UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL
INSTITUTO DE INFORMÁTICA
CURSO DE CIÊNCIA DA COMPUTAÇÃO

SÍLTON LEONARDO PAIVA NUNES

Marca D'Água Digital
Autenticação de Imagens Digitais

Trabalho de Graduação.

Prof. Newton Braga Rosa
Orientador

Porto Alegre, novembro de 2008.

AGRADECIMENTOS

Em memória de Ash (1998-2002).

SUMÁRIO

LISTA DE SÍMBOLOS E SIGLAS

C_{Pr}	Chave Privada
C_{Pu}	Chave Pública
C_S	Chave Secreta
D	Documento Original
DCT	Discrete Cosine Transform (Transformada Discreta do Cosseno)
D_M	Documento Marcado
D_{MI}	Documento Marcado com Marca D'água Invertida
I	Imagem Original
I_F	Falsa Imagem Original
I_M	Imagem Marcada
JPEG	Joint Photographic Experts Group
LSB	Least Significant Bits (Bits Menos Significativos)
M	Marca D'água
M_I	Marca D'água Invertida
MSB	Most Significant Bits (Bits Mais Significativos)
N	Número Inteiro Grande
S	Conjunto de Pixels
S_1	Metade do Conjunto S
S_2	Outra Metade do Conjunto S
SWICO	Single Watermarked Image Counterfeit Original
X	Valor de Incremento ou Decremento

LISTA DE FIGURAS

RESUMO

A disseminação de imagens digitais pela internet criou novos desafios relacionados à autoria e integridade dos documentos transacionados. Um documento de texto submetido à criptografia ou certificação digital fica protegido contra qualquer alteração, por menor que ela seja. Ao contrário, uma imagem deve ser considerada autêntica mesmo que o seu código tenha sofrido alguns tipos de alterações, desde que não mudem a essência da informação contida na imagem, como compressão (JPEG por exemplo), ajuste de brilho, de contraste, entre outros tratamentos usuais.

Neste contexto, uma das soluções para proteção de autoria e integridade de imagens digitais é o uso de marcas d'água digitais, as quais são conceitualmente semelhantes às marcas d'água usadas em documentos físicos, como o papel-moeda.

Este trabalho tem por objetivo fornecer ao leitor um guia simples sobre marcas d'água digitais, incluindo características e aplicabilidade de marcas d'água imperceptíveis em imagens digitais. Ao final, uma bateria de testes avalia a robustez de marcas d'água inseridas por um software líder de mercado (Photoshop e Digimarc) contra ataques maliciosos e tratamentos usuais.

Palavras-chave: Marca d'água digital, imagem, autenticação.

Digital Watermark Authentication of Digital Images

ABSTRACT

The spread of digital images throughout the Internet has created new challenges in regards to authorship and integrity of the exchanged documents. A text document submitted to criptography or digital certification is protected against any alteration, as little as it might be. On the other hand, an image must be considered authentic even if its code has been altered, as long as it does not change the essence of the information contained in the image, such as compression (JPEG for example), adjustment of brightness, contrast balance, among other usual treatments.

In this context, one of the solutions for the protection of authorship and integrity of digital images is the use of digital watermarks, which are conceptually similar to the ones used in concrete documents, such as money bills.

This paper aims at providing the reader a simple guide on watermark, including characteristics and applicability of imperceptible watermarks in digital images. In the end, tests will evaluate the robustness of watermarks embedded by the leading software available in the market (Photoshop and Digimarc) against malicious attacks and usual treatments.

Keywords: Digital watermark, image, authentication.

1 INTRODUÇÃO

Este trabalho tem por objetivo fornecer ao leitor um guia sucinto e simples sobre marcas d'água digitais, mais especificamente sobre o uso de marcas d'água imperceptíveis em imagens digitais. Ao final, é feita uma bateria de testes usando um software líder de mercado (Photoshop) com um módulo chamado Digimarc, que insere e lê marcas d'água. Estes testes procuram mostrar os limites de resistência da marca d'água à ataques na imagem protegida, bem como os limites de resistência a tratamentos usuais e necessários.

Ao longo da história, a humanidade criou sistemas de autenticação de documentos convencionais. Uma assinatura sobre um documento em papel pode assegurar autoria e integridade do conteúdo. Lacres em envelopes foram usados até o século passado com finalidade semelhante. Em vários momentos da história, as sociedades criaram várias formas de cartórios e tabelionatos, de fé pública, para garantir autoria e integridade de documentos convencionais.

Nos últimos anos, a internet disseminou o uso de documentos digitais, criando novos problemas relacionados à autoria e integridade. Cada vez mais, empresas e pessoas assumem compromissos importantes baseados em documentos digitais como e-mail, ordens de compra, ordens bancárias e contratos. Ao receber um desses documentos digitais, surgem perguntas e dúvidas cada vez mais pertinentes:

Quem enviou? (Autoria - quem envia é realmente quem diz ser?)
Alguém mais viu o documento? (Privacidade)
Foi isto mesmo que o remetente enviou? (Integridade)

A partir de 2001, o Brasil editou os primeiros marcos legais para uso de criptografia por chaves públicas, assinaturas eletrônicas, certificados digitais e uma gama de serviços visando dar segurança e validade jurídica aos documentos digitais. O ICP - Brasil é a Autoridade Certificadora Raiz que tem por missão licenciar, auditar e fiscalizar

as AC - Autoridades Certificadoras e AR - Autoridades de Registro no país.

No Estado do Rio Grande do Sul, a lei 12.469/2006 cria a Autoridade Certificadora, AC - RS, envolvendo a Procergs, Secretaria da Fazenda do RS, Tribunal de Justiça e Banrisul. Atualmente, existem no Brasil diversas AC oferecendo diferentes tipos de serviços, como a emissão de certificados digitais para pessoas físicas e jurídicas.

Com a internet, o alcance e a velocidade da disseminação de imagens digitais ganhou um impulso inimaginável. Junto, apareceram novos problemas. A confiança que se tinha numa foto ficou abalada na era digital. Programas para tratamento de imagem digital estão presentes até nos computadores domésticos. Neste contexto, surge a necessidade de autenticação de imagens digitais para garantir a sua autenticidade.

Entretanto, imagens digitais têm necessidades de segurança diferentes dos documentos protegidos por certificados digitais, como os emitidos pelas Autoridades Certificadoras.

Existe uma ampla gama de tratamento digital sobre imagens que, apesar das alterações no código do documento digital, ainda podem ser consideradas fiéis à informação básica que armazenam. Mudanças decorrentes de compactação (como o padrão JPEG) iriam dar um falso negativo (não-autêntica) se a imagem fosse submetida aos rígidos sistemas de autenticação dos documentos digitais bancários, por exemplo. Ou seja, em muitas aplicações com imagens, basta avaliar se o essencial da informação está preservado. Em caso positivo, a imagem digital não deve ser repudiada, apesar de ter sido alterada.

A marca d’água digital é solução na autenticação de imagens digitais para uma ampla gama de aplicações.

As marcas d’água podem ser seguras, robustas, semi-frágeis e frágeis, conforme seu grau de tolerância a alterações no documento original. As seguras e robustas resistem melhor ao tratamento necessário, não malicioso, da imagem do que as frágeis.

A marca d’água frágil não resiste (frágil portanto) a alterações mínimas da imagem, mesmo que seja um tratamento necessário como sua compressão em formato consagrado (JPEG por exemplo) para sua transmissão ou armazenamento.

Em resumo, uma marca d’água digital é um sinal, um código identificador, inserido num documento digital, que pode ser ostensivo, discreto ou imperceptível, conforme for o requisito da aplicação. Esse sinal, normalmente acessível apenas por pessoas autorizadas, serve para identificar o autor ou o detentor dos direitos autorais do documento (autoria), bem como se a informação sofreu algum tipo de alteração (integridade). Remetente e destinatário deverão compartilhar algumas informações de modo que o destinatário consiga fazer a verificação de autoria ou integridade do documento recebido.

2 MARCA D'ÁGUA DIGITAL

2.1 História da marca d'água

Na Europa, ao final do século XIII, aproximadamente 40 moinhos produziam papel de diferentes formatos, qualidade e preço. Entretanto, o papel produzido por estes moinhos era de má qualidade, inútil para a escrita e, por isso, ainda precisava ser tratado por artesãos. Os artesãos suavizavam a superfície do papel com a ajuda de uma pedra dura, chamada calandra, para torná-lo aceitável para a escrita. A seguir, o papel era polido e dividido em folhas por artesãos e só depois comercializado. Num certo momento, a quantidade de moinhos, artesãos e comerciantes era tão grande que não havia a possibilidade de garantir a origem ou a qualidade do papel comercializado [KAT 00].

Na cidade de Fabriano na Itália, em 1292, pela primeira vez um moinho começou a usar marca d'água em seu papel, para diferenciá-lo dos demais. As primeiras marcas d'água eram feitas através da adição de grades aos moldes de papel, tornando possível, pela primeira vez a detecção da origem. A marca d'água se espalhou rapidamente pela Itália, depois pela Europa, passando a identificar mais do que a origem ou o tipo do papel, como também sua qualidade e formato. Depois disso, a marca d'água começou a ser utilizada também na autenticação de documentos [FRE 07] [RUB 07] apud [COX 01].

As marcas d'água que os bancos usam no papel-moeda inspiraram o primeiro uso do termo "marca d'água" no contexto dos documentos digitais [KAT 00]. Apesar da semelhança entre marca d'água e marca d'água digital, a última só surgiu por volta de 1954, quando Emil Hembrooke, pertencente a Corporação Muzak, patenteou um trabalho musical. Para proteger a autoria da música, foi inserido um código de identificação, baseado no Código Morse. O código foi criado com a aplicação de um filtro de 1kHz na música, sendo que a presença ou a ausência de energia nessa freqüência indicava letras, semelhantemente ao Código Morse, que garantiam a autoria pretentida [RUB 07] apud [COX 01].

Komtsu e Tominaga usaram o termo marca d’água digital em 1988 [RUB 07] apud [KOM 88]. A idéia da marca d’água só passou a ser aplicada em imagens digitais a partir de 1990 [RUB 07] apud [JOH 93]. As primeiras publicações para uso de marca d’água em imagens digitais foram publicadas por Tanaka em 1990 e por Caronni e Tirkel em 1993 [KAT 00]. Na metade da década de 90, com o crescente uso de documentos digitais, surgiu o interesse pelas técnicas de marca d’água digital.

A internet, um dos principais fatores que causaram o aumento no uso de documentos digitais, também facilitou a publicação de trabalhos, agilizando a difusão deles [RUB 07] apud [BAR 04-a] [JOH 99] [KIM 01]. Proliferou também a difusão de cópias ilegais dos documentos, gerando problemas de direitos autorais e de autenticidade [RUB 07] apud [ZHU 96].Assim a marca d’água digital vem recebendo maior atenção, sendo um dos assuntos tratados em 1996, no primeiro Information Hiding Workshop. Depois disso, em 1999, o congresso International Society for Optical Engineering realizou uma conferência sobre segurança e marca d’água, chamada "Security and Watermark of Multimedia Contents" [AND 96] [DEL 00].

2.2 Princípios básicos da marca d’água digital

2.2.1 Necessidade da marca d’água digital

A revolução digital e a explosão das redes de comunicação levam ao aumento exponencial do tráfego de documentos digitais (imagens, textos, áudio e vídeo). Esse fenômeno moderno criou novos desafios para proteger e controlar a troca desses documentos, que podem ser facilmente duplicados, modificados e difundidos. Por isso, é tão importante desenvolver sistemas de proteção à direitos autorais e autenticação de conteúdo. A marca d’água digital é uma alternativa para diminuir o problema [PRO 97].

2.2.2 O que é marca d’água digital

O grande objetivo da marca d’água digital é incluir informação (ostensiva, discreta ou oculta, conforme a aplicação) no documento digital para fornecer algum serviço de segurança ou simplesmente para rotulá-lo. Alguns sistemas devem permitir recuperar a informação inserida no documento (a marca d’água) mesmo que ele tenha sido consideravelmente modificado por ataques, maliciosos ou não [REY 02].

Todas as marcas d'água digitais possuem alguns pontos em comum: elas possuem um sistema de inserção e um sistema de recuperação.

O sistema de inserção precisa receber como entrada o documento que será marcado (D), a marca d'água (M) e talvez uma chave secreta (C_S) ou uma chave privada (C_{Pr}). A saída do sistema de inserção é o documento marcado.

SistemaDeInserção (D, M, C_S ou C_{Pr}) ⇒ D_M

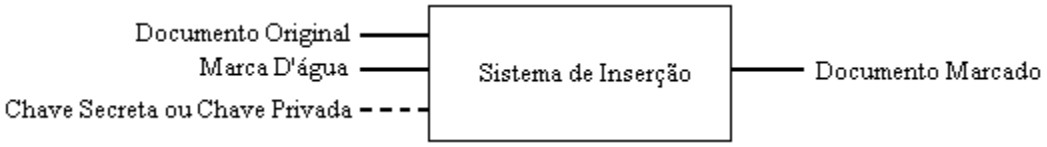

Figura 2.1: Sistema de inserção

O sistema de recuperação precisa receber como entrada o documento marcado (D_M), talvez a marca d'água (M), talvez o documento original (D) e talvez uma chave secreta (C_S) ou uma chave pública (C_{Pu}). A saída do sistema de recuperação pode ser a marca d'água ou uma decisão do tipo "sim" ou "não" que responde a pergunta: A marca d'água encontra-se no documento?

SistemaDeRecuperação (D_M, D, M, C_S ou C_{Pu}) ⇒ M, Sim ou Não

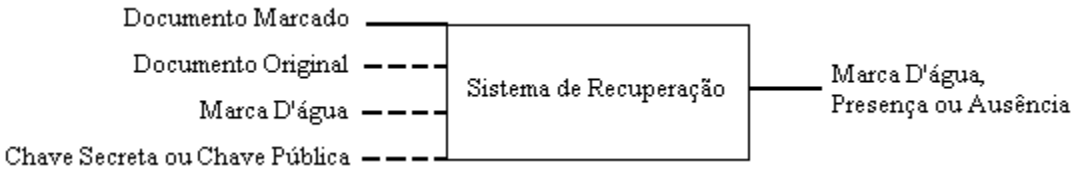

Figura 2.2: Sistema de recuperação

A marca d'água pode ser de qualquer natureza, tal como números, texto ou uma imagem. Generalizando, a informação inserida é um string binário.

A chave pode ser usada para reforçar segurança, prevenir que pessoas não autorizadas recuperem e manipulem a marca d'água. Na prática, todo sistema de marca d'água com utilidade comercial usa pelo menos uma chave ou até mesmo uma combinação de diversas chaves.

2.2.3 Comparação entre marca d'água digital e esteganografia

Esteganografia é uma palavra de origem grega que significa escrita escondida. É o ramo particular da criptografia que faz com que uma mensagem seja camuflada no documento transacionado.

Tanto marca d'água como esteganografia são técnicas usadas para esconder uma informação dentro de outra. As técnicas de esteganografia não costumam ser robustas contra modificações no documento, ou seja, modificações no documento, mesmo pequenas, talvez destruam a informação oculta. As técnicas de esteganografia seriam consideradas frágeis ou semi-frágeis, se analisadas pelos critérios das marcas d'água digitais. Uma implicação prática da exigência de robustez é que métodos de marca d'água robusta ou segura costumam inserir muito menos informação oculta do que métodos de esteganografia.

Marca d'água deve ser usada no lugar de esteganografia toda vez que o documento marcado for disponível para pessoas que sabem da existência de informação oculta e podem ter interesse em removê-la. Uma aplicação popular para marca d'água digital é dar provas de autoria de um documento, isso pode ser feito inserindo no documento declarações de direitos autorais. É óbvio que para esse tipo de aplicação a informação inserida precisa ser robusta contra manipulações que podem tentar removê-la do documento.

2.2.4 Marca d'água digital visível/perceptível

Marca d'água digital visível, como o nome diz, é um padrão visual, como um logotipo, que é inserido em um vídeo ou uma imagem digital da mesma forma que as marcas d'água visíveis em papel.

Figura 2.3: Exemplo de imagem com marca d’água visível (“Wizard of the Coast, all rights reserved”)

Figura 2.4: Exemplo de imagem com marca d’água visível (Logo da Globo)

Marcas d’água digitais visíveis são usadas principalmente em imagens difundidas, pela televisão ou internet por exemplo, como forma de inibir o seu uso comercial indevido. Também é possível marcar áudio desta forma, inserindo um som audível no meio de uma música. Por exemplo, um locutor anuncia uma mensagem comercial orientando como comprar o versão completa daquela música [KAT 00].

2.3 Múltiplas marcas d’água digitais

Algumas aplicações podem exigir que sejam inseridas várias marcas d’água digitais em um único documento. Por exemplo, uma imagem digital pode conter duas marcas d’água, uma para garantir os direitos do autor e outra para permitir que um cliente faça uso da imagem. Tal esquema precisa de um algoritmo mais sofisticado, pois é necessário um maior controle na inserção da segunda marca d’água, de modo que ambas possam ser recuperadas. A escolha deve ainda considerar a interferência de uma marca d’água na outra e o impacto na qualidade do documento original. Geralmente estas interferências são mais críticas quando se usa marcas d’água frágeis.

3 CARACTERÍSTICAS E CLASSIFICAÇÕES DAS MARCAS D'ÁGUA DIGITAIS

É importante analisar as características das marcas d'água digitais para que se atinja o objetivo desejado, seja ele proteção de direitos autorais ou autenticação de conteúdo. Ou seja, não basta apenas esconder informação no documento digital, é preciso entender como essa informação oculta vai fornecer o serviço desejado. Também é necessário estudar o impacto que o uso comum no documento causa na marca d'água digital, para escolher a marca d'água adequada.

Uma marca d'água digital aplicada numa imagem, com o objetivo de identificar o autor dela (proteger direitos autorais) precisa ser robusta. Caso contrário alguém poderia removê-la e em seguida inserir sua própria marca d'água no lugar. Entretanto, existem formas mais sutis de atacar esse sistema. Suponha que, ao invés de tentar remover a marca d'água que contém a identificação do autor, o atacante insira sua própria marca d'água na imagem. Mesmo que a marca d'água do atacante não apague a marca d'água do autor, a presença de ambas na imagem cria dúvidas sobre sua autoria.

Tornando o exemplo anterior mais específico, imagine que Ana marca uma imagem para identificar que é a autora. Após isso, ela torna a imagem marcada, que chamaremos de I_A, pública.

$$I_A = I + M_A$$

Para confundir as evidências que provam a autoria da imagem, Beto pega a imagem publicada por Ana e insere nela a sua própria marca d'água (M_B), criando uma imagem que possui duas marcas d'água (I_{AB}).

$$I_{AB} = I + M_A + M_B$$

Agora é impossível decidir se I_{AB} pertence a Ana ou a Beto, pois essa imagem possui ambas as marcas d'água. Para resolver essa ambiguidade, poderia ser exigido de Ana e Beto que eles mostrem uma cópia da imagem que contém apenas a sua própria marca d'água. Ana poderia satisfazer a exigência facilmente, pois ela é dona da imagem original, já Beto não seria capaz de satisfazer a exigência, pois todas as cópias da imagem que ele possui em mãos também estão marcadas pela marca d'água de Ana. Entretanto, esse fato não é suficiente para garantir os direitos autorais de Ana, pois existem ataques à marca d'água mais sutis, como o SWICO (Single Watermarked Image Counterfeit Original). Suponha que a marca d'água utilizada por Ana tenha um método de recuperação não-cego e que só possa ser detectada, ou seja, para revelar a presença da marca d'água um detector precisa comparar a imagem marcada com a imagem original. Então vamos supor também que a detecção da marca d'água se dá subtraindo a imagem original da imagem marcada. Ana pode usar a imagem original para provar que a imagem que Beto possui também tem a marca d'água dela.

$$I_{AB} - I = (I + M_A + M_B) - I = M_A + M_B$$

Ela também pode usar a imagem original para provar que ela tem cópias que não possuem a marca d'água de Beto.

$$I_A - I = (I + M_A) - I = M_A$$

As duas fórmulas anteriores provam que I_{AB} possui M_A (e também M_B) e que I_A possui apenas M_A.

O problema é que Beto pode fazer o mesmo, criando uma falsa imagem original (I_F) que será usada durante a verificação de autoria. Para criá-la, basta que a marca d'água de Beto seja invertível e que Beto subtraia ela de I_A, afirmando que essa é a imagem original.

$$I_F = I_A - M_B = I + M_A - M_B$$

Desta forma, Beto pode afirmar que ele possui uma imagem (a imagem tornada pública por Ana, I_A) que possui sua marca d'água e não possui a marca d'água de Ana.

$$I_A - I_F = (I + M_A) - (I + M_A - M_B) = M_B$$

Como visto acima, a simples adição de uma marca d'água digital com método de recuperação não-cego não garante autoria, mesmo que a marca d'água seja robusta o suficiente para não ser removida sem destruir o documento original [BAR 04-b].

3.1 Robustez nas marcas d'água digitais

A robustez de uma marca d'água digital é a sua capacidade de sobreviver à manipulações, maliciosas ou não.

Para tornar mais robusta uma marca d'água digital, a maneira mais comum é inserir a informação oculta em lugares mais significantes (da imagem ou do som, por exemplo), onde qualquer alteração é mais perceptível para os sentidos humanos. Por exemplo, se o documento original se trata de uma imagem digital, o melhor seria inserir a marca d'água em regiões de contraste, pois estas regiões são melhores percebidas pelo sistema visual humano e seria improvável que algum algoritmo de compressão com perda alterasse bruscamente esta região.

3.1.1 Marca d'água digital segura

Esse é o tipo mais robusto e demandado. Essas marcas d'água digitais são feitas para proteger direitos autorais e aplicações orientadas à segurança. Esse tipo de marca d'água digital precisa sobreviver a manipulações de vulto, sejam maliciosas ou não. Embora não seja impossível removê-las, o processo deve ser difícil. Caso a qualidade do documento recebido seja boa, a marca d'água segura deve ser passível de recuperação. Ou seja, admite-se a impossibilidade de recuperaçao somente no caso de grande degradação da qualidade.

Quem está atacando uma marca d'água segura provavelmente conhece o algoritmo usado para inserí-la e, assim, pode criar métodos para removê-la.

As marcas d’água seguras devem resistir a diversos tipos de tratamento, como ferramentas de processamento analógico ou digital, compressões com perda, filtros lineares e não-lineares, recortes, escalonamentos, conversões digital-analógico e analógico-digital, inserções de ruído, etc... No caso de imagens digitais, deve resistir a ajustes de contraste, rotações, ampliações, até mesmo permutações de colunas ou linhas. No caso de vídeos, a marca segura deve resistir a permutações de quadros, remoção de quadros, etc... cada documento digital tem suas características específicas [BAR 04-b].

3.1.2 Marca d’água digital robusta

Feitas para resistir a manipulações que não sejam maliciosas, esse tipo de marca tem menor demanda que o tipo seguro. As marcas d’água digitais robustas servem para aplicações em que seria improvável que alguém manipulasse o documento digital com o objetivo de extrair a marca d’água. Por outro lado, a aplicação que utiliza esse tipo de marca constantemente manipula o documento digital, ou seja, o uso comum do documento não deve alterar a informação oculta, por isso a marca d’água precisa ser robusta [BAR 04-b].

3.1.3 Marca d’água digital semi-frágil

Feitas para resistir a um conjunto de manipulações limitado e bem específico, sendo que estas manipulações não são maliciosas e deixam o documento original praticamente intacto.

Este tipo de marca é usado quando a aplicação não exige robustez, mas impõe alguma perda ou alteração no documento marcado. Por exemplo, esse tipo de marca poderia ser inserida apenas para rotular um arquivo, que em seguida sofreria uma compressão com perda e seria armazenado num banco de dados. Então, para recuperar um arquivo desse banco de dados e obter a informação original, seria necessário recuperar a marca d’água dele. Após obtida a informação original, a marca d’água poderia ser descartada [BAR 04-b] [ZHA 03].

3.1.4 Marca d’água digital frágil

Feitas para não resistirem, uma marca d’água digital é considerada frágil se após uma pequena modificação no documento marcado a informação oculta é perdida. A perda

de informação oculta pode ser global, se nenhum pedaço da marca d'água digital puder ser recuperado, ou local, se apenas parte da marca d'água foi danificada.

Usa-se este tipo de marca para fazer verificação de integridade e/ou autenticação de conteúdo no documento, sendo que a perda da marca d'água é usada para indicar manipulações no documento [BAR 04-b].

3.2 Marca d'água digital privada e marca d'água digital pública

3.2.1 Marca d'água digital privada

Uma marca d'água digital é considerada privada se somente pessoas autorizadas podem recuperá-la, ou seja, ela é criada para que seja praticamente impossível recuperá-la sem autorização. Quando uma marca d'água privada também é legível, o leitor extrai a marca d'água do documento marcado (e possivelmente distorcido) e usa o documento original como pista para saber onde a marca d'água poderia estar no documento marcado.

Toda marca d'água que exige um método de recuperação não-cego é naturalmente privada, pois só o dono do documento original pode recuperar a marca d'água.

3.2.2 Marca d'água digital pública

Uma marca d'água digital é considerada pública se a técnica usada para recuperá-la é de conhecimento público.

3.2.3 Comparação entre marca d'água digital privada e marca d'água digital pública

Uma marca d'água digital privada é normalmente mais robusta que uma pública, pois quando a informação oculta se torna conhecida, fica muito mais fácil removê-la ou torná-la ilegível [BAR 04-b].

3.3 Marca d'água digital legível e marca d'água digital detectável

3.3.1 Marca d'água digital legível

Uma marca d'água digital é considerada legível se a informação oculta (os bits inseridos) pode ser lida sem ser conhecida de antemão. Para ler a marca d'água, o leitor só precisa receber como entrada o documento marcado (D_M) e talvez uma chave secreta (C_S).

Leitor (D_M, C_S) ⇒ M

Caso o processo de recuperação seja não-cego, também será necessário fornecer ao leitor o documento original (D).

Leitor (D_M, D, C_S) ⇒ M

Marcas d'água digitais legíveis são mais versáteis e por isso têm uso mais comum, pois normalmente podem ser recuperadas por métodos cegos e semi-cegos.

3.3.2 Marca d'água digital detectável

Uma marca d'água digital é considerada detectável se a informação oculta só pode ser detectada, ou seja, só é possível testar se um determinado código aparece no documento marcado. Para detectar a marca d'água, o detector precisa receber de entrada o documento marcado (D_M), a marca d'água (M) e talvez uma chave secreta (C_S). A saída do detector será uma decisão do tipo "sim" ou "não".

Detector (D_M, M, C_S) ⇒ Sim/Não

Caso o processo de detecção seja não-cego (vide conceito no item 3.4.3), também será necessário fornecer ao detector o documento original (D).

Detector (D_M, D, M, C_S) ⇒ Sim/Não

Como a marca d'água precisa ser conhecida de antemão para a detecção, esse tipo de marca d'água é sempre privada. Além disso, esse tipo é naturalmente mais robusto que o legível.

3.3.3 Marca d'água digital legível *x* detectável

Supondo que uma marca d'água digital, contendo o nome do proprietário, foi inserida numa imagem:

Legível: Quando a marca d'água não é um parâmetro necessário para o processo de recuperação. Basta o documento marcado e uma chave secreta (opcional) para descobrir o nome do proprietário.

Detectável: Quando a marca d'água é um parâmetro necessário para o processo de recuperação. Se a marca d'água é um parâmetro necessário para o processo de recuperação e não é conhecida de antemão, é impossível fazer a detecção e a leitura subseqüente do nome do proprietário [BAR 04-b].

3.4 Método de recuperação cego, método de recuperação semi-cego e método de recuperação não-cego

3.4.1 Método de recuperação cego

Um método de recuperação de marca d'água digital é considerado cego se ele não precisa comparar o documento original com o documento marcado.

3.4.2 Método de recuperação semi-cego

Um método de recuperação de marca d'água digital é considerado semi-cego se ele não precisa comparar o documento original e o documento marcado. Basta conhecer a marca d'água que esta sendo buscada. Ou seja, o semi-cego é um detector que não precisa do documento original.

3.4.3 Método de recuperação não-cego

Um método de recuperação de marca d'água digital é considerado não-cego se ele precisa, obrigatoriamente, comparar o documento original e o documento marcado.

3.5 Marca d'água digital invertível e marca d'água digital quase-invertível

3.5.1 Marca d'água digital invertível

Uma marca d'água digital é invertível se para qualquer documento onde ela pode ser inserida existe um processo inverso de inserção que gera uma marca d'água invertida (M_I). Esse processo mantém a semelhança entre o documento marcado e o documento original. Mais importante do que isso, inserir no documento original (D) a marca d'água invertida e a marca d'água normal (M), causa um cancelamento, ou seja, o documento

reverte ao seu estado original.

$$D + M + M_I = D$$

Caso uma marca d'água não satisfaça essas exigências, ela é dita não-invertível.

Toda marca d'água digital invertível é também reversível em senso amplo (somar $M + M_I$ faz o documento voltar ao original). É adequado usá-las para garantir a integridade de imagens médicas ou militares (como descrito na seção 4.1).

3.5.2 Marca d'água digital quase-invertível

Uma marca d'água digital com método de recuperação não-cego é quase-invertível se para qualquer documento onde ela pode ser inserida existe um processo inverso de inserção que gera uma marca d'água invertida (M_I), sendo que esse processo mantém a semelhança entre o documento marcado (D_{MI}) e o documento original (D).

$$D + M_I = D_{MI}$$

Mais importante do que isso, se o documento original (que não possui nenhum tipo de marca) for testado num detector e o documento com a marca invertida for usado como um falso documento original, o detector deve acusar a presença da marca d'água no documento original.

$$\text{Detector } (D, D_{MI}, M_I) \Rightarrow \text{Sim}$$

Caso uma marca d'água não satisfaça essas exigências, ela é dita não-quase-invertível.

3.6 Marca d'água digital reversível em senso estrito e marca d'água digital reversível em senso amplo

3.6.1 Marca d'água digital reversível em senso estrito

Uma marca d'água digital é reversível em senso estrito se uma vez que ela é

recuperada (lida ou detectada), ela também pode ser removida do documento, tornando possível voltar ao documento original.

Reversibilidade em senso estrito também implica reversibilidade em senso amplo.

3.6.2 Marca d’água digital reversível em senso amplo

Uma marca d’água digital é reversível em senso amplo se, uma vez recuperada (lida ou detectada), é possível torná-la irrecuperável (ilegível ou indetectável) sem produzir distorções perceptíveis no documento marcado.

Para exemplificar: Qualquer marca d’água que só muda os bits menos significativos (LSB) de uma imagem é reversível em senso amplo, pois se alguém descobre que a marca está na imagem e deseja torná-la irrecuperável, basta tornar todos os LSB da imagem iguais a 0 ou iguais a 1. Isso não vai retornar a imagem ao estado original (provavelmente os LSB dela não eram todos 0 ou todos 1), mas vai desmanchar a marca d’água. Como a modificação foi nos LSB, obviamente ela não é perceptível. Outra coisa óbvia que se pode concluir do exemplo: marca d’água que só muda LSB não serve para proteger autoria (pois é fácil apagá-la), mas serve para proteger integridade (testamos a presença da marca d’água, se ausente, a imagem não está íntegra).

3.7 Marca d’água digital simétrica e marca d’água digital assimétrica

3.7.1 Marca d’água digital simétrica

Uma marca d’água digital é simétrica se o método de recuperação usa o mesmo conjunto de parâmetros usados na inserção da marca d’água. Esses parâmetros podem incluir uma chave secreta (opcional), introduzida no processo de inserção da marca para tornar sigiloso os parâmetros que o definem e, principalmente, o número e a posição das partes do documento que serão alteradas pela inserção da marca d’água.

Toda marca d’água digital simétrica é também reversível em senso amplo, já que até hoje não surgiu um algoritmo que contradiga essa afirmação.

3.7.2 Marca d’água digital assimétrica

Uma marca d’água digital é assimétrica se o método de recuperação dela usa parâmetros diferentes dos que foram usados no processo de inserção. Em tais marcas d’água, usam-se duas chaves, uma chave privada e uma chave pública. A chave privada é usada para inserir a informação oculta dentro do documento e a chave pública é usada para recuperar a marca d’água (normalmente a chave pública é um subconjunto da chave privada). Quem conhece a chave pública não tem condições de, a partir dela, descobrir qual é a chave privada.

4 IMAGENS DIGITAIS

4.1 Noções de integridade e autenticação de conteúdo em imagens digitais

Assegurar a integridade de um documento digital é garantir que os dados contidos no documento remetido e os dados contidos no documento recebido são os mesmos. Essa definição pode ser aplicada a qualquer documento digital, mas é pouco útil quando se fala em imagens digitais. No caso de tratamento de imagens, altera-se o valor dos pixels, por exemplo, para clareá-la ou escurecê-la. Isto não altera o significado da informação contida na imagem. Ou seja, o problema da autenticação em imagens digitais não está na integridade absoluta da imagem, mas na parte significativa do conteúdo da imagem (a informação que ela passa).

O problema para as imagens digitais é definir quando uma alteração no documento muda o significado da imagem. Portanto, para que a marca d'água digital forneça um serviço de autenticação à imagem digital, ela precisa saber diferenciar manipulações (maliciosas ou não) feitas na imagem (recortes e inserções) de tratamentos usuais da imagem (mudança de formato/nitidez/contraste e compressões). Infelizmente, nem sempre é fácil diferenciar um tipo de manipulação do outro. Por exemplo, existem métodos de compressão com perda, como o JPEG, que modificam a imagem original, sendo vistos por algumas marcas d'água digitais pouco robustas como uma manipulação maliciosa, o que não é o caso.

A diferença entre uma manipulação ou um tratamento usual tolerável também depende do tipo de imagem e do uso pretendido. Por exemplo, serão diferentes os critérios de integridade utilizados para uma imagem médica e uma imagem artística. Para a imagem médica, perder qualquer detalhe pode torná-la inútil. Já para a imagem artística, um método de compressão com perdas pode não afetar a imagem como um todo, já que estes métodos têm como objetivo causar perdas onde elas são menos perceptíveis para o olho humano.

Embora sejam de uso muito específico, existem métodos dedicados a criar marcas

d’água digitais que garantem a autenticação de conteúdo de imagens cuja aplicação exige muita integridade (imagens médicas ou militares, por exemplo). Nestes tipos de imagem, não se deve permitir modificações de qualquer tipo, inclusive as causadas por uma marca d’água. Um dos métodos usados para resolver esse problema é um sistema de marca d’água reversível, de forma que, se a imagem for considerada autêntica, será possível remover todas as alterações causadas pela inserção da marca d’água (retirar a marca d’água) na imagem original. Outra alternativa é separar a imagem em duas regiões, a região interessante e a região desinteressante. A região interessante é a parte da imagem usada para verificar autenticidade de conteúdo. Nela a integridade da informação deve ser elevada. Já a região desinteressante é a parte da imagem usada para guardar informações de autenticação usadas pela marca d’água digital, nesta região a garantia de integridade da informação é mínima [REY 02] [WON 01].

4.2 Manipulações maliciosas em imagens digitais

Antigamente, uma fotografia não poderia "mentir", era mais fácil duvidar do que estava escrito em um texto do que duvidar da origem ou da integridade de uma fotografia. É por isso que até hoje uma imagem é mais valorizada do que um texto, porque uma imagem é vista pela maioria das pessoas como uma prova da verdade. Já um texto pode ser facilmente colocado em questionamento, devido aos possíveis interesses do autor ou a possibilidade de que ele seja fictício. Entretanto, atualmente é possível editar imagens digitais de forma a criar uma imagem editada que parece genuína, tudo isso com facilidade, rapidez e praticamente sem custo.

Considerando o que foi dito anteriormente, percebe-se que uma marca d’água para autenticação de conteúdo de imagens precisa ser capaz de detectar alterações feitas na imagem após ela ser obtida ou criada, por exemplo, ser capaz de diferenciar a fotografia original de sua versão retocada, para ser publicada em uma revista, jornal ou web site.

Em 2001, uma fotografia publicada na primeira página de um jornal austríaco tinha como objetivo mostrar a agressividade dos manifestantes revoltados com o governo. A fotografia mostrava um manifestante que supostamente tinha atingido um policial.

Usando programas de edição de imagens, a foto foi cortada, a distância entre o manifestante e o policial foi reduzida em aproximadamente dois metros. Mais tarde foi provada a fraude, com a publicação da foto original.

Devido ao fato de que fraudes como essa têm se tornado cada vez mais comuns, o uso de documentos digitais nos tribunais têm se tornado cada vez mais questionável. Ironicamente, o uso de câmeras de vigilância nas portas das residências e em lugares públicos têm aumentado [JEL 00] [REY 02].

4.3 Como deve ser uma marca d'água digital para autenticação de imagens

Para que uma marca d'água digital seja eficiente, ela precisa ter a tolerância e a sensibilidade adequadas ao uso da imagem, sendo que uma destas características pode se destacar mais do que a outra dependendo da finalidade da marca d'água digital e do escopo de uso da imagem.

A tolerância ou robustez de uma marca d'água digital é a capacidade que ela tem de tolerar um pouco de perda de informação decorrente de tratamentos usuais (compressão, nitidez etc). Já a sensibilidade ou fragilidade de uma marca d'água digital é a capacidade que ela tem em ser sensível à manipulações. Por serem características conflitantes, é difícil conciliar tolerância e sensibilidade.

Adicionalmente, é desejável que a marca d'água digital seja capaz de localizar regiões alteradas, ou seja, ela precisa ser capaz de localizar as regiões alteradas por manipulações maliciosas e, ao mesmo tempo, reconhecer como autênticas as regiões intactas. Para algumas aplicações, não é suficiente apenas localizar regiões alteradas, mas também reconstruir essas regiões. Para estas aplicações, a marca d'água digital precisa ser capaz de restaurar, mesmo que de forma incompleta, as regiões alteradas por manipulações maliciosas.

Por se tratar de marca d'água digital, a informação oculta obrigatoriamente deve

estar embutida na imagem digital, ao contrário de outros métodos de autenticação onde a informação pode estar num arquivo separado. Também é conveniente que a informação oculta seja invisível quando feita uma inspeção simples na imagem marcada. O impacto visual da marca d'água deve ser o menor possível, para que a imagem marcada seja idêntica à imagem original. Além disso, deve ser impossível manipular a informação oculta em separado.

O método de recuperação que deve ser usado para recuperar a marca d'água digital vai variar de acordo com o algoritmo de criação dela. Dependendo de como a informação oculta depende da imagem digital, usa-se um método de recuperação cego ou semi-cego. Um método de recuperação que não seja cego necessita da imagem original (e íntegra) para funcionar, obviamente um método assim não serve para nada quando se possui apenas a imagem digital já marcada para analisar.

Para fornecer um bom serviço de autenticação de conteúdo, o algoritmo de criação da marca d'água digital deve ser assimétrico, ou seja, usar um algoritmo de criptografia assimétrica. Isso ocorre porque na criptografia assimétrica só o criador da marca d'água digital terá a chave privada, só ele conhecerá o método utilizado para inserir a marca d'água digital na imagem. Portanto, mesmo que outras pessoas conheçam o método para recuperar a marca d'água digital da imagem, só o criador dela sabe inserí-la, comprovando desta forma que ele é o autor e que ninguém poderia inserir sua marca d'água numa imagem que não é autêntica [MAC 03] [REY 02].

4.4 Marcas d'água digitais frágeis e semi-frágeis para uso em imagens

Se o objetivo é autenticar o conteúdo da imagem com mais rigor, isto é, proteger o significado dela, as marcas d'água digitais frágeis e semi-frágeis são o método mais indicado. A idéia principal aqui é inserir uma marca d'água que não depende da imagem digital, ou seja, uma marca d'água aditiva. Assim, qualquer alteração na imagem marcada alterará a marca d'água. O método de recuperação da marca d'água digital consiste em localizar regiões em que foram feitas alterações na marca d'água, desta forma também localizando as regiões da imagem que foram alteradas.

4.4.1 Patchwork

O algoritmo chamado Patchwork é uma das primeiras marcas d'água que foram descritas na literatura científica. Aqui ele será descrito em sua versão original, embora com o passar do tempo, diversas modificações tenham sido propostas, para superar os limites da versão original.

Patchwork é uma marca d'água típica do domínio espacial, que usa um algoritmo aditivo (tal algoritmo não leva em consideração o valor original do pixel para determinar qual será sua mudança). Dependendo de uma chave secreta, determina-se um número grande e par que chamaremos de N. Depois escolhe-se N pixels da imagem digital, os quais farão parte do conjunto S. Divide-se S em duas partes iguais, dois subconjuntos, S_1 e S_2. Os pixels pertencentes a S_1 serão incrementados com um pequeno valor, de X unidades; os pixels pertencentes a S_2 serão decrementados em X unidades.

Se (pixel $\in$ S)
  Então Se (pixel $\in$ S_1)
    Então (pixel $\Leftarrow$ pixel + X)
    Senão (pixel $\Leftarrow$ pixel - X) //pixel $\in$ S_2
Senão (pixel $\notin$ S)

Fica claro que para uma imagem não marcada, a diferença média entre pixels de S_1 e S_2 deveria ser próxima de 0. Já para uma imagem marcada, tal diferença deveria ser próxima de 2X. Desta forma é possível distinguir uma imagem marcada de uma não marcada.

O grande problema desta marca d'água é que ela só serve para autenticar a imagem como um todo, ela não permite que se localizem possíveis regiões alteradas. Enfim, a marca d'água (Patchwork) apenas responde a pergunta: A imagem está ou não está marcada?

Os métodos seguintes procuram resolver este problema dividindo a imagem em

vários blocos 8x8 e fazendo a autenticação dos blocos individualmente. Entretanto, aplicar o Patchwork em poucos pixels comprometeria a pressuposição estatística de que os conjuntos S_1 e S_2 inicialmente eram semelhantes [BAR 04-b] [BEN 95] [KAT 00].

4.4.2 Dígito verificador nos bits menos significativos (LSB)

O método mais simples para autenticar imagens é tornar dígito verificador os bits menos significativos (LSB) da imagem digital.

A marca d'água digital simétrica proposta por Walton em 1995 consiste em selecionar, de acordo com uma chave secreta, um grupo pseudo-randômico de pixels. Nos pixels selecionados, somam-se os 7 bits mais significativos (MSB), guardando o resultado nos LSB, transformando-os em dígito verificador. O algoritmo de inserção da marca d'água funciona da seguinte forma:

1) Escolhe-se um número inteiro grande (N).
2) Divide-se a imagem em blocos 8x8 (cada bloco fica com 64 pixels).
3) Para cada bloco:

3.a) Define-se uma caminhada pseudo-randômica através dos 64 pixels do bloco. Essa caminhada depende do número do bloco e da chave secreta escolhida. De acordo com a ordem em que é visitado, cada pixel do bloco recebe um número entre 1 e 64 (p_1, p_2, p_3,..., p_{64}).

3.b) Gera-se uma seqüência pseudo-randômica de 64 números inteiros (a_1, a_2, a_3,..., a_{64}), comparáveis em tamanho com N.

3.c) Para cada pixel p_j, obtêm-se o nível de cinza determinado por seus 7 MSB, depois multiplica-se esse valor por a_j e por último o resultado é dividido por N. O resto da divisão inteira é acumulado em S. S é guardado nos LSB de cada pixel do bloco.

$S \Leftarrow 0$;

Para j = 1 até 64

  $S \Leftarrow S + \text{NívelDeCinzaDos7MSB}(p_j) \times a_j \bmod N$;

InsiraNosLSBDoBloco (S);

Ou seja, S é igual a:

$$\sum_{j=1}^{64} aj \; x \; NivCinza(pj) \; mod \; N$$

A recuperação da marca d'água é similar ao processo de inserção. Ela consiste em comparar, para cada bloco, a soma dos MSB dele com o que está armazenado nos LSB do bloco.

A grande vantagem deste método é que ele não produz alterações visíveis na imagem e possui uma grande probabilidade de detecção de alterações. Por exemplo, se quaisquer 2 pixels de um mesmo bloco forem trocados, todo o bloco será dado como modificado, pois cada pixel p_j é multiplicado por um valor a_j diferente. Além disso, como a caminhada pseudo-randômica através dos pixels p_j e os valores a_j dependem do bloco em questão, é praticamente impossível permutar blocos inteiros sem causar mudanças indetectáveis. Uma das desvantagens da marca d'água LSB é que é possível permutar blocos idênticos (mesma posição) de duas imagens diferentes marcadas com a mesma chave secreta [WAL 95] [REY 02].

4.4.3 Auto-inserção

A marca d'água proposta por Fridrich e Goljan consiste em inserir uma imagem digital nela mesma, com o objetivo de proteger o conteúdo da imagem. Por causa disso, essa marca d'água permite reparar parcialmente regiões da imagens que forem cortadas, alteradas ou substituídas.

Para ser possível inserir a imagem nela mesma, a imagem original é compactada e inserida nos LSB de seus pixels. Como todo método de marca d'água que insere a informação oculta nos LSB, esse método não produz alterações visíveis na imagem original. O algoritmo consiste em dividir a imagem em blocos 8x8, ajustar os LSB de cada pixel para 0 e depois calcular a transformada discreta do cosseno (DCT) para cada bloco. Após, a matriz da DCT é quantizada com uma matriz de quantização correspondente a uma qualidade JPEG de 50%. O resultado é guardado usando apenas 64 bits e inserido nos LSB

de outro bloco. É desejável que o bloco protegido e o bloco marcado sejam distantes entre si, para prevenir que uma modificação em um pequeno pedaço da imagem danifique ambos simultaneamente.

A qualidade do reparo fornecido por essa marca d'água é ligeiramente pior que 50% de qualidade JPEG, mas suficiente para informar o conteúdo original da região reparada.

O algoritmo de inserção da marca d'água funciona da seguinte forma:

1) Torna-se 0 todos os LSB dos pixels da imagem.
2) Divide-se a imagem em blocos 8x8 (cada bloco fica com 64 pixels).
3) Para cada bloco:
   3.a) Calcula-se a DCT.
   3.b) Multiplica-se a matriz da DCT por uma matriz de quantização.
   3.c) De acordo com uma chave secreta, define-se outro bloco que irá guardar o resultado em seus LSB.

A maior desvantagem deste método é que a informação inserida não é robusta, ao contrário, é muito frágil. Se várias regiões distintas são modificadas, a informação de reparação também pode ficar corrompida. Além disso, após modificações globais na imagem, como filtragem ou compressão com perda, a maior parte da informação de reparação estará corrompida, pois os valores presentes nos LSB são modificados por estes tipos de operação [FRI 99] [REY 02].

5 BATERIA DE TESTES

Esta bateria de testes tem por objetivo testar a robustez de marcas d'água contra ataques maliciosos e tratamentos usuais.

Software de tratamento digital da imagem:
Adobe Photoshop CS3 Extended, versão 10.0.

Software para inserção e recuperação de marca d'água:
Digimarc Corporation - https://www.digimarc.com/about

A Digimarc é uma empresa que se posiciona no mercado com a missão de implementar novas soluções destinadas a ampliar a segurança, combater fraude, contravenções e pirataria de imagens.

Digimarc também é o nome do software de marca d'água embutido na versão do Photoshop usada nesta bateria de testes. Ele insere e lê marcas d'água imperceptíveis.

Uma aplicação corrente é a proteção de imagens de fotógrafos, agências de publicidade e veículos de comunicação (jornais e revistas). No caso de uso indevido da imagem (cópia ou adulteração), o autor consegue provar autoria, pois ele consegue recuperar a marca d'água imperceptível que ele próprio inseriu na imagem.

Normalmente, esta aplicação usa a opção marca d'água segura, ou seja, a marca d'água resiste, continua existindo apesar da manipulação maliciosa da imagem, preservando a identidade do autor.

Esta bateria de testes procura mostrar a resistência da marca d'água robusta e imperceptível que será inserida na imagem a seguir:

Figura 5.1: Imagem original (Oath of Druids)

A imagem 5.1 é a original, ela se chama “Oath of Druids”. Trata-se de uma imagem colorida no formato bitmap (390x316 pixels, 362KB, 24 bits por pixel, 8 pixels para cada canal). Esta imagem não tem nenhuma marca d’água.

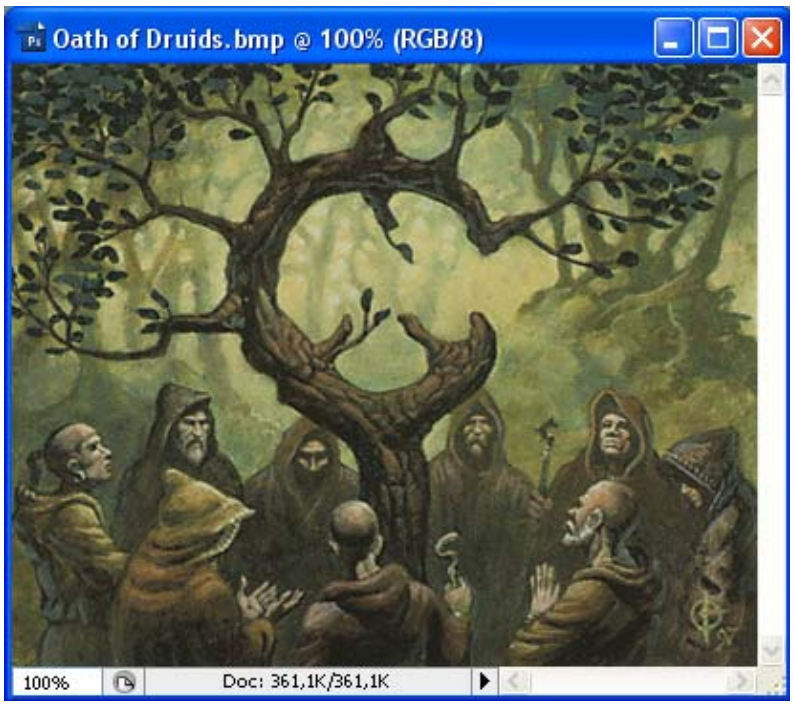

Figura 5.2: Imagem original aberta no Photoshop

A imagem 5.2 é a imagem 5.1 aberta no programa Adobe Photoshop CS3 Extended, ainda sem marca d'água. Não existe nenhuma diferença perceptível entre as imagens 5.1 e 5.2, conforme esperado, pois nenhuma modificação foi feita.

5.1 Inserção de Digimarc na imagem original

No Adobe Photoshop CS3 Extended, a inserção da marca d'água digital segura e imperceptível Digimarc é feita no menu abaixo:

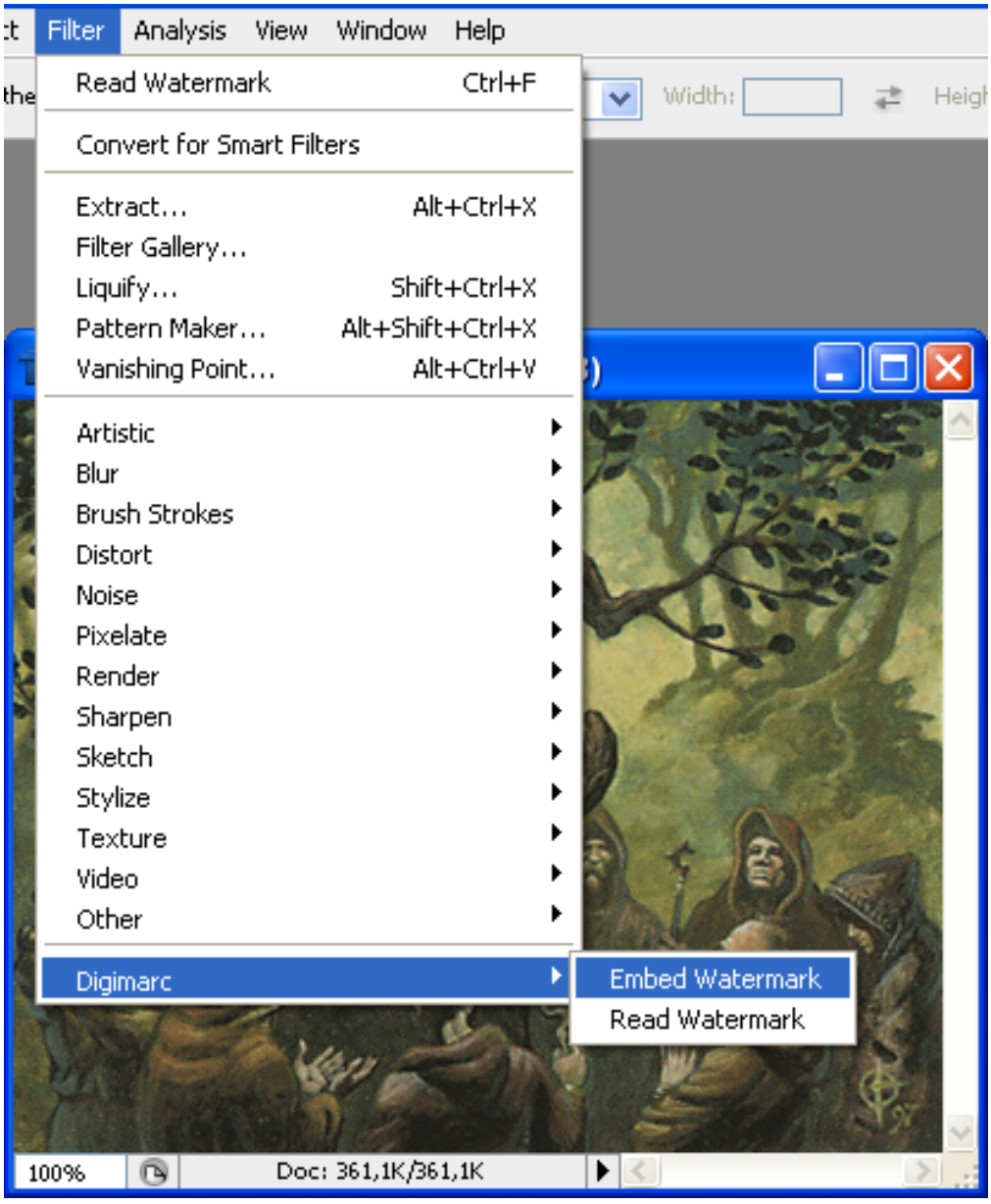

Figura 5.3: Tela ensinando como inserir Digimarcs no Photoshop

Abaixo, aparece uma janela de escolha de parâmetros para a inserção. O parâmetro “Watermark Durability” indica a robustez da marca d’água, em escala crescente de 1 a 4. O número “2008” ao lado de “Image ID” é uma informação que será escondida na imagem. Poderia ser qualquer número: o CPF do autor ou o número seqüencial desta foto no arquivo do autor, por exemplo. A Digimarc exige que o conteúdo da marca d’água seja um número, não pode ser um texto.

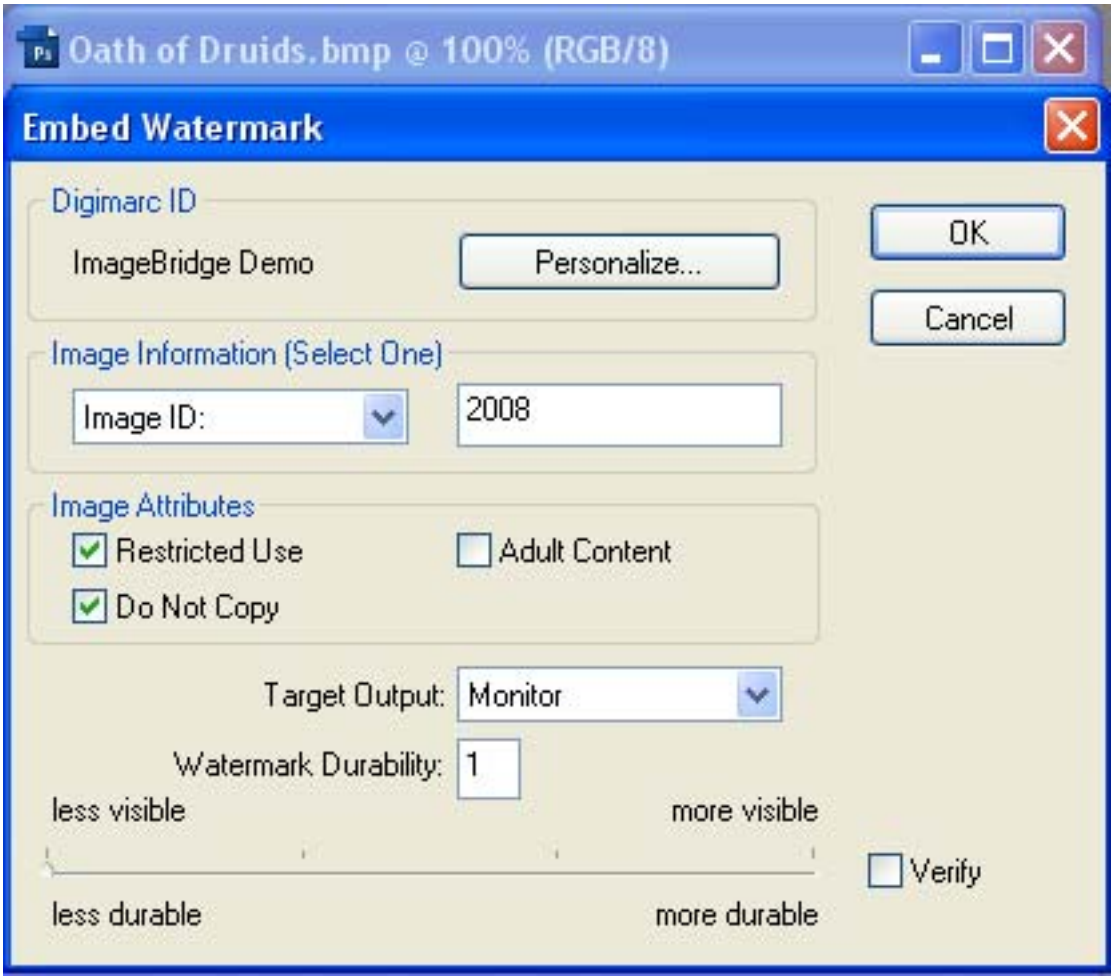

Figura 5.4: Janela de escolha de parâmetros para inserção

A seguir, a imagem marcada através do procedimento anterior. As Digimarcs não causaram perda de qualidade.

Figura 5.5: Oath of Druids marcado com Digimarc de durabilidade 1

A janela abaixo mostra o resultado da leitura da marca d'água presente na imagem acima. Foi lido o número "2008", inserido anteriormente.

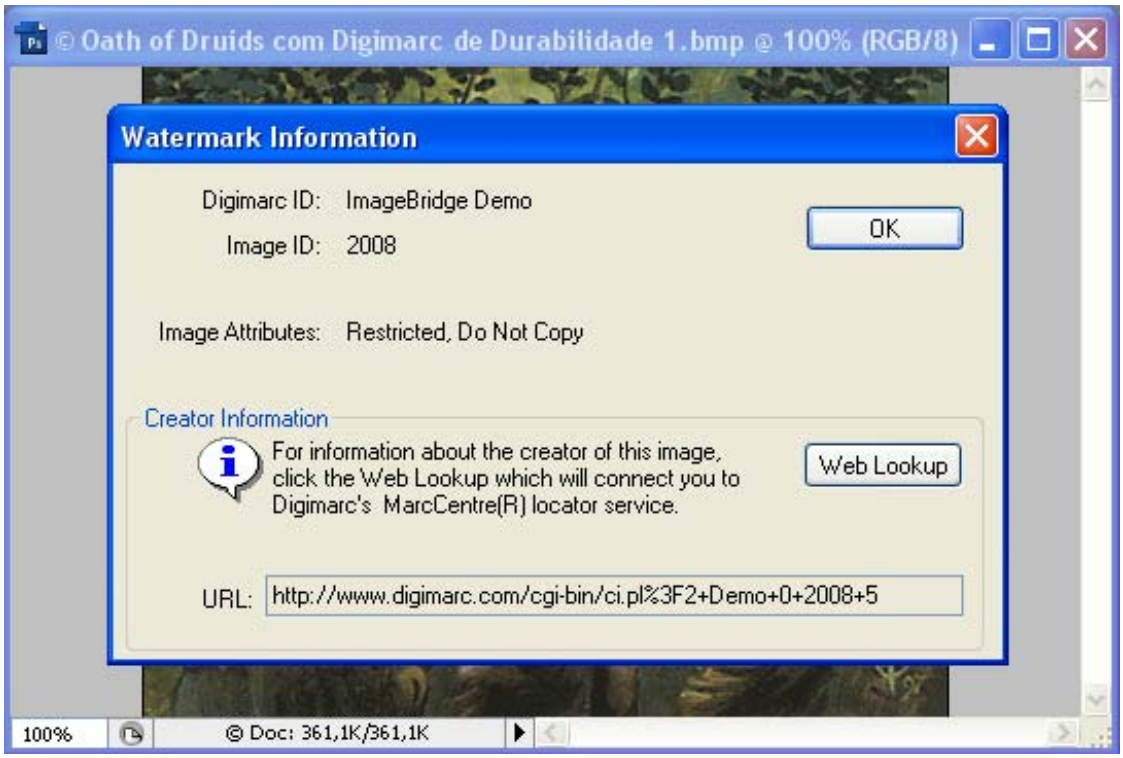

Figura 5.6: Janela mostrando leitura bem sucedida de Digimarc

Ataques maliciosos ou tratamentos que ultrapassam certos limites, podem destruir a marca d'água, como mostra a janela abaixo (o ruído gaussiano destruiu a Digimarc):

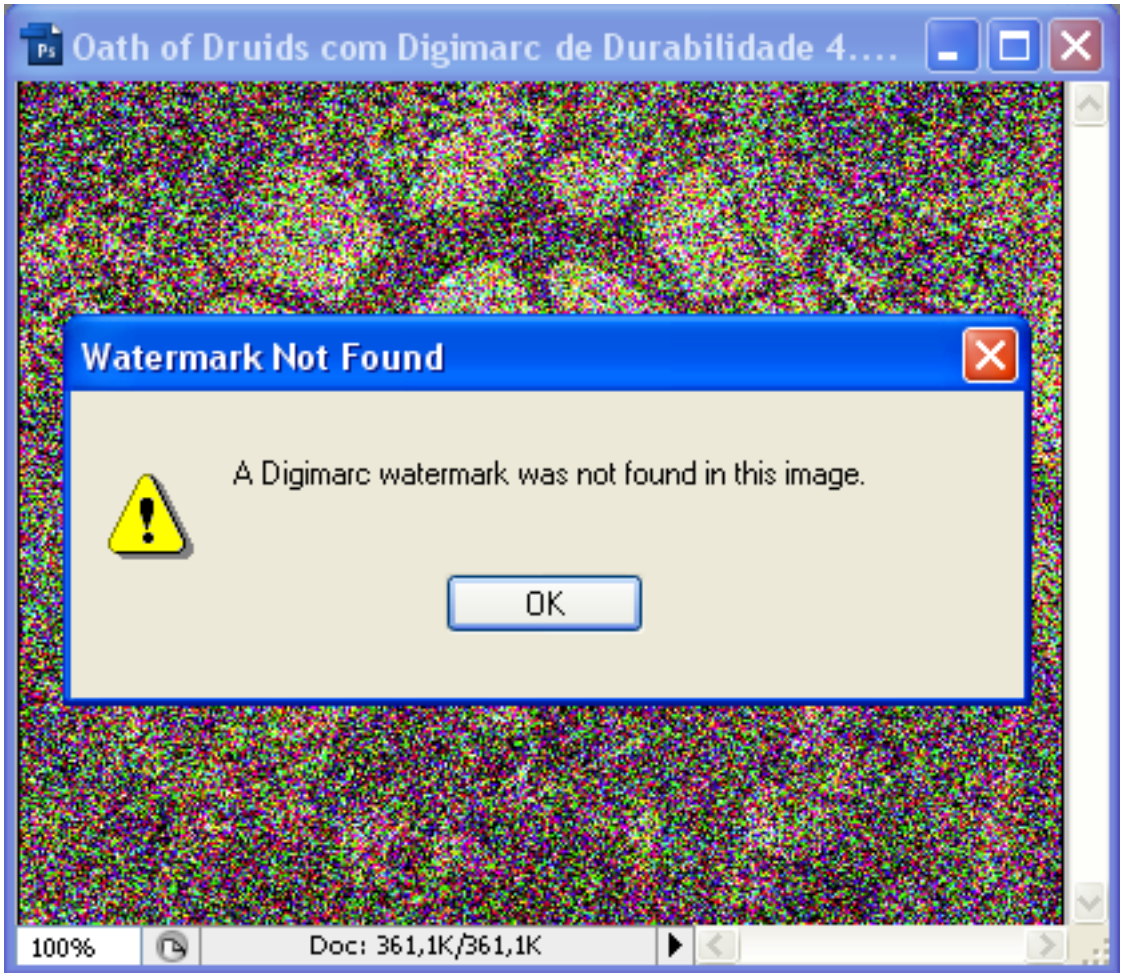

Figura 5.7: Janela mostrando leitura mal sucedida de Digimarc

5.2 Teste A: Resistência da marca d'água a recorte

Em marcas d'água visíveis, é fácil remover a marca d'água através de recorte na imagem marcada. Normalmente, uma imagem recortada para remover este tipo de marca d'água continua passando a mesma informação.

As duas imagens seguintes passam a mesma informação, um carro atolado na água (ou tentando atravessar um obstáculo). A diferença entre elas é que a primeira imagem

possui uma marca d’água visível (chakal.com), na segunda imagem, a marca d’água foi removida através de recorte.

Figura 5.8: Imagem com marca d’água visível (“chakal.com”)

Figura 5.9: Imagem cuja marca d’água visível foi recortada

Figura 5.10: Recorte extraído de Oath com Digimarc 1

A Digimarc de durabilidade 1 resistiu até o recorte acima (a cabeça de um dos monges, 64x72 pixels), ou seja, a imagem perdeu todo o seu significado e a marca d'água ainda protege o autor. A marca d'água só se perde em recortes menores do que este.

5.3 Teste B: Resistência da marca d'água a variação de brilho e contraste

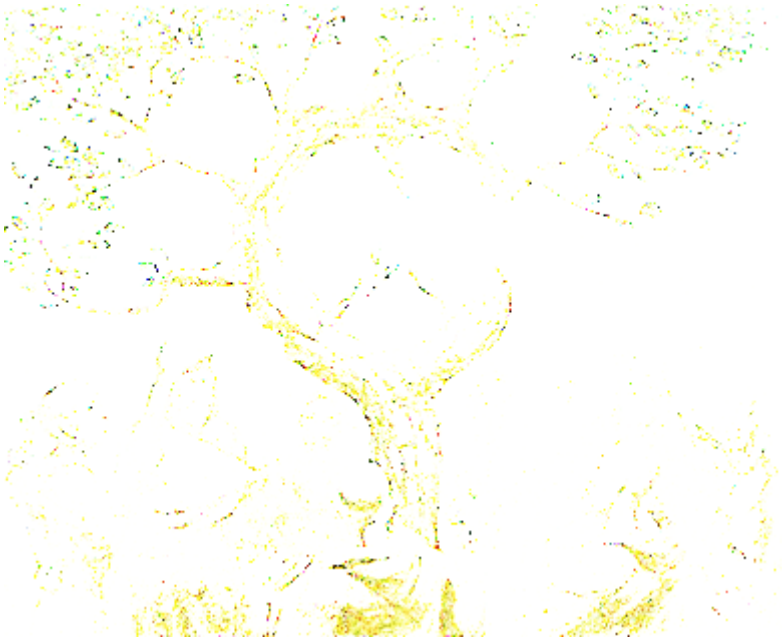

Figura 5.11: Oath com Digimarc 1, brilho e contraste aumentados

Os níveis de brilho e contraste foram aumentados até se perder a marca d'água. Pouco antes de perder a marca d'água, a imagem já estava irreconhecível como mostra a imagem acima. Ou seja, inútil para uso não autorizado, mas a marca d'água estava lá, pronta para indicar o seu autor.

Figura 5.12: Oath com Digimarc 1, brilho e contraste diminuídos

Na imagem acima foi diminuído o brilho e o contraste. Mesmo a Digimarc mais frágil, de durabilidade 1, resistiu até o resultado mostrado. Ou seja, não se tem imagem, mas a marca d'água pode ser lida.

5.4 Teste C: Resistência da marca d'água a redução das dimensões

Figura 5.13: Oath com Digimarc 1 e dimensões reduzidas

As Digimarcs (independentemente da durabilidade de 1 a 4) resistiram até o resultado mostrado na imagem 5.13, onde largura e altura foram reduzidas (272x220 pixels). Ou seja, alguém interessado no uso indevido ainda conseguiria uma boa imagem SEM a marca d'água do autor, embora com dimensões reduzidas. A proteção do autor nos outros testes (recorte, ruído gaussiano, compressão, contraste e brilho) é mais eficiente do que a proteção quanto à redução das dimensões.

5.5 Teste D: Resistência da marca d'água a ruído gaussiano

Ruído gaussiano é uma degradação comum em imagens. Pode ocorrer devido a erros de transmissão ou ser inserido propositalmente.

Figura 5.14: Oath com Digimarc de durabilidade 1 e ruído gaussiano de 25%

Foram testados todos os níveis de robustez, a partir da durabilidade 1 até a durabilidade 4. Para cada nível, foi introduzido ruído gaussiano a partir de 10%, em pequenos acréscimos. Para cada nível de ruído introduzido, verificava-se se a marca d'água ainda resistia.

A Digimarc de durabilidade 1 resistiu até a 25% de ruído gaussiano.

As Digimarcs de durabilidade 2 e 3 resistiram até 26%, um percentual muito parecido com o do teste com durabilidade 1. A imagem com 26% de degradação é praticamente igual àquela com 25% de ruído gaussiano (vide imagem 5.14).

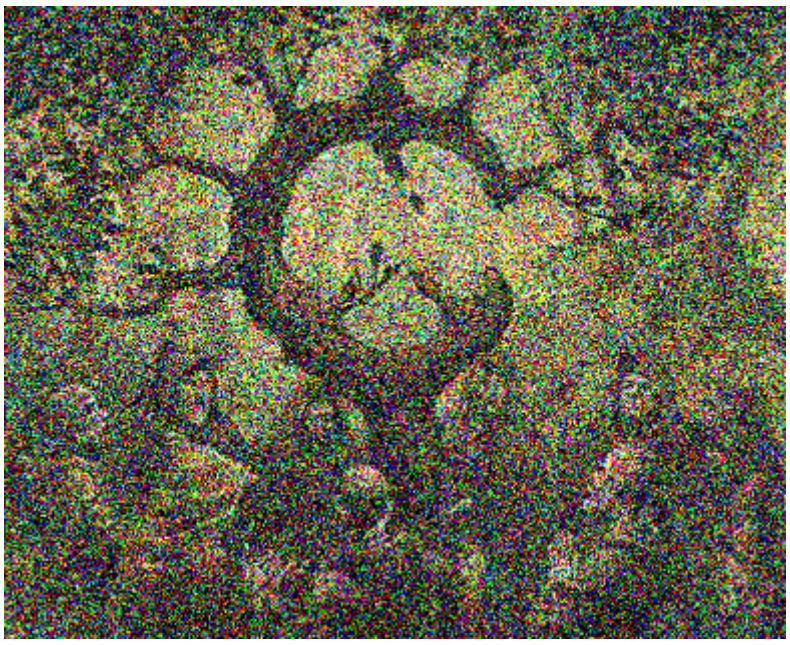

Figura 5.15: Oath com Digimarc de durabilidade 4 e ruído gaussiano de 40%

A Digimarc de durabilidade 4 demonstrou um salto na robustez, comparada com as anteriores, resistindo a ruído gaussiano de até 40%. A imagem está quase inutilizada para fins indevidos, mas a marca d'água ainda pode ser lida. O direito autoral continua preservado, mesmo após o colapso da imagem.

5.6 Teste E: Resistência da marca d’água a compressão JPEG

Figura 5.16: Oath com Digimarc 1 em formato jpg

A Digimarc de durabilidade 1 resistiu à máxima compressão JPEG disponível. A mudança de formato (bmp para jpg) mudou o tamanho do arquivo de 362KB para 36KB (90% de perda de dados). As outras durabilidades mostraram o mesmo desempenho.

6 CONCLUSÃO

Ao longo dos tempos, as sociedades desenvolveram técnicas para dar segurança a documentos convencionais com relação a sua autoria e integridade. A assinatura em um cheque bancário ou em um contrato comercial serve para dar segurança às partes, inclusive validade jurídica. Os Cartórios Notariais e Tabelionatos são exemplo de instituições de fé pública, que oferecem serviços de Reconhecimento de Assinaturas e Autenticação de Documentos convencionais, indispensáveis para a segurança e credibilidade das relações formais numa sociedade organizada.

De forma análoga, estas sociedades organizadas precisam de mecanismos, como os Certificados Digitais, para garantir a segurança dos documentos digitais. Uma assinatura digital tem por objetivo garantir a integridade do documento no seu nível mais alto. Ou seja, basta uma alteração mínima, a nível de bit, para que a manipulação seja detectada.

No caso de imagens, é necessário maior tolerância a alterações. Existe uma ampla gama de operações com imagens (tratamento digital) que, embora mudem alguns pixels, ainda podem ser consideradas fiéis à informação básica que armazenam. Mudanças decorrentes de compactação (como o padrão JPEG) iriam dar um falso negativo (não-autêntica) se a imagem fosse submetida aos rígidos sistemas de autenticação usados em documentos digitais bancários, por exemplo. Ou seja, em muitas imagens digitais, o objetivo é avaliar se o essencial da informação está preservado. Uma marca d'água frágil ou semi-frágil, adequadamente escolhida e aplicada, não deve provocar repúdio de um documento submetido a alterações toleráveis na aplicação em questão.

A literatura sobre marca d'água digital trata, tipicamente, da sua aplicação em imagens digitais. As marcas d'água podem ser seguras, robustas, semi-frágeis e frágeis, conforme seu grau de tolerância a alterações do documento original. As seguras e robustas resistem melhor a tratamentos necessários na imagem.

No outro extremo, existem aplicações que exigem marcas d'água frágeis ou semi-frágeis para autenticar imagens. Ou seja, a marca d'água não resiste (frágil portanto) a alterações mínimas da imagem, mesmo que seja uma compressão em formato consagrado, como o JPEG.

Este trabalho conclui sobre a necessidade de maior exploração e entendimento dos limites toleráveis no tratamento digital de imagens. Foram feitas pesquisas sobre softwares disponíveis ao usuário leigo. A primeira constatação é que a oferta é limitada e as informações sobre os níveis de segurança oferecido pelos produtos é confusa.

Na outra ponta, existe um usuário que sabe que precisa de um pouco mais de segurança quanto à autoria e integridade das imagens com as quais trabalha. Existem relatos de agências de propaganda e meios de comunicação que já tiveram problemas em imagens trocadas pela internet. Mesmo assim, a grande maioria ignora o problema ou prefere correr riscos em vez de investir em consultoria e produtos de eficácia que ele, usuário, desconhece.

Marca d'água é um assunto novo no mundo corporativo. Muito investimento ainda deve ser feito para que o volume de tráfego de imagens com marcas d'água seja significativo.

Este trabalho procura trazer sua contribuição, reunindo de uma forma sintética os principais conceitos relacionados às marcas d'água. Tece considerações sobre aplicação de marcas d'água imperceptíveis em imagens digitais. A título de exemplo, mostra algumas conclusões sobre o uso das ferramentas de segurança do Photoshop, escolhido pela popularidade e liderança mundial em softwares para edição e tratamento de imagens digitais.

Futuros trabalhos poderiam explorar melhor um problema crítico relacionado à aplicação prática de marcas d'água. É necessário uma normalização dos limites, muitas vezes tênues, para diferenciar o tratamento necessário de imagens digitais da sua

manipulação maliciosa em algumas aplicações.

Aplicações críticas como, por exemplo, diagnóstico médico por imagem ou inspeção de peças (aeronáuticas, navais e outros segmentos industriais) vão requerer pessoal de informática mais preparado, maior conhecimento pelos usuários e produtos mais fáceis de serem utilizados.

Há um longo caminho a percorrer na busca de maior segurança com relação a autoria e integridade de imagens digitais.

REFERÊNCIAS

[AND 96] ANDERSON, R. **Information Hiding**. Lectures Notes in Computer Science - Springer - Verlag, 1174:38-48, 1996.

[BAR 04-a] BARCELOS, C. A. Z.; et al. **Introdução à marca d'água digital**. XV Jornada de Matemática do Catalão, 1:1-9, 2004.

[BAR 04-b] BARNI, Mauro; BARTOLINI, Franco. **Watermarking Systems Enginnering Enabling Digital Assets Security and Other Applications**. Signal Processing and Communications Series. Marcel Dekker. 2004.

[BEN 95] BENDER, W. R.; GRUHL, D.; MORIMOTO, N. **Techniques for data hiding**. Storage and Retrieval of Image and Video Databases III. Proceedings of the SPIE 2420, W. Niblack and R. C. Jain, eds., San Jose, CA, USA. 1995.

[COX 01] COX, I. J.; et al. **Digital Watermarking**. Morgan Kaufmann Publishers, 2001.

[DEL 00] DELP, E. J. **Security and watermarking of multimedia contents**. Proc. of the Society of Photo-optical Instrumentation Engineers, 3657, 2000.

[FRE 07] FREDERES, Thiago Albuquerque. **Digital Watermarking: Autenticação de imagens com o uso de marca d'água digital**. 2007. 38 f. Trabalho de graduação. Universidade Federal do Rio Grande do Sul.

[FRI 99] FRIDRICH, J.; GOLJAN, M. **Protection of Digital Images Using Self Embedding**. 1999. Symposium on Content Security and Data Hiding in Digital Media. New Jersey Institute of Technology, Newark, NJ, USA.

[JEL 00] JELLINEK, Brigitte. **Invisible Watermarking of Digital Images for Copyright Protection**, 2000, 130 f. Dissertação. Universidade de Salzburgo. Disponível em: http://citeseer.ist.psu.edu/cache/papers/cs/31936/http:zSzzSzwww.horus.comzSz~bjellizSzunizSzbjelli-di-1.2.pdf/jellinek00invisible.pdf. Acesso em: abril 2008.

[JOH 93] JOHNSON, J.; JAYANT, N.; SAFRANEK, R. **Signal compression based models of human perception**. Proc. of the IEEE, 81:1385-1422, 1993.

[JOH 99] JOHNSON, N. F. **A introduction to watermarking recovery from images**. Proc. of the SANS. Intrusion Detection and Response Conference - (IDR'99), pages 9-13, 1999.

[KAT 00] KATZENBEISSER, Stefan; PETITCOLAS, Fabien A. P. **Information Hiding Techniques for Steganography and Digital Watermarking**. Artech House. 2000.

[KIM 01] KIM, H. Y. **Marcas d'água frágeis de autenticação para imagens em tonalidade contínua e esteganografia para imagens binárias e meio-tom**. RITA, 8(1), 2001.

[KOM 88] KOMTSU, N.; TOMINAGA, H. **Authentication system using concealed images in telematics**. Memoirs of the School of Science and Engineering, 52:45-60, 1988.

[MAC 03] MACHADO, Marlon Gaspar. **Transport Layer Security**. 2003. Grupo de Teleinformática e Automação. Universidade Federal do Rio de Janeiro. Disponível em: http://www.gta.ufrj.br/grad/01_2/tls. Acesso em: maio 2008.

[REY 02] REY, Christian; DUGELAY, Jean-Luc. **A Survey of Watermarking Algorithms for Image Authentication**. 2002. EURASIP Journal on Applied Signal Processing. Pages 613-621. 6º edition.

[PRO 97] PROKOPETZ, Klaus. **Watermark em Documentos Eletrônicos para Proteção de Direitos de Autor**. 1997. 38 f. Universidade Federal do Rio Grande do Sul.

[RUB 07] RUBIN, Vinícius. **Análise de Marca D'água Digital em Imagens Não Compactadas**. 2007. 50 f. Trabalho de graduação. Universidade Federal do Rio Grande do Sul.

[WAL 95] WALTON, S. **Information Authentification for a Slippery New Age**. 1995. Dr. Dobbs Journal, vol. 20, nº 4.

[WON 01] WONG, Peter H. W.; et al. **A Data Hiding Techniques in JPEG Compressed Domain**. 2001. Disponível em: http://citeseer.ist.psu.edu/609998.html. Acesso em: agosto 2008.

[ZHA 03] ZHAO, Yang. **Dual Domain Semi-fragile Watermarking for Image Authentication**. 2003. 118 f. Dissertação de mestrado. Departamento de Engenharia Elétrica e de Computação. Universidade de Toronto, Toronto. Disponível em:

http://www.ece.tamu.edu/~deepa/theses/zhao03.pdf. Acesso em: março 2008.

[ZHU 96] ZHU, B.; et al. **Transparent robust image watermarking**. SPIE, Conference on Visual Communications and Image Processing, 1996.