imagem I' e da estego-chave K . Podem ser descritas como funções $I' \times K \rightarrow W$ e são um dos maiores desafios do estudo de marcação digital, uma vez que não necessitam da imagem original I nem da marca W .

MARCAÇÃO DIGITAL SEMI-PÚBLICA

Sistemas de marcação semi-pública usam a imagem guardada I para gerar a estego-chave K . Podem ser descritas como composição da função $I \rightarrow K$ com a função de marcação digital pública $I' \times K \rightarrow W$, como ilustrado na Figura 7 (e). Tais esquemas de marcação digital não podem ser considerados públicos e possuem um universo mais limitado de aplicações [Park, 2001].

MARCAÇÃO DIGITAL ASSIMÉTRICA

A marcação digital assimétrica (ou marcação digital de chave pública) possui a propriedade de que um usuário pode ler a marca W da estego-imagem I' , mas não é capaz de extraí-la. Nesse contexto, a inserção pode ser representada como sendo uma função do tipo $I \times K_e \times W \rightarrow I'$

onde K_e representa a estego-chave de inserção, somente conhecida pelo autor da imagem. A extração pode ser representada como uma função do tipo $I' \times K_d \rightarrow W$ onde K_d representa a estego-chave de extração, publicamente conhecida por qualquer pessoa.

É esperado que sistemas de marcação digital privada ofereçam maior robustez do que os outros tipos de sistemas, uma vez que têm acesso à imagem original I e, no caso do Tipo 2, à marca W . Os sistemas de marcação digital privada e semi-privada são importantes em proteção de direitos autorais, comprovação desses direitos no tribunal, controle de cópias, entre outras aplicações. Entretanto, o universo de aplicações de sistemas de marcação digital pública aparenta ser muito maior do que os de marcação digital privada e semi-privada. Exemplos de uso desses sistemas são o controle de cópias, as legendas em imagens e vídeos, a proteção de direitos autorais, a seriação de obras etc. Além disso, algoritmos de marcação digital pública podem, em sua maioria, ser estendidos em algoritmos privados [Kutter, 1999].

3.2.6. CLASSIFICAÇÃO PELA PERSISTÊNCIA DA MARCA

A marcação digital pode ser dividida em duas categorias, como mostrado na Figura 1. Entretanto, existe já na literatura um novo conceito conhecido como marcação digital semi-frágil [Park, 2001] que será abordado logo abaixo.

3.2.6.1. MARCAÇÃO DIGITAL FRÁGIL

Os estego-objetos possuem marcas que são destruídas assim que eles são modificados de um certo número e/ou conjunto de operações. As marcas, assim, servem como prova de que o objeto foi alterado e podem ser de grande utilidade se imagens digitais forem usadas como evidência em um tribunal.

3.2.6.2. MARCAÇÃO DIGITAL ROBUSTA

Neste caso, os estego-objetos possuem marcas robustas, ou seja, que têm a propriedade de ser praticamente impossível removê-las ou torná-las inúteis sem que, ao mesmo tempo, o objeto seja destruído. Este tipo de marcação é utilizada na proteção de direitos autorais, na seriação,

em legendas de imagens, entre outras aplicações. Pela sua relevância, o conceito de robustez de marcas será tratado com mais detalhes na seção 5.1.4 deste trabalho.

3.2.6.3. MARCAÇÃO DIGITAL SEMI-FRÁGIL

Esquemas desse tipo são equivalentes a esquemas de marcação digital frágil. Entretanto, marcas de sistemas desse tipo sobrevivem a operações de compressão, como por exemplo a compressão JPEG de imagens [Wallace, 1991].

4. APLICAÇÕES

*Give me where to stand, and I will
move the earth.
(Archimedes)*

Uma proposta de terminologia para a língua portuguesa empregada para as diversas técnicas e metodologias da área de mascaramento de informações foi apresentada no capítulo anterior. Além disso, foi apresentada também proposta uma classificação dessa área.

Nesse capítulo serão apresentados alguns exemplos de aplicações da área de mascaramento de informações. Muitos exemplos aqui apresentados já possuem implementações reais, como os exemplos das seções 4.1, 4.2 e 4.3. Entretanto, muitos outros exemplos ainda não foram implantados devido a problemas diversos de padronização, como detalhadamente discutido em [Mintzer, 1998].

4.1. COMUNICAÇÃO ENCOBERTA

Este é um exemplo clássico de uso de mascaramento de informações. Suponha que um usuário de computador deseja mandar uma mensagem eletrônica secreta para determinada pessoa. Ele não sabe o quanto confiável é a rede onde ele se encontra, podendo até existir um atacante ativo, ou seja, um atacante que tem o poder de interceptar e bloquear mensagens. O uso de criptografia, nesse caso, alertaria ao atacante que algo de estranho está acontecendo, e provavelmente ele iria bloquear a mensagem para tentar extrair a informação nela escondida. Entretanto, o uso de esteganografia tornaria possível a comunicação entre os usuários, sem que o atacante tomasse conhecimento dessa comunicação.

A Figura 2 apresenta um exemplo de aplicação de comunicação encoberta. Nela, a imagem original (a) foi modificada para conter uma informação (senha), gerando assim a estego-imagem (b), que pode ser transmitida sem levantar suspeitas de um possível atacante.

É importante lembrar que, nesse exemplo de uso, é muito comum o uso de esteganografia como uma aliada da criptografia. Para dificultar ainda mais um possível ataque,

a mensagem seria cifrada, e depois escondida em determinado objeto-guarida. Isso faria com que, mesmo se o atacante descobrisse que o objeto-guarida contém alguma informação e interceptasse essa informação, ele ainda teria que decifrar a mensagem. Dependendo da criptografia utilizada, decifrar a mensagem pode levar alguns anos, décadas ou até mais [Schneier, 1996] usando equipamentos e técnicas atuais.

4.2. PROTEÇÃO DE DIREITOS AUTORAIS

Aplicações desse tipo são as mais utilizadas e pesquisadas na atualidade. Suponha que um autor de uma imagem, vídeo, som ou até mesmo texto deseja assinar sua obra de tal forma que nenhuma pessoa possa atribuir a ela sua autoria. Não é conveniente meramente anexar uma assinatura ao objeto, uma vez que pode ser facilmente removida ou substituída. Além disso, no caso de imagens, o uso exclusivo de assinaturas visíveis na própria imagem deve ser evitado, pois a maioria das técnicas que permitem trabalhar com assinaturas visíveis é de fácil falsificação.

Exemplos desse tipo de aplicação foram apresentados na Figura 3, onde imagens digitais foram marcadas com diferentes técnicas de marcação digital. As imagens (a) e (b) foram marcadas utilizando técnicas esteganográficas. As imagens (c) e (d) foram marcadas com técnicas não esteganográficas.

4.3. SERIAÇÃO (*FINGERPRINTING*)

Existem inúmeras empresas de software que utilizam seriação na distribuição de seus produtos, sendo a plataforma Office da Microsoft um exemplo famoso. Esta técnica consiste em colocar, escondidos ou não, identificadores únicos do usuário em objetos, da mesma forma em que cada cópia de uma xilogravura é idêntica às outras a menos do número que a identifica dentro da série produzida (1/ 20, 2/ 20 etc.). Dessa forma, é possível detectar e identificar a cópia ilegal de produtos. No passado, duplicar um trabalho artístico era muito complicado e necessitava de um especialista de tal modo que a cópia parecesse com o trabalho original, o que acarretava em grandes gastos de dinheiro. Entretanto, no mundo digital, isso não é verdade.

4.4. CERTIFICAÇÃO E CONTROLE DE ACESSO

A certificação é uma operação importante em documentos oficiais como, por exemplo, carteiras de identidade e passaportes. A marcação digital permite validar as informações contidas em um documento através da sua vinculação. Um exemplo dessa aplicação pode ser visto no cartão de identificação mostrado na Figura 8. Nesse cartão, o identificador do cartão é mostrado em formato textual abaixo da imagem, mas também é escondido na fotografia. Dessa forma, se o cartão fosse falsificado seria possível detectar a alteração pois o vínculo entre o conteúdo textual explícito e a informação escondida estaria perdido. Para isso, basta ter acesso às informações escondidas na fotografia através da digitalização da mesma.



Figura 8: Exemplo de um cartão de identificação marcado. O número de identificação "123456789" está escrito em forma de texto e também escondido como uma marca na foto. Fonte: [Kutter, 2001].

Outro exemplo de aplicação possível é na padronização entre navegadores para Internet, como descrito em [Fridrich, 1998]. Os navegadores poderiam possuir ferramentas de tal forma que, após o navegador baixar uma imagem, a mesma fosse verificada em busca da presença de marcas digitais e suas propriedades. Caso assim especificasse o dono da imagem, o visitante teria acesso à imagem e o navegador a exibiria. Entretanto, caso o detentor dos direitos sobre a imagem especificasse que o usuário não teria acesso à imagem, o usuário não teria acesso mesma, o navegador não a exibiria e a apagaria do computador. Neste caso, para o usuário ter acesso a essa imagem, ele teria que se registrar para receber um arquivo de configuração que lhe franquearia o acesso às informações desejadas. A mesma idéia pode ser estendida para outros tipos de mídia, não necessariamente suportados por navegadores, como é o caso de DVDs (*Digital Video Discs*).

4.5. LEGENDAS EM IMAGENS E VÍDEOS

Em aplicações desse tipo, as legendas são escondidas em imagens ou vídeos de modo que as mesmas possam ser extraídas e apresentadas. Um exemplo de uso seria um filme com legendas de diferentes idiomas escondidas no filme. Dessa forma, VCRs (*Video Cassette Recorders*), aparelhos de DVD e até mesmo aparelhos televisores poderiam ter acesso e decodificar as legendas desejadas em tempo real de cada quadro e apresentá-las na tela da TV. É importante observar que esse método não se limita somente a legendas, podendo ser utilizado também para o som ou para as informações adicionais de um filme de DVD, por exemplo.

4.6. CONTROLE DE CÓPIAS

O controle de cópias poderia ser empregado pelas empresas fabricantes de DVDs. Um filme comercial poderia conter uma marca digital que especificasse se e quando o filme poderia ser copiado. O aparelho de DVD capaz de acessar a marca poderia, então, proibir a cópia do disco para outro disco. Entretanto empresas que pagaram para ter acesso a cópias de DVDs, poderiam ter outros aparelhos que quando acessassem a marca digital, teriam a gravação franqueada.

Muitas companhias estão trabalhando em controle de cópias para o DVD. Muitas soluções já foram propostas e algumas já estão funcionando. Entretanto, atualmente, elas ainda não foram inteiramente aprovadas pelos produtores e fabricantes, dificultando assim a padronização. Para maiores informações e discussões sobre padronização de técnicas de marcação digital para DVD e outras aplicações, o leitor pode consultar [Mintzer, 1998].

4.7. AUTENTICAÇÃO E VERIFICAÇÃO DA INTEGRIDADE

Atualmente, as imagens não podem ser aceitas como provas em julgamentos devido ao fato de que ainda é fácil alterá-las sem que seja possível detectar se houve manipulação. Com o uso de marcas digitais essa situação poderia ser alterada em favor do uso deste tipo de mídia.

Uma câmera digital, por exemplo, pode incluir uma marca na imagem antes que ela seja gravada em meio permanente. Dessa forma, o uso de marcação digital em imagens para a identificação do lugar de origem e a verificação de alterações na imagem desempenhará um

papel importante na detecção de fraudes digitais e poderão ser usadas como provas ou contra-provas num julgamento.

Outro exemplo desse tipo de aplicação pode ser visto na Figura 9. Nela, a figura à esquerda mostra uma foto de um carro que foi protegida com uma marca digital. Ao centro, a mesma figura é mostrada mas com uma pequena alteração: a placa do carro foi alterada. A figura à direita mostra a foto após rodar o programa de detecção de marca digital na foto alterada. As áreas indicadas de branco no centro da imagem mostram onde ocorreu a alteração.



Figura 9: Uso de marcação digital para verificação da integridade de imagens. À esquerda, a imagem protegida. Ao centro, a imagem alterada. À direita, as áreas modificadas descobertas.

Fonte: [Kutter, 2001].

5. REQUISITOS E ATAQUES

*Science is nothing but trained and
organized common sense
(T.H. Huxley, 1878)*

O capítulo anterior apresentou algumas possíveis aplicações para a área de mascaramento de informações. Os exemplos de aplicações citados formam apenas uma amostra do universo de aplicações que podem ser desenvolvidas na área.

Neste capítulo serão apresentados os principais requisitos de aplicações de mascaramento de informações. Apesar de também poderem ser usados no contexto de esteganografia, os requisitos Robustez e Falsos positivos devem ser mais considerados para aplicações de marcação digital.

Além disso, o presente capítulo também apresenta possíveis ataques a mascaramento de informações. Novamente essa seção é voltada para aplicações de marcação digital, uma vez que essas demandam maior complexidade nos ataques. Entretanto, ataques descritos na subseção 5.2.1 podem também ser utilizados no contexto de esteganografia.

5.1. REQUISITOS

Essa seção apresenta os principais requisitos de aplicações de mascaramento de informações. É importante mencionar que os requisitos aqui apresentados são dependentes da aplicação que, normalmente, não exige todos simultaneamente.

Como dito anteriormente, é importante mencionar que o requisito de robustez, apesar de também poder ser utilizado em aplicações de esteganografia, é mais amplamente usado em aplicações de marcação digital.

5.1.1. *INVISIBILIDADE (TRANSPARÊNCIA PERCEPTUAL)*

A impossibilidade de perceber a marca é um requisito importante para algumas técnicas de marcação digital. Esse conceito é baseado nas propriedades do sistema visual humano. O

maskamento de mensagens é verdadeiramente imperceptível se nenhuma pessoa pode diferenciar entre a imagem guardada e a estego-imagem [Swanson, 1998].

Métricas como Erro Quadrático Médio, Relação Sinal/ Ruído e Similaridade de Histograma, entre outras, são utilizadas para medir quão diferentes são a imagem guardada e a estego-imagem. Além dessas métricas, é comum também o uso de testes de imperceptibilidade. Nesses testes, pessoas são apresentadas aleatoriamente a imagens que contém mensagens atreladas e a imagens que não contém tais mensagens. Logo em seguida essas pessoas são questionadas a determinar qual imagem possui uma maior qualidade. Se a probabilidade estimada de selecionar a imagem sem informações atreladas não for significativamente diferente de $1/2$, a técnica de maskamento de informações produz estego-imagens com alterações imperceptíveis (em sentido estatístico) em relação à imagem guardada.

Para maiores informações sobre as métricas acima citadas e outras métricas, o leitor pode consultar [Kutter, 1999] e [Eskicioglu, 1995].

5.1.2. CUSTO COMPUTACIONAL

Algumas aplicações necessitam que os dispositivos de inserção e/ ou extração trabalhem em alta velocidade. Entretanto, é importante deixar claro que tal necessidade depende quase que exclusivamente da aplicação em questão.

Como exemplo, aplicações como a inserção de marcas em vídeos a serem transmitidos, como no caso de sistemas televisivos, o processo de inserção e extração das marcas deve ser de tempo real. Por outro lado, um detector de direitos autorais será útil mesmo que ele leve dias até encontrar a marca [Cox, 2000].

Além disso, é importante lembrar que nem sempre é desejável que o processo de inserção e/ ou extração da mensagem/ marca seja feito sempre a uma alta velocidade. Como exemplo, é importante que sistemas de marcação digital pública (ver seção 3.2.5.4) levem bastante tempo na detecção/ extração da marca, evitando assim um possível ataque de força bruta na estego-chave.

5.1.3. CAPACIDADE

Algumas aplicações de maskamento de informações, como proteção de direitos autorais, autenticação e serialização, necessitam relativamente de poucos dados a serem incluídos

repetidamente na imagem. Entretanto, outras aplicações como comunicação encoberta e legendas em imagens necessitam de uma banda maior uma vez que a quantidade de informações que serão atreladas à imagem não é pequena.

A habilidade de atrelar quantidades altas de dados em uma imagem guardada dependerá muito de como o algoritmo de mascaramento de informações poderá adaptar sua estratégia de inserção às informações envolvidas. Para uma maior estudo sobre a capacidade de mascaramento de informação em imagens digitais, o leitor pode consultar [Rankumar, 2001].

5.1.4. ROBUSTEZ

Algumas técnicas de marcação digital para imagens necessitam ser resistentes em relação a diferentes técnicas de processamento de imagens. Tal robustez é importante uma vez que um possível atacante pode fazer uso dessas mesmas técnicas de processamento para tentar remover a marca da estego-imagem. Logo abaixo estão descritas algumas técnicas de processamento de imagens importantes nesse contexto.

5.1.4.1. COMPRESSÃO/DESCOMPRESSÃO JPEG

A compressão (e descompressão) JPEG é uma das mais utilizadas técnicas de codificação de imagens com perda. Dessa forma, técnicas robustas de marcação digital devem ser resistentes a algum grau de compressão/ descompressão. Para maiores informações sobre a técnica de compressão/ descompressão JPEG, o leitor pode consultar [Wallace, 1991].

5.1.4.2. TRANSFORMAÇÕES

Serão descritas a seguir as principais transformações de imagens que podem ser usadas para remover marcas escondidas. Para tanto, a imagem de interesse será denotada como uma função g definida sobre um suporte que é o produto cartesiano de dois intervalos de inteiros, de m colunas por n linhas, denotado $S = [0, m - 1] \times [0, n - 1] \subset \mathbf{Z}^2$ e com contradomínio um conjunto conveniente K [Banon, 1998]. As transformações definidas a seguir irão construir uma nova imagem g' alterando o suporte de g .

ESPELHAMENTO HORIZONTAL

Formalmente esta operação consiste em transformar $g \rightarrow g'$ fazendo $g'(i, j) = g(m - i - 1, j)$ para toda coordenada (i, j) . Muitas imagens podem ser espelhadas horizontalmente sem perder qualquer valor, como por exemplo paisagens nas quais não aparece nenhum conteúdo textual (ver Figura 10). A maioria das técnicas de marcação digital não é robusta a esse tipo de transformação.



Figura 10: Exemplo de espelhamento horizontal. À esquerda, a imagem original e à direita a imagem transformada.

RECORTE (CROPPING)

Algumas vezes, possíveis atacantes só estão interessados na parte central da imagem e podem usar o recorte para obter a informação desejada. Esta transformação consiste, portanto, em construir uma nova imagem g' com domínio $S' = [a_1, b_1] \times [a_2, b_2] \subset S$ fazendo $g \rightarrow g'$ com $g'(i, j) = g(i, j)$ para $a_1 \leq i \leq b_1$ e $a_2 \leq j \leq b_2$. Um exemplo dessa transformação pode ser vista na Figura 11. Em muitos casos, a marca não resiste a esse tipo de ataque.



Figura 11: Exemplo de recorte. À esquerda, a imagem original. À direita, um recorte da imagem original.

ROTAÇÃO

Normalmente aliadas a recortes (*cropping*), pequenas rotações não chegam a alterar o valor comercial de uma imagem, mas podem fazer com que a marca digital nela contida desapareça. Um exemplo dessa transformação aliada à transformação de recorte pode ser visto na Figura 12.



Figura 12: Exemplo de rotação e recorte. À esquerda, a imagem original. À direita, a imagem originada a partir da rotação (0.3 graus horários) e recorte da imagem original.

AJUSTES DE ESCALA

Ajustes de escala podem ser divididos em dois grupos: uniformes (isotrópicos) e não-uniformes. No primeiro caso, o fator de escala é o mesmo, tanto para a direção horizontal como para a vertical. Já no caso de ajustes não-uniformes, cada direção possui fatores de escala diferentes. A maioria das técnicas de marcação digital só é resistente a ajustes uniformes de escala. A Figura 13 mostra um exemplo de ajuste de escala.



Figura 13: Exemplo de ajuste de escala. À esquerda, a imagem original. À direita, a imagem obtida através de um ajuste uniforme de escala (75%).

REMOÇÃO DE LINHAS E/OU COLUNAS

Remoção aleatória de algumas linhas e/ ou colunas normalmente destrói a marca sem destruir completamente a imagem.

COMBINAÇÕES DE TRANSFORMAÇÕES

Combinações de transformações como, por exemplo, ajustes não-uniformes de escala combinados com rotações e cortes aumentam as chances da marca ser destruída. Algumas vezes, essas combinações são seguidas ou precedidas por compressão e/ ou descompressão JPEG para dificultar ainda mais a resistência da marca na imagem.

DISTORÇÕES ALEATÓRIAS

Esses tipos de distorções formam a base do ataque StirMark [Petitcolas, 2001]. Para maiores informações sobre esse tipo de transformações, o leitor pode consultar [Petitcolas, 1998].

5.1.4.3. CONVERSÕES DIGITAL/ANALÓGICO E ANALÓGICO/DIGITAL

Esses tipos de conversões normalmente adicionam ruídos e/ ou artefatos ao objeto original. Esse tipo de conversões pode ser feito pela impressão de uma imagem e posterior digitalização dessa impressão e normalmente destrói a marca.

5.1.4.4. ADIÇÃO DE RUÍDOS

A adição de ruídos (Gaussianos ou não) é muito utilizada para testar a resistência da marca em uma imagem. Em sua maioria, as técnicas de marcação digital são resistentes a essa técnica. Um exemplo desse tipo de processamento pode ser visto na Figura 14, onde a imagem a direita foi gerada a partir de uma adição de ruído da imagem a esquerda. A ferramenta empregada para ilustrar esta operação é o Photoshop [Adobe, 2003] que, por ser uma plataforma de edição pictórica de imagens, não fornece subsídios teóricos suficientes para formalizar a operação aplicada.



Figura 14: Exemplo de adição de ruído. À esquerda, a imagem original. À direita, a imagem adicionada de um ruído segundo uma distribuição uniforme.

5.1.4.5. *FILTROS PASSA-BAIXA*

É desejável também que as técnicas de marcação digital sejam resistentes a filtros lineares e não-lineares. Para testes, os filtros mais freqüentemente utilizados são os filtros da mediana (não linear) e de convolução com núcleo Gaussiano (linear) [Jain, 1988].

5.1.4.6. *QUANTIZAÇÃO DE CORES*

Em sua maioria, este processamento é aplicado na conversão da imagem para os formatos GIF (*Graphics Interchange Format*) [Compuserve, 2003] e PNG (*Portable Network Graphics*) [Boutell, 2003], intensamente usados para publicações de imagens na Web. O formato GIF, por exemplo, admite apenas 256 cores diferentes, e se a marca estava originalmente escondida empregando um número maior de cores ela poderá ser alterada por esta transformação. Formalmente, a quantização de cores é uma transformação entre contradomínios, isto é, a imagem $g : S \rightarrow K$ é transformada na imagem $g' : S \rightarrow K'$ fazendo $g'(s) = \Psi(g(s))$.

5.1.5. *SEGURANÇA*

Em muitas aplicações, o mascaramento de informações deve ser seguro no sentido que um usuário não-autorizado não possa detectar a presença da mensagem atrelada nem possa removê-la.

Normalmente, a segurança de técnicas de mascaramento de informações é interpretada da mesma forma que a segurança de técnicas de criptografia, obedecendo assim ao princípio de

Kerckhoffs [Kerckhoffs, 1883], o qual afirma que a segurança de um sistema criptográfico (no nosso caso, de mascaramento de informações) deve restringir-se somente à escolha da chave, supondo assim que as técnicas de inserção/ detecção/ extração são conhecidas pelo atacante³. Assim, o sistema não deve poder ser quebrado até que um usuário não-autorizado tenha acesso a uma chave secreta (no nosso caso, a estego-chave) que controla a inserção da informação na imagem guardada.

Um algoritmo de mascaramento de informações é completamente seguro se, mesmo o conhecimento do algoritmo não ajuda pessoas não-autorizadas a detectar a presença da mensagem atrelada. Entretanto, se um possível atacante suspeitar da existência da mensagem e conhecer o algoritmo de inserção, ele poderá usar ataques, como o de força-bruta ou do dicionário, para determinar a estego-chave [Schneier, 1996].

5.1.6. FALSOS POSITIVOS

Um falso positivo ocorre quando a detecção de uma marca em um possível estego-objeto ocorre, mas a marca não existe no estego-objeto (logo, o estego-objeto é um objeto guardado!) Denominamos “taxa de falsos positivos” o número de ocorrências de falsos alarmes que se espera obter rodando um número grande de vezes o detector para diferentes entradas. Logo, podemos analisar a probabilidade de um falso positivo em cada rodagem do detector fazendo uma experiência hipotética com um número infinito de ensaios independentes.

A probabilidade de falsos positivos aceitáveis depende do contexto da aplicação. Numa aplicação de proteção de direitos autorais, probabilidades iguais ou inferiores a 10^{-6} são suficientes para garantir a qualidade do detector.

Por outro lado, em uma aplicação de controle de cópias, milhões de dispositivos de detecção podem estar processando milhares de mídias. Dessa forma, a geração de um falso positivo por uma mídia não marcada pode causar sérios problemas. Logo, estima-se que aplicações desse tipo devem possuir probabilidades de falso positivo menores do que 10^{-12} [Cox, 2000].

³ Princípio (original) de Kerckhoffs: “*Il faut qu’il n’exige pas le secret, et qu’il puisse sans inconvénient tomber entre les mains de l’ennemi*”. Fonte: [Kerckhoffs, 1883].

5.2. ATAQUES

Segundo [Craver, 1998], os ataques a sistemas de marcação digital podem ser divididos em quatro categorias definidas logo abaixo. É importante observar que a robustez só impede ataques de uma das quatro categorias.

5.2.1. *ATAQUES DE ROBUSTEZ*

É o principal tipo de ataque a técnicas de marcação digital, entretanto não é o único. Ataques desse tipo baseiam-se em remover ou dificultar a detecção da marca do objeto marcado sem prejudicar o mesmo de forma significativa. No caso de imagens, esses ataques alteram os valores dos pixels das imagens de modo que as marcas desapareçam sem alterar a percepção das imagens por parte dos usuários. Esse tipo de ataque pode ainda ser dividido nas categorias tratadas nas seguintes seções.

5.2.1.1. *ATAQUES DE ROBUSTEZ BASEADOS EM OPERAÇÕES DE PROCESSAMENTO*

Ataques desse tipo se resumem a operações comuns ou “inocentes” de processamento como as técnicas descritas na seção Robustez. Este tipo de ataque poderia ser considerado “ataque por força bruta”, já que não leva em conta explicitamente as propriedades matemáticas da técnica empregada. Como descrito na seção 5.1.4, muitas técnicas de marcação digital não resistem a tais processamentos. Por isso, muitos softwares de domínio público obtiveram sucesso em eliminar marcas digitais de imagens produzidas por softwares comerciais de marcação digital [Petitcolas, 2001], [Craver, 1998].

5.2.1.2. *ATAQUES DE ROBUSTEZ ANALÍTICOS*

Esse tipo de ataque utiliza-se de falhas e fraquezas dos métodos específicos de inserção, detecção e extração da marca digital. Muitas vezes, um estudo analítico da técnica utilizada é suficiente para o atacante descobrir brechas e *backdoors*⁴ para um ataque mais sofisticado e

⁴ Termo do jargão de segurança de sistemas referente a brechas na segurança que exploram falhas pouco ou não documentadas.

eficiente do que um feito a força bruta. Um exemplo clássico desse tipo de ataque é descrito em [Petitcolas, 2001] e é chamado ataque de colisão.

Esse ataque é muito utilizado em ataques a aplicações de seriação. Dois usuários com duas versões do objeto podem produzir uma nova versão do mesmo, uma vez que os identificadores escondidos em cada objeto são únicos permitindo, assim, que os dois objetos sejam comparados e que seja identificada a região em que os identificadores se encontram. Em seguida, essas regiões são alteradas de forma que não se altere o conteúdo do objeto, mas destruindo o identificador. Um exemplo desse ataque pode ser visto na Figura 15.

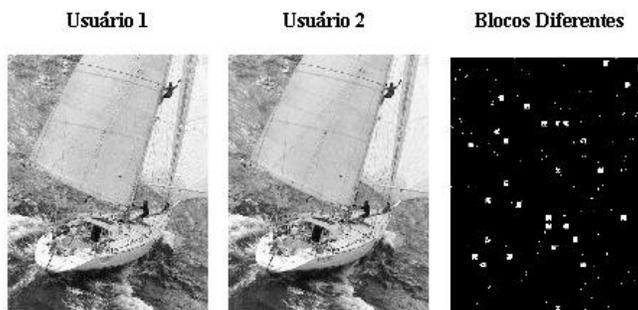


Figura 15: Exemplo de ataque de colisão. À esquerda e ao centro, imagens visualmente idênticas com identificadores diferentes. À direita, imagem gerada determinando áreas de diferenças entre as imagens. Fonte: [Petitcolas, 2001].

5.2.2. ATAQUES DE APRESENTAÇÃO

Esse tipo de ataque difere do ataque de robustez no sentido de que não é necessário remover a marca do estego-objeto. Alternativamente, o conteúdo é manipulado de tal forma que o detector não consiga ter acesso à estego-imagem. Um exemplo desse tipo de ataque foi desenvolvido por Petitcolas, e é conhecido como ataque mosaico [Fridrich, 1998], [Craver, 1998], [Petitcolas, 1998], [Petitcolas, 1999]. Esse ataque tem como finalidade enganar sistemas automáticos de detecção de cópias não autorizadas (um WebCrawler como o Google [Google, 2002], por exemplo), ou seja, sistemas que varrem a Internet a procura de cópias ilegais de imagens marcadas com uma determinada marca. A idéia por trás do ataque mosaico consiste em “quebrar” a imagem em porções menores e reorganizá-las em uma página da Internet de forma que, aparentemente, as imagens como um todo formam a imagem original. Como imagens com dimensões abaixo de um certo limite não podem ser marcadas, o sistema (WebCrawler) não irá detectar a marca em nenhuma parte do mosaico. A composição

de mosaicos é uma ferramenta comumente encontrada em sistemas de criação de sites, como o Dreamweaver [Macromedia, 2002] por exemplo. Um exemplo desse ataque pode ser visto na Figura 16.



Figura 16: Exemplo de ataque mosaico. As seis porções à esquerda formam à figura a direita (o mosaico). Fonte: [Petitcolas, 2002].

Outro exemplo desse tipo de ataque consiste em mascarar imagens em Applets Java ou Objetos ActiveX de tal forma que os WebCrawlers não consigam reconhecer as imagens, uma vez que não são mais imagens.

5.2.3. ATAQUES DE INTERPRETAÇÃO

Em alguns sistemas de marcação digital, a detecção da presença da marca pode causar múltiplas interpretações da origem dos dados. Um atacante pode criar uma situação que neutraliza qualquer evidência da marca. Por exemplo, um atacante pode tentar adicionar outra marca (a dele) na estego-imagem com mesma “presença” que a marca original, criando assim uma situação de *deadlock* [Craver, 1998].

Um possível ataque desse tipo é descrito em [Craver, 1997]. Suponha que o dono de uma imagem I e marca W publique uma versão marcada $I + W$. Um atacante que registrou a marca W' pode dizer-se dono da imagem e dizer que a “imagem original” dele era $I + W - W'$. Nesse caso, a situação de *deadlock* foi alcançada uma vez que ambos podem dizer-se donos da imagem [Petitcolas, 1998]. Maiores discussões sobre esse tipo de ataque e maneiras

para contornar problemas semelhantes ao descrito acima pode ser visto em [Craver, 1997], [Craver, 1998], [Petitcolas, 1998] e [Petitcolas, 1999].

5.2.4. ATAQUES LEGAIS

Os ataques legais consistem em aproveitar uma série de fatores que podem beneficiar o atacante devido aos aspectos legais de marcação digital [Craver, 1998]. Ataques legais envolvem legislação existente ou futura em leis de direitos autorais, interpretações diferentes das leis em varias jurisdições, credibilidade do dono da imagem e do atacante, a habilidade do atacante em gerar dúvida com relação à técnica de marcação digital em processos e muitos outros aspectos. Esses ataques também estão envolvidos com o poder financeiro do dono da imagem versus o poder financeiro do atacante, boas testemunhas e bons advogados.

6. ARQUITETURA PROPOSTA

*Bloody instructions which, being
learned, return to plague the
inventor.
(Shakespeare)*

Os capítulos anteriores tentaram demonstrar a importância da área aqui discutida, o mascaramento de informações. Foram apresentados os principais aspectos históricos, demonstrando assim que a área é bastante antiga, apesar de só recentemente ter sido levada ao contexto digital. Em seguida, foram ilustrados vários exemplos de aplicações de mascaramento de informações, mas sem a pretensão desta discussão esgotar os exemplos possíveis. Além disso, e dada a falta disto na literatura em português consultada, foi apresentada uma sugestão de terminologia e classificação para a área, bem como apresentados os principais requisitos e ataques referentes à área de mascaramento de informações.

Esse capítulo é considerado o capítulo principal da pesquisa por tratar da modelagem da arquitetura para aplicações de mascaramento de informações em imagens digitais. É importante mencionar que, apesar de bem fundamentada, a arquitetura aqui apresentada deve ser implementada e verificada sua eficácia, sua robustez e sua estensibilidade em relação ao uso de novas técnicas de mascaramento de informações.

Por se tratar de imagens, e pelo fato de várias técnicas de mascaramento de informações em imagens utilizarem técnicas específicas da área de processamento de imagens, tal como descrito nos capítulos 3 e 5, é importante que a arquitetura permita uma possível estensibilidade da mesma para técnicas de processamento de imagens, como por exemplo transformações de domínio. Tal extensão pode ser facilitada com a unificação do sistema com *frameworks* já existentes para o processamento de imagens, como, por exemplo, o JDIPF (*Java Digital Image Processing Framework*) [Castor, 2001].

Em vista disso, as seções a seguir irão apresentar e discutir as principais partes da arquitetura. A seção 6.1 descreve a modelagem do tipo imagem, onde são levantados e resolvidos problemas como o encapsulamento de diversos formatos de dados. A seção 6.2

descreve a modelagem dos métodos que fornecem o acesso aos dados. A seção 6.3 descreve a modelagem das técnicas de mascaramento que poderão ser aplicadas às imagens modeladas e trabalhadas nas seções anteriores. A seção 6.4 descreve componentes adicionais do sistema e, finalmente, a arquitetura final é descrita na seção 6.5.

6.1. MODELAGEM DA IMAGEM

Para ser feita a modelagem de uma imagem, é preciso entender a natureza da mesma. Como descrito na seção 5.1.4.2, uma imagem pode ser definida como uma função g , definida sobre o suporte de m colunas por n linhas $S = [0, m - 1] \times [0, n - 1]$ e com contradomínio K (um subconjunto dos reais, dos complexos ou p réplicas dele) [Banon, 1998]. Sejam os elementos genéricos do suporte $(i, j) \in S$ e do contradomínio $k \in K$, logo, cada mapeamento $(i, j) \rightarrow k$ é conhecido como pixel. Como diferentes imagens podem ter diferentes contradomínios (como os Reais, os Inteiros, etc.), é importante generalizar uma imagem para que ela também suporte diferentes tipos.

Para atingir esse nível de generalidade foi criada uma interface chamada `PixelInterface`. Sua principal funcionalidade é a da generalização das operações de um pixel. As operações que são definidas pela interface `PixelInterface` podem ser vistas na Figura 17.

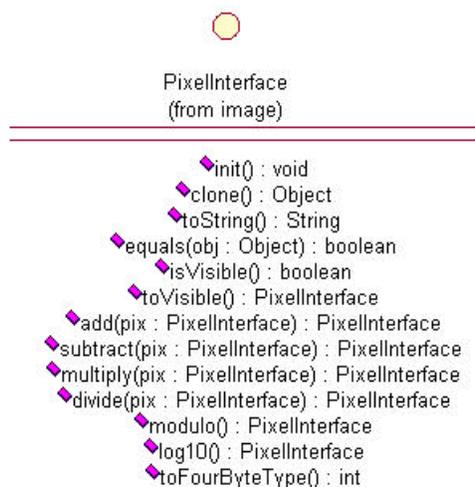


Figura 17: Operações da interface `PixelInterface`.

Nessa interface podem ser definidos dois grupos de operações: as gerais e as matemáticas. As operações gerais tratam do objeto em si, como as operações `init`, `toString`, `equals`, `isVisible`, `toVisible` e `toFourByteType`. Por outro lado, as operações matemáticas fazem operações matemáticas no valor do pixel, como as operações `modulo` e `log10`, ou fazem operações matemáticas entre os valores do pixel referido com outro pixel, como as operações `add`, `subtract`, `multiply` e `divide`.

Uma vez definida essa interface, é importante definir outra interface, referente à generalização da imagem. Essa interface foi chamada de `ImageInterface` e pode ser vista na Figura 18.

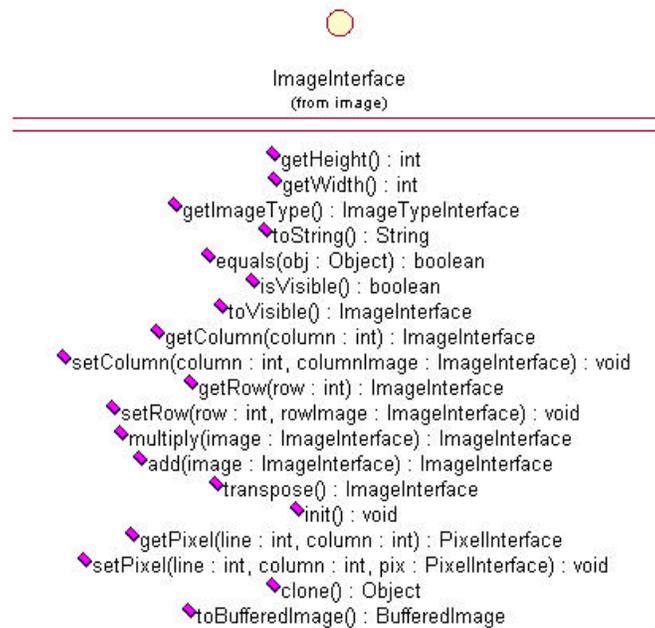


Figura 18: Operações da interface `ImageInterface`.

Da mesma forma que a interface `PixelInterface`, algumas operações dessa interface implementam operações entre imagens. Esse é o caso das operações `multiply` e `add`. A operação `transpose` retorna a imagem transposta da imagem em questão. Além disso, pode-se observar que operações como `getPixel`, `setPixel`, `getColumn`, `setColumn`, `getRow` e `setRow` permitem o acesso e manipulação de partes da imagem, sejam elas linhas, colunas ou até mesmo um pixel específico.

Outras operações dessa interface são semelhantes às da interface `PixelInterface` e não serão explicadas. Entretanto, a operação `getImageType` merece uma atenção especial. Essa operação existe devido à importância de se saber com que tipo de imagem está sendo trabalhado. Apesar das interfaces `PixelInterface` e `ImageInterface` já possibilitarem a criação de diferentes imagens com diferentes contradomínios, é importante saber distinguir uma imagem de um certo tipo de outra imagem de outro tipo. Para tal, é definido a interface `ImageTypeInterface`, como apresentado na Figura 19.

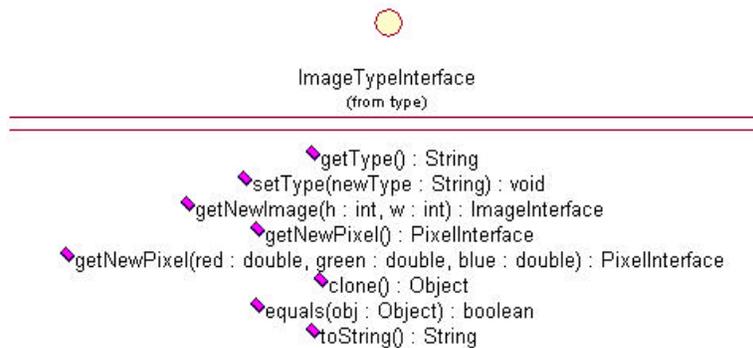


Figura 19: Operações da interface `ImageTypeInterface`.

Além das operações gerais dessa interface (como as operações `clone`, `equals`, `toString`), as operações `getType` e `setType` permitem o acesso e manipulação do tipo em questão. Além disso, as operações `getNewImage` e `getNewPixel` permitem a criação de novas imagens e pixels baseadas no tipo da imagem.

Uma vez criadas essas três principais interfaces, observa-se a necessidade de criação de duas classes abstratas, chamadas `Image` e `ImageType`. Essa necessidade é constatada pelos seguintes motivos:

- Em primeiro lugar, os atributos da imagem ainda não foram especificados, atributos esses como a matriz de `PixelInterface` e o tipo da imagem;
- Outro fator importante é que muitas operações das interfaces `ImageInterface` e `ImageTypeInterface` não precisam ser realmente implementadas para todas as classes que as implementam. Dessa forma, as classes abstratas `Image` e `ImageType` implementam essas

operações e deixam o que for essencial para as classes seguintes. Por exemplo, o método `getColumn` é o mesmo para todos os formatos de imagem.

As classes abstratas mencionadas acima podem ser vistas na Figura 20.

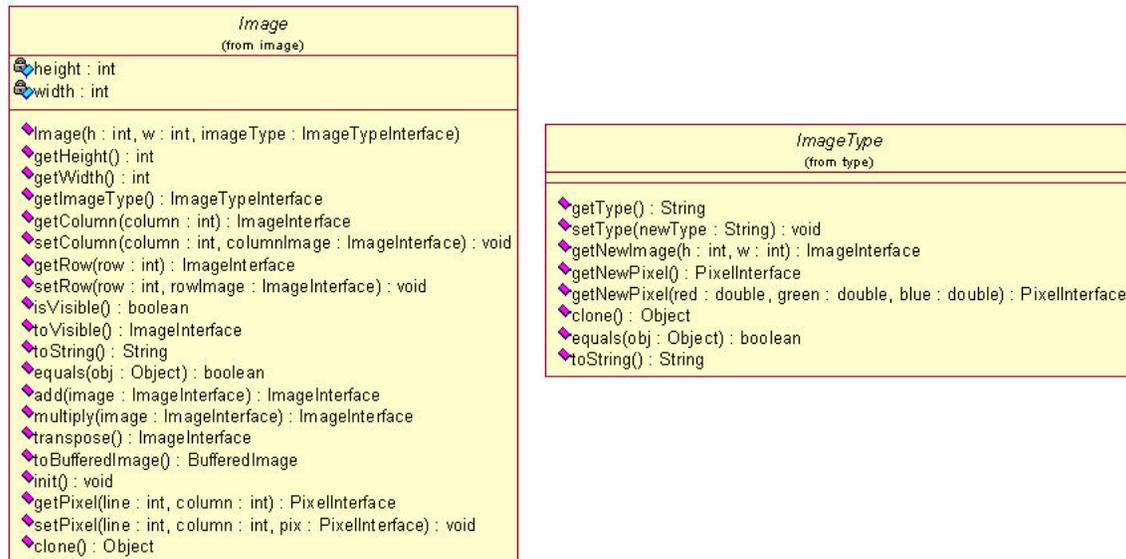


Figura 20: Classes abstratas *Image* e *ImageType*.

Dessa forma, fica completa a parte da arquitetura referente à imagem. Entretanto, é importante observar um caso de uso da utilização dessa imagem para a criação de um formato de imagem. Como caso de uso, será definida uma imagem em tons de cinza. Para tal, é importante observar que, apesar de ser necessária a criação de três novas classes, a relação entre essas novas classes com as aqui apresentadas diminui bastante o número de métodos que o desenvolvedor terá que implementar.

Como exemplo, para a criação de um novo formato de imagem em tons de cinza é necessária a implementação de três classes: *GrayscalePixel*, *GrayscaleImage* e *GrayscaleImageType*. Cada uma dessas classes deve implementar suas interfaces, ou seja, as interfaces *PixelInterface*, *ImageInterface* e *ImageTypeInterface*, respectivamente. Além disso, as classes *GrayscaleImage* e *GrayscaleImageType* devem herdar os atributos e métodos já implementados das classes abstratas *Image* e *ImageType*.

Como exemplo final da estensibilidade dessa parte da arquitetura, pode-se observar na Figura 21 as relações não apenas entre as interfaces e classes abstratas, mas também entre as

novas classes, de um formato de imagem criado pelo desenvolvedor. Nessa figura foram ocultadas as assinaturas dos métodos das classes já vistas, deixando apenas as assinaturas dos métodos das novas classes.

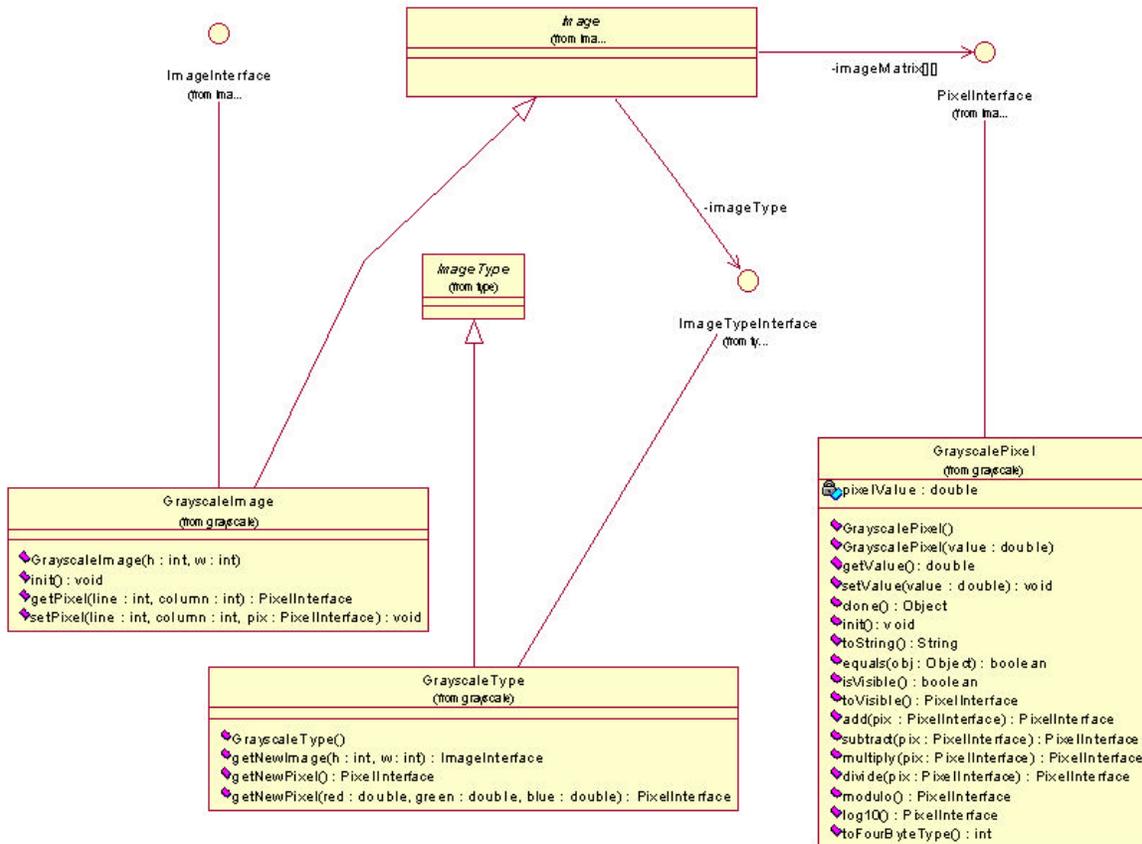


Figura 21: Estudo de caso da modelagem do formato de imagem tons de cinza.

6.2. MODELAGEM DO ACESSO À IMAGEM

Uma vez feita a modelagem da imagem, é importante fazer a modelagem do acesso aos dados contidos no arquivo da imagem. A idéia é criar uma arquitetura, consistente com a apresentada anteriormente, mas que possibilite a leitura de diferentes formatos de imagens de forma transparente para o desenvolvedor. Outro requisito adicional é o acesso da imagem no formato desejado, ou seja, no caso da leitura, deve ser passado o tipo da imagem (ImageTypeInterface) e deve ser retornada a imagem (ImageInterface) no formato especificado.

Para tal, observou-se a necessidade de um padrão de projeto (*design pattern*) conhecido como *Composite* [Gamma, 1995]. Com a utilização desse padrão, cada leitor/gravador de imagem é criado de maneira independente para cada formato, ou seja, um leitor é feito para imagens do tipo BMP (*Windows Bitmap File*), outro leitor é criado para imagens do tipo JPEG [Wallace, 1991] e assim sucessivamente. Em seguida é criada uma classe *composite* que acessa o arquivo solicitado e repassa o seu conteúdo para cada uma dessas classes. Cada classe identifica (pela extensão) se é ela que trata daquele tipo de arquivo e, caso positivo, assim o faz; caso negativo, repassa o arquivo para outro leitor.

Dessa forma, a utilização desse padrão na leitura e gravação de imagens em arquivos permite a criação e adaptação iterativa e incremental da plataforma conforme o *framework* vai sendo construído e estendido. A modelagem detalhada dessa parte da arquitetura pode ser vista na Figura 22, onde se observa a criação de um par leitor/gravador como exemplo de uso (nesse caso, o leitor/gravador de arquivos BMP).

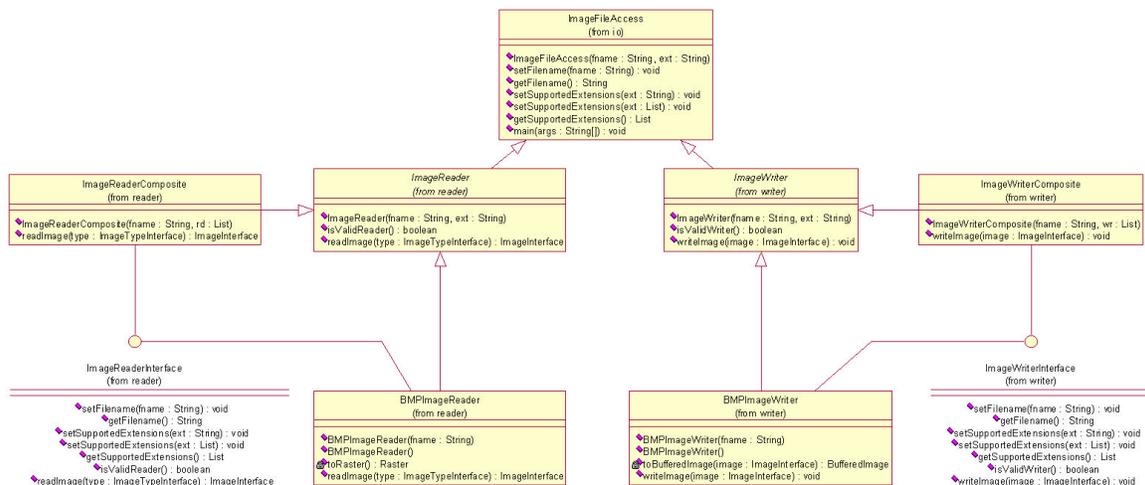


Figura 22: Modelagem do acesso a arquivos de imagens.

6.3. MODELAGEM DO MASCARAMENTO DE INFORMAÇÕES

Uma vez criada a parte da arquitetura que trata da manipulação de imagens, observa-se a necessidade da modelagem das operações que implementam o mascaramento de informações. Para tal as informações de entrada e saída das técnicas, explicadas na seção 3.2.5.4, são de fundamental importância para uma modelagem consistente com a realidade das aplicações de mascaramento de informações.

Entretanto, observa-se que dois objetos de fundamental importância ainda não foram modelados: chave e mensagem (ou marca). Uma chave pode ser considerada como um *array* de bytes que, de alguma forma (dependente do algoritmo utilizado), gerenciam o processo de inserção/ extração/ detecção da mensagem na imagem. Uma mensagem também é considerada como um *array* de bytes. As modelagens desses dois objetos podem ser vistas na Figura 23.

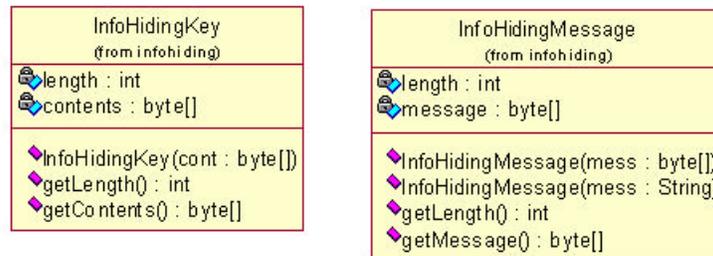


Figura 23: Classes InfoHidingKey (chave) e InfoHidingMessage (mensagem).

Como dito anteriormente, a modelagem do mascaramento de informações para imagens se baseia nas entradas e saídas descritas na seção 3.2.5.4. Dessa forma, é importante observar que o escopo da função de inserção da imagem é o mesmo para diferentes tipos de mascaramento de informações.

Nesse sentido, é definida a classe abstrata `InfoHiding`. Essa classe implementa dois métodos de acesso e manipulação do nome da técnica de mascaramento de informações (`getInfoHidingName` e `setInfoHidingName`). Além disso, essa classe define a assinatura do método abstrato `hide`, regido pela estego-chave, responsável por esconder uma informação em uma imagem guardada produzindo, assim, uma estego-imagem.

Além disso, foi definida para cada tipo de mascaramento de informações uma interface que, por sua vez, define a assinatura do método `unhide`. Dessa forma, durante o processo de criação de uma nova técnica de mascaramento de informações, o desenvolvedor deve criar uma classe que herda da classe `InfoHiding` (implementando assim o método `hide`) e implementar uma (ou mais) interface(s), fazendo com que o(s) método(s) `unhide` seja(m) implementado(s).

É importante observar que a arquitetura descrita acima possibilita a implementação de diferentes tipos de mascaramento de informações. Uma mesma técnica pode implementar mais de uma interface e, dessa forma, ter diferentes assinaturas para o método `unhide`. Tal

funcionalidade se torna um requisito desejável uma vez que possibilita que desenvolvedores criem técnicas de mascaramento de informações e as adaptem para diferentes aplicações.

A Figura 24 apresenta a modelagem da arquitetura referente ao mascaramento de informações em imagens. Nessa, uma implementação foi sugerida como estudo de caso, sendo ela a inserção LSB (*Least Significant Bit*), técnica bastante conhecida na área. Para maiores informações sobre essa técnica, o leitor pode consultar [Katzenbeisser, 2000].



Figura 24: Modelagem das técnicas de mascaramento de informações.

Algumas observações devem ser feitas em relação à arquitetura apresentada acima. Em primeiro lugar, deve-se observar que a assinatura do método unhide da interface SemiPublicInfoHidingInterface não está consistente com a definição apresentada na seção 3.2.5.4. Entretanto, deve-se observar que, nas técnicas de marcação digital semi-pública, a chave é gerada a partir da imagem original (imagem guardada). Dessa forma, as entradas são realmente a imagem guardada e a estego-imagem e a saída é a mensagem (marca).

Uma segunda observação deve ser feita uma vez que não foi feita nenhuma menção na arquitetura exposta à marcação digital assimétrica. É importante deixar claro que em termos de entradas/saídas, a marcação digital assimétrica assemelha-se à marcação digital pública. A diferença existe uma vez que na marcação digital pública a estego-chave é a mesma, tanto para o processo de inserção como extração e, na marcação digital assimétrica, existem duas estego-chaves diferentes, uma para inserção e outra para extração. Entretanto, a marcação digital assimétrica tem como fundamento que o relacionamento entre essas duas chaves é dado pela

natureza do algoritmo, deixando assim a assinatura do método igual ao da marcação digital pública.

Logo, para a criação de uma técnica assimétrica, o desenvolvedor deve implementar a interface `PublicInfoHidingInterface`, mas na implementação do método `unhide` deve ser garantido que o mesmo irá retornar a mensagem (marca) caso seja passada a chave complementar, ou seja, a estego-chave de extração.

6.4. MODELAGEM DE COMPONENTES COMPLEMENTARES

Nessa seção serão apresentadas modelagens de componentes complementares à arquitetura já descrita. Apesar de também integrarem a arquitetura proposta, as classes aqui apresentadas fogem um pouco ao objetivo principal desse documento. Entretanto, para uma implementação real e operacional do sistema proposto, elas devem ser consideradas, não só por facilitar o desenvolvimento, mas também como possibilitadoras da expansão do *framework* de forma robusta.

6.4.1. EXCEÇÕES

Apesar de não apresentadas nas seções anteriores, uma grande quantidade de exceções deve ser criada para possibilitar a detecção (e tratamento) de possíveis erros. Exceções como `IllegalImageSizeException`, `ImageIndexOutOfBoundsException`, `InvalidImageException`, `InvalidImageOperationException` e `InvalidPixelException` devem ser lançadas e tratadas para diferentes erros referentes a imagens e pixels. Em particular, as exceções `InvalidImageException` e `InvalidPixelException` devem ser lançadas quando se tenta operar imagens (e pixels) de diferentes tipos.

Além disso, exceções como `ImageReaderException` e `ImageWriterException` devem ser levantadas (e tratadas) quando da ocorrência de qualquer erro possível na leitura e escrita de imagens.

Semelhantemente, erros referentes à aplicação de técnicas de mascaramento de informações devem levantar e tratar a exceção `InfoHidingException`.

Além disso, a criação de uma exceção chamada `NullPointerException`, responsável pelo tratamento de erros do tipo `NullPointerException`, pode facilitar a detecção de erros em potencial e o tratamento de alguns desses erros em tempo de execução.

6.4.2. *OBJECTFACTORY E NATIVEFACTORY*

Além das exceções, outras classes importantes para uma boa modelagem são as classes `ObjectFactory` e `NativeFactory`. Em ambos os casos, elas foram baseadas no padrão de projeto chamado *Factory* [Gamma, 1995], funcionando como fábricas ou servidores.

A classe `ObjectFactory` funciona como um servidor de objetos e seus métodos podem e devem ser acessíveis de qualquer parte do *framework*. Seus métodos `getNewMap`, `getNewSet` e `getNewList` permitem o acesso a novos objetos `Map`, `Set` e `List`, respectivamente. Além disso, como todas as criações desses objetos são feitas por chamadas aos métodos do `ObjectFactory`, as implementações dessas classes podem ser alteradas em todo o projeto apenas alterando as implementações dos métodos da classe `ObjectFactory`. Por exemplo, a implementação de `List` pode ser alterada em todo o projeto de `Vector` para `LinkedList` apenas alterando a implementação do método `getNewList`. Além disso, o `ObjectFactory` também pode atuar como servidor de novas imagens e pixels através de seus métodos `getNewImage` e `getNewPixel`.

A classe `NativeFactory` funciona como uma porta de acesso para implementações mais eficientes. Essa classe foi concebida na possibilidade da implementação ser feita na linguagem Java, que se pode demonstrar ineficiente para algumas técnicas de processamento de imagens. Dessa forma, essa classe permitiria a chamada de métodos nativos Java (*Java Native Interface* – JNI) [Stearns, 2003], normalmente implementados numa linguagem mais eficiente como C ou C++. Entretanto, a criação e utilização dessa classe podem impactar na perda de portabilidade do projeto, sendo assim responsabilidade do desenvolvedor utilizá-la ou não.

Além disso, observa-se que a classe `NativeFactory`, por ter acesso a métodos nativos, torna-se o local mais apropriado para chamadas a *benchmarks* já existentes para testes de robustez de técnicas de mascaramento de informações como, por exemplo, o `StirMark` [Petitcolas, 2001] e o `Checkmark` [Checkmark, 2003]. Assim, o desenvolvedor só precisa criar um método nativo de acesso ao *benchmark* específico e converter os valores de retorno para o *framework*.

As definições das classes `ObjectFactory` e `NativeFactory` podem ser vistas na Figura 25. Na classe `NativeFactory` foi implementado um método nativo que faz a multiplicação de duas imagens, operação bastante comum e computacionalmente cara no contexto de transformações de domínio. O método de acesso a *benchmarks* não é exibido nesta figura.

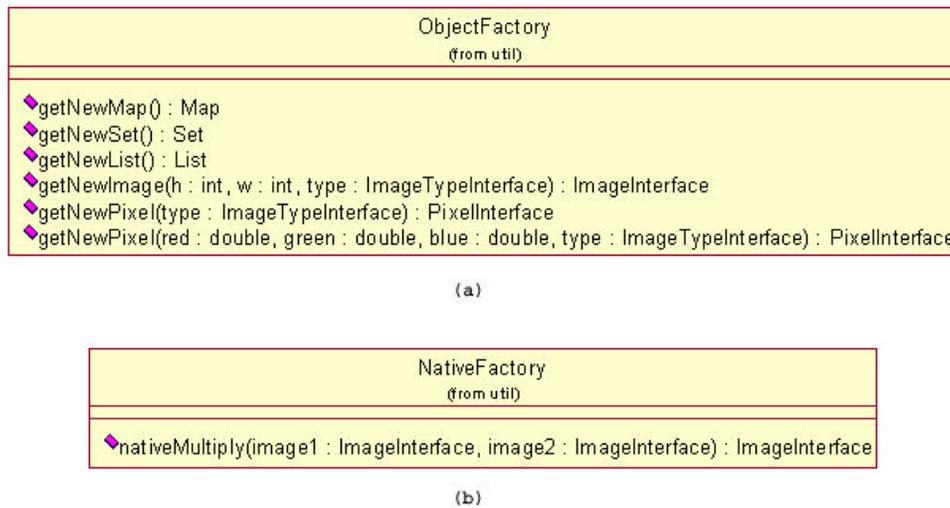


Figura 25: Classes `ObjectFactory` (a) e `NativeFactory` (b).

6.4.3. FACHADA E INTERFACE GRÁFICA (GUI)

Uma vez criada a arquitetura descrita acima, observa-se a necessidade da modelagem de uma fachada (ou conjunto de fachadas) que possam prover funcionalidades à interface gráfica (GUI - *Graphical User Interface*). Além disso, é importante não acoplar a fachada e a interface gráfica uma vez que diferentes interfaces gráficas podem ser desenvolvidas para uma mesma fachada (ou para um mesmo conjunto de fachadas).

Em primeiro lugar, observa-se a necessidade de um pequeno conjunto de fachadas, cada uma responsável por parte da arquitetura: uma para a manipulação de imagens, outra para a chamada de técnicas de mascaramento de informações, e assim sucessivamente para cada futura implementação de técnicas de processamento de imagens. É importante que essas fachadas sejam baseadas nos padrões de projeto *Facade* (possibilitando a centralização de funcionalidades e o acesso dessas pela GUI) e *Singleton* (fazendo que só exista uma única instância de cada fachada) [Gamma, 1995].

Em segundo lugar, através desse conjunto de fachadas, diferentes interfaces gráficas poderão ser construídas. Como primeira sugestão, a construção de uma interface gráfica ou janela para cada funcionalidade do *framework* aparenta ser a decisão mais intuitiva, mas esta deve ser verificada durante a prototipação do *framework*.

6.5. ARQUITETURA FINAL

A arquitetura final, principal objetivo desse trabalho, foi amplamente discutida e apresentada no decorrer desse capítulo. A Figura 26 apresenta a arquitetura completa, incluindo exceções, fábricas, fachadas e interfaces gráficas.

É importante fazer algumas discussões finais sobre a importância da arquitetura apresentada nesse capítulo, fazendo assim uma avaliação crítica deste trabalho.

Em primeiro lugar, pode-se observar a falta de relacionamentos fortes entre as partes principais do sistema. Essa característica é muito importante no projeto de sistemas uma vez que essa coesão e fraco acoplamento entre as classes permitem uma maior independência entre as mesmas, aumentando assim a modularidade do sistema.

Outro fator importante é a constante preocupação por parte da arquitetura em relação extensibilidade. A preocupação com esse requisito não-funcional forma a base das modelagens das imagens e do acesso a mesmas.

Um terceiro e último comentário surge com relação a modelagem do mascaramento de informações. A modelagem apresentada na seção 6.3 permite a construção fácil de diferentes técnicas de mascaramento de informações. Além disso, técnicas semelhantes podem ser facilmente trocadas devido ao uso das interfaces definidas na Figura 24. Outro fator, como mencionado na seção 6.3, é a capacidade de estender uma técnica de mascaramento de informações para diferentes tipos de aplicações, bastando para isso que a técnica implemente diferentes interfaces e, conseqüentemente, diferentes métodos `unhide`.

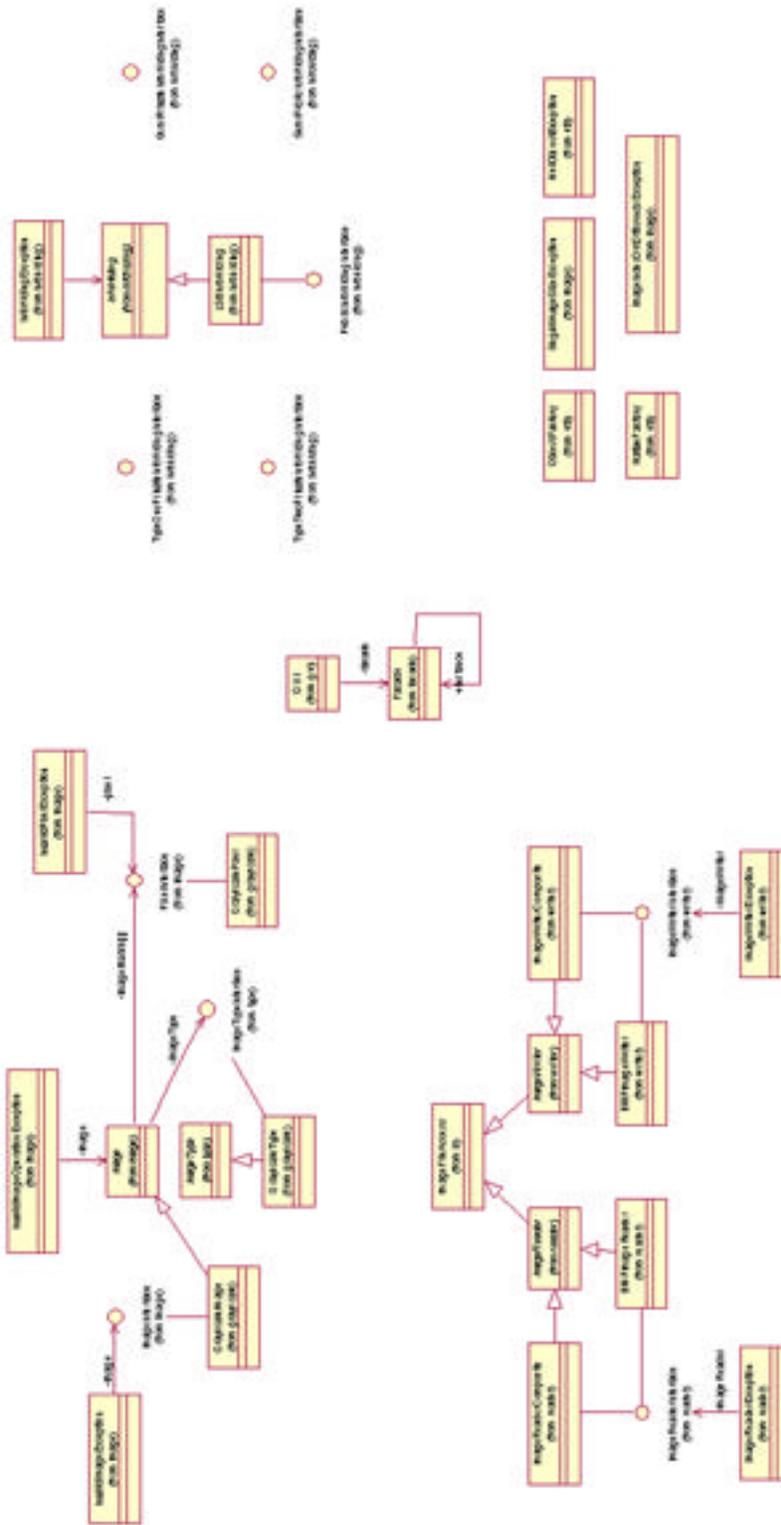


Figura 26: Arquitetura Final.

7. CONCLUSÕES E TRABALHOS FUTUROS

Second thoughts are ever wiser.

(Eurípides)

Esse capítulo apresenta os principais objetivos alcançados e as dificuldades encontradas no decorrer desse trabalho. Além disso, é feita uma discussão sobre possíveis trabalhos futuros referentes à arquitetura e possíveis linhas de pesquisa referentes à área de mascaramento de informações.

7.1. OBJETIVOS ALCANÇADOS

O desenvolvimento de uma arquitetura robusta e extensível apresentada no capítulo 6 deste documento pode ser considerado o principal objetivo alcançado no decorrer desse trabalho. A implementação de arquitetura proposta irá facilitar implementações futuras e permitir a criação de um “laboratório virtual” que irá permitir a criação e análise de novas técnicas de mascaramento de informações, propostas por qualquer pesquisador conectado a Internet.

O desenvolvimento do capítulo 2 pode ser considerado como o segundo objetivo alcançado. Na pesquisa para o desenvolvimento desse trabalho, aspectos históricos surgiram em vários artigos, mas quase todos de forma complementar. Esse capítulo relata uma revisão geral dos aspectos históricos da área de mascaramento de informações. Nesse contexto, tentou-se detalhar (em ordem cronológica) alguns exemplos históricos abrangendo as duas principais sub-áreas (marcação digital e esteganografia) e diferentes tipos de mídias (texto, imagem, música etc).

Um terceiro objetivo alcançado é o conhecimento apreendido durante o estudo e análise da área de mascaramento de informações. Tal aprendizado permitiu propor uma terminologia para a área na língua portuguesa, uma vez que não existe um consenso dos termos adotados nessa língua. Além disso, os conhecimentos adquiridos no decorrer desse trabalho também permitiram propor uma classificação das técnicas de mascaramento de informações mais abrangente do que as encontradas na literatura. A terminologia e classificação propostas foram amplamente discutidas e detalhadas no capítulo 3 desse trabalho.

Além disso, uma revisão geral dos principais requisitos e possíveis ataques referentes a técnicas de mascaramento de informações foi detalhadamente descrita no capítulo 5.

Um último objetivo alcançado foi a identificação de linhas de pesquisa na área de mascaramento de informações. Tais linhas são detalhadamente descritas na seção 7.4.

7.2. DIFICULDADES ENCONTRADAS

No decorrer do desenvolvimento da pesquisa e projeto, várias dificuldades foram encontradas.

Como primeiro exemplo, o acesso a aspectos históricos foi de grande dificuldade, uma vez que livros como [Schotti, 1665] e [Trithemius, 1500] são de difícil acesso e trato, uma vez que se encontram em latim. Além disso, o acesso ao artigo [Kerckhoffs, 1883] foi dificultado também pelo problema da língua, uma vez que o mesmo se encontra escrito em francês.

Outro problema referente ao acesso a informações históricas surgiu com a indisponibilidade eletrônica de alguns artigos, como por exemplo [Kobayashi, 1997]. Esse problema foi solucionado através do contato estabelecido com a autora do artigo, que gentilmente cedeu uma cópia do mesmo para fins acadêmicos.

Uma vez que essa ciência é bastante recente no contexto digital, a falta de conceitos padronizados dificultou bastante o aprendizado dos mesmos. Entretanto, essa mesma falta abriu as portas para as contribuições feitas nas seções Terminologia e Classificação do capítulo 3.

Um terceiro problema foi encontrado pelo autor no desenvolvimento desse documento: a falta de experiência em escrever um documento de qualidade e com notações matemáticas dificultou bastante o desenvolvimento desse trabalho. Essa dificuldade foi parcialmente superada através de consultas à coleção sobre normas [UFPR, 2000].

7.3. TRABALHOS FUTUROS

Ao término do planejamento da arquitetura para aplicações de mascaramento de informações observa-se que ainda há muito a ser feito.

Em primeiro lugar, implementações das principais técnicas de mascaramento de informações em imagens digitais formam uma das principais expansões do projeto. Além disso, é importante fazer também uma análise da viabilidade da modificação da arquitetura para uma arquitetura baseada em *provedores de implementações*, permitindo assim que uma mesma

técnica possa ser implementada por diferentes pessoas/ instituições deixando a critério do usuário final a escolha de que implementação usar. Uma descrição e exemplo desse tipo de arquitetura pode ser encontrada na *API Java Cryptography Architecture*, da Sun Microsystems [Microsystems, 2003].

Além disso, o leitor pode observar que a arquitetura aqui proposta visa apenas o desenvolvimento de aplicações de mascaramento de informações em imagens digitais, não abrangendo assim outras mídias importantes como texto, som digital e vídeo. Assim, como segunda possibilidade de trabalho futuro, o estudo de uma possível expansão dessa arquitetura para suportar tais mídias tornaria o *framework* mais abrangente. Para tal, API's como Java Media Framework [JMF, 2003] e JavaSound [JavaSound, 2003] e semelhantes para outras linguagens podem facilitar o processo de extensão do *framework* para diferentes mídias.

Finalmente, uma terceira expansão diz respeito aos ataques e requisitos, principalmente em relação à robustez. A modelagem genérica de um ataque de robustez permitiria que vários pesquisadores desenvolvessem diferentes ataques e testassem os mesmos em técnicas de mascaramento de informações, desenvolvidas ou não por eles.

7.4. LINHAS DE PESQUISA

Um dos objetivos alcançados durante o desenvolvimento desse trabalho foi a identificação de algumas linhas de pesquisa promissoras referente à área de mascaramento de informações.

Como primeira linha de pesquisa, podemos citar a análise mais detalhada do uso de transformações de domínio em aplicações de mascaramento de informações. Como citado em 3.2.4.2, o recente trabalho de Rankumar e outros [Rankumar, 2001] afirma que a capacidade de informações que podem ser atreladas a imagens no domínio transformado é superior à capacidade de informações que podem ser atreladas no domínio espacial sem que se cause uma perda perceptível da estego-imagem em relação à imagem guardada. Dessa forma, uma análise de que transformações de domínio (seno, cosseno, Fourier, Hadamard, Haar etc.) são mais adequadas a diferentes tipos de imagens (paisagens, *banners*, etc.) em aplicações de mascaramento de informações pode ajudar no desenvolvimento de novas técnicas mais robustas e seguras.

Uma segunda linha de pesquisa consiste em uma análise quantitativa da capacidade de armazenamento de informações em relação a cada transformação de domínio. Para tal,

métricas que consigam definir o grau de transparência perceptual devem ser estabelecidas a fim de estabelecermos análises *Capacidade de Armazenamento x Transparência Perceptual* para cada transformação e, assim, estabelecermos que transformação é mais adequada para cada tipo de aplicação de mascaramento de informações.

Uma terceira linha de pesquisa surge a partir da anterior. Para que o estudo da relação descrita acima seja feito, deve-se anteriormente fazer um estudo detalhado das métricas estatísticas e não-estatísticas que melhor descrevam a transparência perceptual em aplicações de mascaramento de informações aplicado a imagens digitais. Métricas como Erro Quadrático Médio, Relação Sinal/ Ruído e Similaridade de Histograma, entre outras, são utilizadas para medir quão diferentes são a imagem guardada e a estego-imagem [Eskiciouglu, 1995].

Uma quarta e última linha de pesquisa diz respeito a uma avaliação da fidelidade com que as métricas descritas acima refletem a invisibilidade das mensagens escondidas. Outro tópico a ser tratado é a proposta de novas métricas que capturem de forma mais adequada os aspectos perceptuais (subjetivos) da análise que os indivíduos fazem das imagens exibidas. Neste sentido, melhores métricas e testes poderão quantificar de forma mais adequada o conceito de invisibilidade (transparência perceptual), permitindo que novas e mais robustas técnicas de mascaramento de informações possam ser desenvolvidas.

As duas primeiras linhas de pesquisa estão sendo desenvolvidas pelo autor e orientador.

REFERÊNCIAS BIBLIOGRÁFICAS

- [Adobe, 2003] Adobe Systems Incorporated. “Adobe Photoshop 7.0”. Editor de imagens digitais, 2003.
- [Aeneas, 1997] Aeneas, T. “Aineias the Tactician: How to Survive Under Siege (Clarendon Ancient History Series)”. Clarendon Pr, 1997.
- [Anderson, 1998] Anderson, R. J. & Petitcolas, F. A. P. “On the limits of steganography”. IEEE Journal of Selected Area in Communications, (16-4):474-481, 1998.
- [Bach, 2001] Bach, J. S. “Morimur”. The Hilliard Ensemble & Christoph Poppen, ECM New Records. 1 CD (61 min.): digital estéreo, 2001.
- [Bach, 2002] Bach, J. S. “ECM Records: Morimur”. Disponível em <http://www.ecmrecords.com/ecm/recordings/1765.html>. Consultado em 11 de janeiro de 2003.
- [Banon, 1998] Banon, G. J. F. “Formal introduction to digital image processing”. Disponível em <http://dpi.inpe.br/banon/1998/07.02.12.54>. Consultado em 3 de setembro de 2002.
- [Barán, 2001] Barán, B.; Gómez, S. & Bogarín, V. “Steganographic watermarking for documents”. Proceedings of the 34th Hawaii international conference on system sciences, 2001.
- [Bender, 1996] Bender, W.; Grukl, D.; Marimoto, N. & Lu, A. “Techniques for data hiding”. IBM Systems Journal, (35):313-336, 1996.
- [Booch, 1998] Booch, G.; Jacobson, I.; Rumbaugh, J. & Rumbaugh, J. “The Unified Modeling Language User Guide”. 1st edition, Addison-Wesley, 1998.
- [Boutell, 2003] Boutell, T. “PNG (Portable Network Graphics) Specification”. Disponível em <http://www.w3.org/TR/REC-png/>. Consultado em 31 de janeiro de 2003.

- [Castor, 2001] Castor, F.; Cravo, M. & Frery, A. C. “JDIPF: Java Digital Image Processing Framework”. Proceedings of the XIV Brazilian Symposium on Computer Graphics and Image Processing, 401, 2001.
- [Checkmark, 2003] Checkmark. “Checkmark Benchmarking”. Disponível em <http://watermarking.unige.ch/Checkmark/>. Consultado em 31 de janeiro de 2003.
- [Compuserve, 2003] Compuserve Incorporated. “Graphics Interchange Format version 89a Specification”. Disponível em <http://www.dcs.ed.ac.uk/home/mxr/gfx/2d/GIF89a.txt>. Consultado em 31 de janeiro de 2003.
- [Corbis, 2002] Corbis. “Corbis – Stock photography and pictures”. Disponível em <http://www.corbis.com/>. Consultado em 18 de novembro de 2002.
- [Cox, 2000] Cox, I. J.; Miller, M. L. & Bloom, A. E. “Watermarking applications and their properties”. Proceedings of the International Conference on Information Technology: Coding and Computing, 6-10, 2000.
- [Craver, 1997] Craver, S.; Memon, N.; Yeo, B.-L. & Yeung, M “Can invisible watermarks resolve rightful ownerships?”. Proceedings of SPIE – Electronic Imaging – Storage and Retrieval of Image and Video Databases, 310-321, 1997.
- [Craver, 1998] Craver, S.; Yeo, B.-L. & Yeung, M “Technical trials and legal tribulations”. Communications of ACM, (41-7) 45-54, 1998.
- [Davern, 1995] Davern P. & Scott, M. “Steganography: its history and its application to computer based data files”. Internal Report of School of Computer Applications, Dublin City University, Dublin, Ireland, 1995.
- [Eskicioglu, 1995] Eskicioglu, A. M. & Fisher, P. S. “Image quality measures and their performance”. IEEE Transactions on Communications, (43-12) 2959-2965, 1995.

- [Fridrich, 1998] Fridrich, J. “Applications of data hiding in digital images”. Tutorial for the international symposium on intelligent signal processing and communication systems, 1998.
- [Gamma, 1995] Gamma, E.; Helm, R.; Johnson, R. & Vlissides, J. “Design Patterns: Elements of Reusable Object-Oriented Software”. Addison-Wesley, 1995.
- [Google, 2002] Google. “Google”. Disponível em <http://www.google.com/>. Consultado em 18 de dezembro de 2002.
- [Hartung, 1999] Hartung, F. & Kutter, M. “Multimedia watermarking techniques”. Proceedings of the IEEE, 1079-1107, 1999.
- [Herodotus, 1972] Herodotus. “The Histories (trans. A. de Selincourt)”. Reprint edition. Penguin, Middlesex, England, 1972.
- [Homero, 2002] Homero. “Ilíada de Homero (trans. H de Campos)”. Mandarim, São Paulo, Brasil, 2002.
- [Jain, 1988] Jain, A.K. “Fundamentals of digital image processing”. Prentice Hall, Englewood Cliffs, NJ, 1988.
- [JavaSound, 2003] Java Sound. “Java Sound API Home Page”. Disponível em <http://java.sun.com/products/java-media/sound/>. Consultado em 25 de janeiro de 2003.
- [JMF, 2003] Java Media Framework. “JMF Home Page”. Disponível em <http://java.sun.com/products/java-media/jmf/>. Consultado em 25 de janeiro de 2003.
- [Kahn, 1996] Kahn, D. “The codebreakers: the story of secret writing”. Scribner, New York, NY, 1996.
- [Katzenbeisser, 2000] Katzenbeisser, S. & Petitcolas, F. A. P. “Information Hiding – Techniques for steganography and digital watermarking”. Artech House, 2000.

- [Kazaa, 2002] Kazaa. “Kazaa Media Desktop”. Aplicação P2P (*Peer-to-Peer*). Disponível para download em [http:// www.kazaa.com](http://www.kazaa.com). Consultado em 18 de novembro de 2002.
- [Kerckhoffs, 1883] Kerckhoffs, A “La Cryptographie Militaire”. Journal des Sciences Militaires, vol. 9, 1883.
- [Kobayashi, 1997] Kobayashi, M. “Digital Watermarking: Historical Roots”. IBM Research Report, RT0199, 1997.
- [Kutter, 1999] Kutter, M. & Petitcolas, F. A. P. “A fair backmark for image watermarking systems”. Proceedings of Electronic Imaging, Security and Watermarking of Multimedia Contents, 226-239, 1999.
- [Kutter, 2001] Kutter, M. & Jordan, F. “Digital watermarking technology”. Disponível em [http:// www.alpvision.com/ watermarking.html](http://www.alpvision.com/watermarking.html). Consultado em 18 de novembro de 2002.
- [Lee, 2001] Lee, S.-J. & Jung, S.-H. “A survey of watermarking techniques applied to multimedia”. Proceedings of the IEEE international symposium on industrial electronics, 272-277, 2001.
- [Macromedia, 2002] Macromedia. “Macromedia Dreamweaver MX”. Ferramenta de desenvolvimento de websites, 2002.
- [Memom, 1998] Memom, N. & Wong, P. W. “Protecting digital media content”. Communications of ACM, (41-7) 35-43, 1998.
- [Microsystems, 2003] Microsystems, S. “Sun Microsystems Homepage”. Disponível em [http:// www.sun.com/](http://www.sun.com/). Consultado em 16 de janeiro de 2003.
- [Mintzer, 1996] Mintzer, F. C.; Boyle, L. E.; Cazes, A. N.; Christian, B. S.; Cox, S. C.; Giordano, F. P.; Gladney, H. M.; Lee, J. C.; Kelmanson, M. L.; Lirani, A. C.; Magerlein, K. A.; Pavani, A. M. B. & Schiattarella, F. “Toward on-line, worldwide access to Vatican Library materials”. IBM Journal of Research and Development, vol. 40, n. 2, 1996.

- [Mintzer, 1998] Mintzer, F.; Braudaway, G. W. & Bell, A. E. “Opportunities for watermarking standards”. *Communications of ACM*, (41-7) 57-64, 1998.
- [Morpheus, 2002] Morpheus. “Morpheus”. Aplicação P2P (*Peer-to-Peer*). Disponível para download em <http://www.musiccity.com>. Consultado em 18 de novembro de 2002.
- [Neobyte, 2002] Neobyte Solutions. “Invisible Secrets 2002”. Ferramenta de segurança de informações. Disponível para download em <http://www.neobytesolutions.com/invsecur/>. Consultado em 22 de dezembro de 2002.
- [Optimark, 2003] Optimark. “Optimark Benchmarking”. Disponível em <http://poseidon.csd.auth.gr/optimark/>. Consultado em 10 de janeiro de 2003.
- [Park, 2001] Park, H. “Visible watermarking using verifiable digital seal image”. Master’s thesis, School of Engineering – Information and Communication University, 2001.
- [Petitcolas, 1998] Petitcolas, F. A. P.; Anderson, R. J. & Kuhn, M. G. “Attacks on copyright marking systems”. *Second Workshop on Information Hiding*, 218-238, 1998.
- [Petitcolas, 1999] Petitcolas, F. A. P.; Anderson, R. J. & Kuhn, M. “Information hiding: a survey”. *Proceedings of the IEEE*, (87) 1062-1078, 1999.
- [Petitcolas, 2001] Petitcolas, F. A. P.; Stainebach, M.; Raynal, F.; Dittman, J. & Fàtes, N. “A public automated web-based evaluation service for watermarking schemes: StirMark benchmark”. *Proceedings of Electronic Imaging 2001, Security and Watermarking of Multimedia Contents*, 2001.
- [Petitcolas, 2002] Petitcolas, F. A. P. “Fabien A. P. Petitcolas steganography and watermarking homepage”. Disponível em <http://www.cl.cam.ac.uk/~fapp2/>. Consultado em 30 de novembro de 2002.

- [Pfitzmann, 1996] Pfitzmann, B., “Information hiding terminology”. Information hiding: First international workshop, 347-350, 1996.
- [Rankumar, 2001] Rankumar, M. & Akansu, A. N., “Capacity estimates for data hiding in compressed images”. IEEE Transactions on Image Processing, (10-8):1252-1263, 2001.
- [Rudin, 1990] Rudin, B., “Making paper: a look into the history of an ancient craft”. The Lyons Press, 1990.
- [Schneier, 1996] Schneier, B. “Applied cryptography – protocols, algorithms and source code in C”. 2nd edition, John Wiley & Sons, 1996.
- [Schotti, 1665] Schotti, G. “Schola Steganographica: In classes octo distributa”. Whipple collection ed., 1665.
- [Stearns, 2003] Stearns, B. “Java Native Interface”. Disponível em <http://java.sun.com/docs/books/tutorial/native1.1/>. Consultado em 27 de janeiro de 2003.
- [Steganos, 2003] Steganos. “Steganos Security Suite”. Ferramenta de segurança de sistemas. Disponível para download em <http://www.steganos.com/en/>. Consultado em 31 de janeiro de 2003.
- [Swanson, 1998] Swanson, M.; Kobayashi, M. & Tewfik, A. “Multimedia data-embedding and watermarking technologies”. Proceedings of the IEEE, 1064-1087, 1998.
- [Trithemius, 1500] Trithemius, J. “Steganographia”. Disponível em <http://www.esotericarchives.com/tritheim/stegano.htm>. Consultado em 18 de novembro de 2002.
- [UFPR, 2000] Universidade Federal do Paraná, Sistemas de Bibliotecas, “Normas para Apresentação de Documentos Científicos”. Editora da UFPR, 2000.
- [Wallace, 1991] Wallace, G. K. “The JPEG still picture compression standard”. Communications of the ACM, 1991.

ANEXO A

Nessa seção estão apresentados alguns trechos referentes a *Ilíada* [Homero, 2002], primeira referência do uso de esteganografia. O Trecho 3 conta a história de Belerofonte, que resiste aos encantos da rainha Antéia e é enviado ao rei de Lícia com uma mensagem que contava as intenções do rei Próito.

*“...Próito,
porém, maquinou contra ele coisas malignas.
Escorraçou-o de Argos: tinha mais poder,
rei por graça de Zeus; Antéia, diva e rainha,
num arroubo de amor, secretamente quis
entregar-se a ele. Não seduziu ao prudente
Belerofonte, mente limpa! Antéia ao rei
mentiu: «Ou matas quem me quis tomar à força,
ou, ao invés, será melhor que morras», disse
e o rei se enraiveceu, mas lhe faltou coragem
para matá-lo. A Lícia o manda, com mensagem
que grafara – funestos signos – em tabuinhas
fechadas, para o sogro (os sinais insinuavam
que fosse executado).”*

Trecho 3: Belerofonte, por recusar a rainha, é enviado ao rei de Lícia com uma mensagem que, secretamente, insinuava que ele fosse executado. Fonte: [Homero, 2002].

Ao chegar, Belerofonte foi bem recebido. Passados dez dias, o rei ordena que Belerofonte compareça a sua presença para entregar a mensagem do rei Próito. Ao observar a mensagem com as instruções fatais, o rei de Lícia ordenou que Belerofonte matasse a Quimera – “um monstro selvagem”. Em seguida, Belerofonte tinha que lutar contra a gloriosa tribo de Sólimos. Finalmente, ele teve que lutar contra as Amazonas, mas o grande Belerofonte conseguiu vencer todos os desafios. Achando que Belerofonte estava sob proteção divina, o rei de Lícia deu a ele a mão de sua filha e metade do seu reino: O trecho de *Ilíada* [Homero, 2002] referente às tarefas designadas a Belerofonte pode ser visto no Trecho 4.

*“...Quando, porém, no dia décimo, despontava
a Aurora, dedos-rosa, no horizonte, o rei
indaga-lhe dos signos que, por meio deles,
o genro, Próito, certo lhe mandara. Logo
que examinou os fúnebres sinais, o rei
ordenou-lhe matar a Quimera imbatível,
de inumana, divina estirpe: cara, leão;
rabo, serpente; dorso caprino, resfolgo
hórrido, de furor e fogo. O herói matou-a,
confiado nos acenos celestes. Depois
tocou-lhe combater os afamados Sólimos,
seu mais terrível prélio, ele mesmo o dizia.
Vencer as Amazonas: o terceiro encargo.
Cumpriu-o. Ao retornar, um arдил o esperava;
dentre os Lícios, o rei, escolhendo os melhores,
armou-lhe uma emboscada: à casa, nenhum deles
voltou. Belerofonte, imáculo, destruiu-os.
Reconhecendo a estirpe divina do herói,
o rei o conseguiu reter e deu-lhe a filha
por esposa e a metade dos poderes régios.”*

Trecho 4: O rei de Lícia recebe a mensagem secreta e é enviado para as missões. Fonte: [Homero, 2002].

ANEXO B

Nessa seção estão apresentados trechos de mensagens inseridas nas seis peças para solo de violino de Bach, comprovados pela professora Helga Thoene [Bach, 2001], da Universidade de Düsseldorf. Segundo Helga Thoene, essa obra se encontra repleta de menções à morte e indicações para interpretá-la não como solo de violino senão com acompanhamento de corais.

O Trecho 5 apresenta um exemplo de mensagem escondida nessa obra. Para maiores informações o leitor pode consultar [Bach, 2001] e [Bach, 2002].

*“The death no one could subdue
Amongst all mankind’s children;
This was all caused by our sin,
No innocence was found then.
From this came, then, death so quick
And seized power over us,
Held us in his realm as captives.
Halleluja!”*

...

*“Christ lay in death’s bondage;
For all our sin was given;
He is once more arisen
And hath us brought true life now;
For this shall we joyful be,
To God giving praise and gratitude,
And singing Halleluja
Halleluja!”*

Trecho 5: Mensagem inserida na obra de Bach. Fonte: [Bach, 2001].