XXIV CONGRESSO NACIONAL DO CONPEDI - UFMG/FUMEC/DOM HELDER CÂMARA

DIREITO, INOVAÇÃO, PROPRIEDADE INTELECTUAL E CONCORRÊNCIA

MARALUCE MARIA CUSTÓDIO

JOÃO MARCELO DE LIMA ASSAFIM

D598

Direito, inovação, propriedade intelectual e concorrência [Recurso eletrônico on-line] organização CONPEDI/ UFMG/FUMEC/Dom Helder Câmara;
coordenadores: Maraluce Maria Custódio, João Marcelo de Lima Assafim – Florianópolis: CONPEDI, 2015.

Inclui bibliografia
ISBN: 978-85-5505-122-7
Modo de acesso: www.conpedi.org.br em publicações
Tema: DIREITO E POLÍTICA: da vulnerabilidade à sustentabilidade

1. Direito – Estudo e ensino (Pós-graduação) – Brasil – Encontros. 2. Inovação. 3. Propriedade Intelectual. 4. Concorrência. I. Congresso Nacional do CONPEDI - UFMG/FUMEC/Dom Helder Câmara (25. : 2015 : Belo Horizonte, MG).

CDU: 34

CONPEDI
Conselho Nacional de Pesquisa e Pós-Graduação em Direito

Florianópolis – Santa Catarina – SC
www.conpedi.org.br

XXIV CONGRESSO NACIONAL DO CONPEDI - UFMG/FUMEC /DOM HELDER CÂMARA

DIREITO, INOVAÇÃO, PROPRIEDADE INTELECTUAL E CONCORRÊNCIA

Apresentação

Apresentação não realizada pelos Coordenadores do GT.

PROPRIEDADE INTECTUAL NAS EMPRESAS E A PROTEÇÃO DE IMAGENS DIGITAIS POR MEIO DE MARCAS DÁGUA INVISÍVEIS

INTELLECTUAL PROPERTY ON ENTERPRISES AND THE DIGITAL IMAGES PROTECTION BASED ON INVISIBLE WATERMARKING

Cinthia O. A. Freitas

Resumo

Nos dias atuais é possível criar e distribuir conteúdo digital de maneira rápida e barata. A preocupação está no uso indevido ou não autorizado deste conteúdo. A necessidade de proteger a propriedade intelectual de conteúdos, em especial de imagens digitais, é o foco do artigo. O artigo apresenta a propriedade intelectual sob a ótica da segurança das informações nas empresas e a proteção das imagens digitais por meio das marcas d´água. Apresenta-se a conceituação de imagem digital e também os conceitos de esteganografia, criptografia, marcação de autoria de modo a evitar confusões de terminologia. A marcação de autoria associada à criptografia estabelece um conjunto de técnicas para permitir que o conteúdo digital seja verificado e constatado o uso indevido e/ou não autorizado.

Palavras-chave: Propriedade intelectual, Direito autoral, Novas tecnologias, Marca dágua, marcação de autoria, Imagem digital

Abstract/Resumen/Résumé

Nowadays it is possible to create and distribute digital content quickly and cheaply. The concern is the improper or unauthorized use of this content. The need to protect the intellectual property of content, especially digital images, is the focus of the paper. The paper presents the intellectual property from the perspective of information security on enterprises and the protection of digital images through watermarks. It presents digital image concepts and also the concepts of steganography, encryption, copyright marking in order to avoid terminological confusion. The copyright marking associated with encryption establishes a set of techniques to allow the digital content verification of improper or unauthorized use.

Keywords/Palabras-claves/Mots-clés: Intellectual property, Copyright law, New technologies, Watermarking, Copyright marking, Digital image

1. INTRODUÇÃO

No contexto da Internet, a qual tornou possível a disponibilização de conteúdos *online*, toma-se como facilitado o acesso e a busca dos mais variados tipos de conteúdos por todos que possuem computador, celular, *tablet* ou *smartphone*. Desta forma, o fato de que ilimitadas reproduções podem ser geradas sem as devidas autorizações, tem causado preocupações tanto às pessoas que produzem o material digital quanto às empresas que podem ser proprietárias de conteúdo digital e, portanto, necessitam proteger tal contéudo.

A necessidade de proteção advém para assegurar o Direito de Autor em, por exemplo, imagem e vídeo digitais. O artigo foca a propriedade intelectual sob a ótica da segurança das informações nas empresas e a proteção das imagens digitais por meio das marcas d´água (*watermarking*).

O tema realcioando com as iamgens digitais ter por motivação, por exemplo, a quantidade de imagens veiculadas na rede social Instagram (https://instagram.com), a qual completou 4 anos em 2014 e foi desenvolvida pelo brasileiro Mike Krieger e pelo americano Kevin Systrom, estreando na App Store (loja virtual da Apple) em 2010. Alcançou 1 milhão de usuários de dezembro de 2010. Em 2012, foi comprada pelo Facebook por US$ 1 bilhão. Em 2015, alcançou 30 milhões de usuários ativos. Mas não são estes números que motivam este artigo e, sim, a quantidade de imagens digitais postadas na rede social, ou seja, 55 milhões de imagens por dia. As imagens totalizam 1,2 bilhões de *likes* por dia. Sob um olhar simplificado, pode-se afirmar que o mundo digital é uma grande fotografia.

Neste contexto em que a associação entre dispositivos móveis com câmeras digitais e aplicativos especializados, a frase do filósofo chinês Confúcio, “Uma imagem vale por mil palavras” nunca foi tão real. Surge então a problemática relacionada à segurança da informação, no caso em questão deste artigo às imagens digitais e ao seu conteúdo propriamente dito. Interessa às empresas criar imagens digitais e ter a certeza de que tais imagens não serão copiadas, modificadas ou adulteradas, seja com interesses comerciais ou para fins ilícitos.

A segurança da informação na Internet tem três conceitos básicos, a saber: confidencialidade, integridade e disponibilidade (BOWEN et al., 2006, p. 75). Os autores apresentam tais conceitos como sendo

> Confidentiality: Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.

> Integrity: Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.
> Availability: Ensuring timely and reliable access to and use of information.

Entende-se, portanto, que por meio da confidencialidade toda a informação deve ser protegida de acordo com o grau de sigilo de seu conteúdo, visando à limitação do seu acesso e uso apenas às pessoas para quem as informações são destinadas. A integridade, por sua vez garante que toda informação deve ser mantida na mesma condição em que foi disponibilizada pelo seu proprietário, visando protegê-las contra alterações indevidas, intencionais ou acidentais. E, por último, a disponibilidade assegura que toda informação gerada ou adquirida por um indivíduo ou instituição deve estar disponível aos seus usuários no momento em que os usuários necessitem das informações para qualquer finalidade.

Para proteger tais conceitos, é vital que sejam implantados sistemas de identificação dos usuários e, também, implementados controles de segurança, assegurando assim a conexão entre sistemas e a transmissão de dados entre sistemas. Marcon Jr. (2010, p. 55) explica que

> O esquema de segurança computacional necessita preservar as propriedades básicas: confidencialidade, integridade, disponibilidade, autenticidade e não repúdio. Além disto, alguns princípios devem ser considerados: responsabilização dos autores por suas ações fornecimento do mínimo de privilégios possível para o desempenhar de uma atividade minimização (da quantidade, do tamanho e da complexidade) dos componentes confiáveis do sistema e priorização do modo de operação seguro durante a implantação e utilização do sistema.

Para tal, agregam-se outros três elementos à segurança da informação, a saber: identificação, autorização e não-repúdio (do inglês, *authentication*, *authorization*, e *nonrepudiation*). A identificação permite, por meio de mecanismos informáticos, aferir o acesso aos dados somente a aqueles que possuem a devida autorização para fazê-la. O conceito mais importante neste contexto é o não repúdio, ou seja, garantir a irretratabilidade (não-repúdio) que consiste na não negação de um ato prévio (ALJIFRI e NAVARRO, 2003, p. 1), seja este ato, por exemplo, negar falsamente a criação de um documento, armazenamento de dados ou assinatura de um documento eletrônico por meio de assinatura digital (FREITAS et al., 2011, p. 167).

Cabe, portanto, o seguinte questionamento: como garantir estas características nas imagens digitais? A busca por meios cada vez mais eficientes e eficazes de proteção e garantia de propriedade de imagens digitais é um campo de pesquisa interessante e, portanto, entram em cena contra-medidas que envolvem a aplicação de técnicas de marcas d'água (*watermarking*) e de identificação por digitais (*fingerprinting*). Tais medidas integram o

estudo da Marcação de Autoria (*Copyright Marking*), área inserida no estudo da Ocultação de Conteúdo (*Information Hiding*). Este artigo trata das marcas d'água e apresenta como este tipo de solução técnica pode auxiliar na garantia do Direito de Autor. Portanto, no caso em questão, a proteção de direitos autorais diz respeito à identificação positiva de propriedade de um determinado conteúdo, a fim de proteger os direitos do proprietário, sendo as marcas d'água utilizadas para auxiliar tal proteção.

Tem-se inicialmente que a propriedade intelectual divide-se entre os direitos autorais e conexos, e a propriedade industrial, regulada no Brasil pelo Instituto Nacional da Propriedade Industrial (INPI). Porém, nem toda produção intelectual é merecedora de proteção, seja por Direito de Autor ou por meio de Patente, o qual gera os denominados direitos intelectuais (BARBOSA, 2010, p.1883). No Brasil os Direitos de Autor são regulados pela Constituição Federal, pelo Direito Civil e, ainda, pela Lei de Direitos Autorais - Lei No. 9.610/98 (BRASIL, 1998), a qual protege o autor e sua obra seja esta artística ou literária.

Considerando-se o exposto, o artigo é resultado de método dedutivo de pesquisa e se propõe a apresentar e discutir o Direito de Autor relacionado às imagens digitais no âmbito empresarial, apresentando soluções técnicas e comprováveis juridicamente em casos de litígio. O estudo aborda as técnicas de marcas d'água, explicando a área de Marcação de Autoria e as categorias de marcas d'água: visíveis e invisíveis. O interesse recai sobre as marcas invisíveis e os métodos de comprovação de uso indevido ou não autorizado, visto que tais técnicas e métodos são pouco conhecidos. Busca-se a integração entre o Direito e a Tecnologia, sendo a Tecnologia meio para auxiliar o Direito em questões relacionadas à propriedade intelectual e ao Direito de Autor em imagens digitais.

2. IMAGENS DIGITAIS E USO INDEVIDO OU NÃO AUTORIZADO

De um modo simplificado, pode-se definir imagem digital como a representação de uma imagem bidimensional utilizando-se números binários (0 ou 1) codificados de modo a permitir o armazenamento, transferência, impressão, reprodução e, ainda, o processamento por meio de métodos e técnicas computacionais ou meios eletrônicos, por exemplo, câmeras digitais, celulares e computadores.

De acordo com Marques Filho e Vieira Neto (1999, p. 19) tem-se que "uma imagem digital pode ser descrita matematicamente por uma função $f(x,y)$ da intensidade luminosa, sendo seu valor, em qualquer ponto de coordenadas espaciais (x,y), proporcional ao brilho (ou nível de cinza ou cor) da imagem naquele ponto". Os autores explicam que

> A função *f(x,y)* representa o produto da interação entre a iluminância *i(x,y)* - que exprime a quantidade de luz que incide sobre o objeto - e as propriedades de refletância ou de transmitância próprias do objeto, que podem ser representadas pela função *r(x,y)*, cujo valor exprime a fração de luz incidente que o objeto vai transmitir ou refletir ao ponto *(x,y)*.

Compreende-se destas explicações que uma imagem digital é uma matriz de pontos (representação matricial ou *raster*), sendo que cada ponto possui como características a iluminância e a refletância. A iluminância descreve a quantidade de luz que atravessa ou é emitida de uma superfície em questão e a refletância é a proporção entre o fluxo de radiação eletromagnética incidente numa superfície e o fluxo que é refletido (MARQUES FILHO e VIEIRA NETO, 1999, p. 21-25).

Imagens digitais geralmente são armazenadas em arquivos com pixels (*pictory element*) de tamanho entre 8-bit a 24-bit (bits por pixel). Desta forma, uma imagem com 24-bits oferecerá maior espaço para esconder informações e permitirá que o conteúdo cifrado na imagem não seja percebido pelo olho humano.

Visando a padronização das imagens foram criados os modelos de cores.Um modelo de cor facilita a especificação de cores respeitando um padrão de representação. Além de o modelo representar a cor propriamente dita (que também pode ser em níveis de cinza ou preto&branco), representa também os relacionamentos das cores entre si. Mais especificamente, um modelo de cor é uma especificação de um sistema de coordenadas tridimensionais e um subespaço dentro deste sistema onde cada cor é representada por um único ponto.

Diferentes sistemas de processamento de imagem utilizam diferentes modelos de representação de cores. Dentre os modelos mais utilizados no mercado encontram-se: RGB (*Red, Green, Blue*), CMY (*Cian, Magenta, Yellow*), HSV (*Hue, Saturation, Value*) ou HSI (*Hue, Saturation, Intensive*), HSL (*Hue, Saturation, Lightness*). A escolha de um modelo de cor para um determinado sistema depende de diversas variáveis, como por exemplo: área de atuação do sistema, tempo necessário para o processamento de imagens, informações relevantes da imagem para tratamento, condições ideais para o algoritmo de tratamento de imagens, entre outras. Os modelos mais usados para imagens coloridas são o RGB e o HSV, os quais são utilizados pelos computadores e demais equipamentos eletrônicois (monitores coloridos e câmeras digitais) (GONZALEZ e WOODS, 2002, p. 282-348).

A partir da conceituação teórico-matemática de imagens digitais e, ainda, levando em consideração que na rede social Facebbok são postadas “300 milhões de imagens por dia, o

que perfaz um total de 109,5 bilhões de fotos publicadas na rede social num ano" (MACHADO, 2013, p. 01), surge o questionamento: como garantir a autoria de imagens e proteger o a produção intelectual das empresas e pessoas?

Inicialmente, deve-se levar em consideração que o uso indevido de imagens pode ocorrer em dois contextos distintos, a saber: o pessoal e o profissional. No contexto pessoal, o uso indevido ocorre quando outras pessoas fazem uso das imagens para fins comerciais ou não, apresentando a imagem como de autoria própria. Além disto, podem associar à imagem comentários caluniosos ou difamatórios, sendo que em alguns casos o uso pode ser a divulgação de pornografia, dependendo da cena mostrada na imagem e do contexto (cenário). E, ainda, pode ocorrer das pessoas serem "marcadas" em fotos comprometedoras, o que pode afetar não somente a vida pessoal, mas também profissional.

No contexto profissional, as imagens são utilizadas sem o devido ressarcimento e também podem ser modificadas para criar imagens fraudulentas. Outro ponto relevante é o repasse de segredos industriais ou empresariais por meio de imagens, as quais podem invalidar ou mesmo atrapalhar lançamento de produtos, projetos e criações.

Su et al. (1999, p. 2) já alertavam as imagens digitais apresentam vantagens, mas criam problemas para as partes que pretendam impedir a reprodução e distribuição não autorizada de dados digitais importantes e valiosos, tais como, protegidos por direitos autorais, documentos comerciais, privilegiados, sensíveis e/ou secretos. Os autores apresentam que existem dois métodos para proteção de documentos: a criptografia (*encryption*) e a proteção contra cópias (*copy protection*). No entanto, uma vez descriptografado, um documento pode ser copiado e distribuído facilmente, e mecanismos de proteção contra cópia muitas vezes pode ser contornados. Neste sentido, os autores apresentam que medidas de salvaguarda contra falhas de criptografia e/ou proteção contra cópia, envolvem a aplicação de marcas d'água digitais visando criar uma "última linha de defesa" contra a distribuição não autorizada de mídias digitais. Entra em cena a Marcação de Autoria (*Copyright Marking*).

3. MARCAÇÃO DE AUTORIA E MARCAS D'ÁGUA

A esteganografia é uma das técnicas conhecidas para mascarar informações e Su et al. (1998, p. 688) apresentam que um sistema digital de marcas d'água incorpora informações diretamente em um documento, ou seja, esconde informações relacionadas a autoria do

documento ou imagem digital, podendo-se citar como exemplos: nome da empresa, data e hora da criação da imagem, destinatinatário da imagem, entre outros dados.

Historicamente, a estaganografia foi aplicada em diversas situações tais como mensagens cifradas em tempos de guerra, mas sua origem remonta o ano de 440 a.C. com Herodotus, filósofo grego que deu exemplos da técnica em seu livro *A História de Herodotus*, onde o personagem principal, Demeratus, escreve um aviso de um ataque à Grécia numa placa de madeira e a cobre com cera" (DUARTE et al., 2015, p. 4). Relatam os autores, que "Outro antigo exemplo foi o de Histiaeus, que raspou sua cabeça e tatuou uma mensagem. Depois que seu cabelo cresceu, a mensagem que continha dados de um plano de revolta contra os persas ficou assim escondida" (DUARTE et al., 2015, p. 4). Muitos anos depois, na Segunda Guerra Mundial, " os alemães inventaram os micropontos, que nada mais eram do que pequenos pontos impressos que, quando ampliados, possuíam a clareza de páginas datilografadas em tamanho normal" (DUARTE et al., 2015, p. 4). Um exemplo, é a mensagem enviada por um espião alemão durante a 2ª. Guerra Mundial que dizia: "Apparently neutral's protest is thoroughly discounted and ignored. Isman hard it. Blockade issue affects pretext for embargo on by-products, ejecting suets and vegetable oils". Usando somente a segunda letra de cada palavra é possível forma a seguinte frase: "*Pershing sails from NY June 1*"[1].

Diferentemente da criptografia, a qual permite a transmissão cifrada de conteúdos (texto, imagens, vídeos) entre interessados prevenindo o acesso do conteúdo por meio da aplicação de chaves (simétrica ou assimétrica0 (EFING; FREITAS, 2008), a esteganografia apresenta-se como uma alternativa à proteção de dados por meio do ocultamento da totalidade do conteúdo ou do ocultamento de dados e informações. Assim, Petittcolas et al. (1999, p. 1062) explicam que "enquanto a criptografia se preocupa em proteger o conteúdo da mensagem, a esteganografia trata do ocultamento da existência da mesma". Os autores, ampliam a definição de esteganografia quando afirmam que um significado mais amplo para a palavra poderia ser definido como uma informação que é oculta em outra informação (PETITCOLAS et al., 1999, p. 1062). Atualmente a esteganografia não está esquecida, apenas vem se adaptando para agregar os conhecimentos das novas tecnologias, especialmente da área de Informática.

3.1. Marcação de Autoria

[1] Disponível em: <http://www.jjtc.com/stegdoc/sec202.html> Acesso em 30 jul. 2015.

Inicialmente, deve-se considerar a classificação apresentada por Petitcolas et al. (1999, p. 1063), a qual apresenta o esquema de derivação das áreas relacionadas à ocultação de conteúdo, de modo a especificar as técnicas envolvidas (Figura 01). Esta classificação tem o objetivo de evitar confusões entre termos e técnicas, erroneamente utilizadas na literatura, visto que os termos ocultação de informação (*Information Hiding*), esteganografia (*Steganography*) e marcação de autoria (*Copyright Marking*) são muitas vezes utilizados como sinônimos. Petitcolas et al. (1999, p. 1063) esclarecem que a marcação de autoria é o oposto da esteganografia, visto que tais técnicas apresentam a característica de robustez contra alteração ou destruição das marcas d'água.

Esclarece-se também que este artigo utiliza o termo conteúdo para exemplificar tanto texto, como imagens, videos, músicas, entre outros conteúdos que podem ser ocultados dentro de arquivos digitais. Ressalta-se que o artigo trata da derivação pelo caminho: marcação de copyright/marcação robusta/marca d'água.

Assim, os dois tipos de marca d'água classificadas na literatura são assim denominadas: visível e invisível ou transparentes (PETITCOLAS et al., 1999, p. 1063). As marcas d'água visíveis são aquelas, que como a própria denominação indica, são visíveis, ou seja, pode-se facilmente identificar o nome da empresa a que pertence determinado texto, documento ou imagem. Estas marcas são comparáveis as filigranas utilizadas em papéis, sendo que sua origem surgiu no século XIII com a finalidade de diferenciar os fabricantes de papel da época (PETITCOLAS et al., 1999, p. 1063). Atualmente, as marcas visíveis aplicadas em documentos digitais constituem padrões visuais, por exemplo a logomarca de uma empresa, sobrepostas às imagens digitais. Por outro lado, as marcas invisíveis são aquelas que não são facilmente detectáveis à olho nu. Tais marcas encontram-se ocultadas no conteúdo original. Importante destacar que ambas as marcas têm o interesse de informar quem é o proprietário do conteúdo (PETITCOLAS et al., 1999, p. 1064).

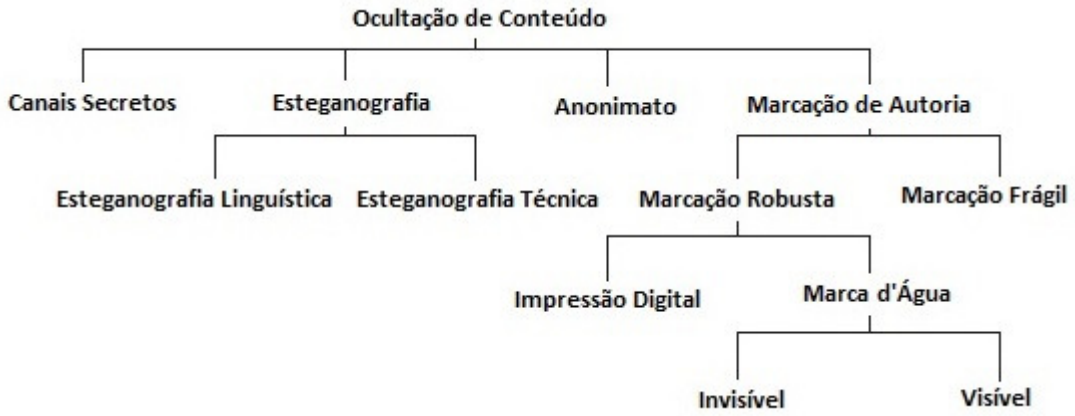

Figura 01: Classificação das Técnicas de Ocultação de Conteúdo
(Adaptado de: PETITCOLAS et al., 1999, p. 1062).

Observa-se, de acordo com a Figura 01, que estes tipos de marcas d'água derivam da marcação dita robusta, a qual tem a propriedade de não ser exeqüível removê-las ou torná-las inúteis sem que o conteúdo sofra alteração ou destruição. Isso significa que a marca deve ser incorporada aos componentes mais perceptivelmente significativos do conteúdo, ou seja, nos componentes que realmente carregam informação relevante (PETITCOLAS et al., 1999, p. 1064). A marcação frágil é aquela em que a marca é destruída logo que o objeto é modificado ou alterado, sendo que Petitcolas et al. (1999, p. 1064) apontam que esta característica pode ser útil quando o interesse é demonstrar, em caso de litígio, que um determinado conteúdo não sofreu adulterações.

Deste modo, as marcas d'água apresentam diversas propriedades, as quais fazem deste recurso uma solução ponderosa, a saber (Su et al, 1999, p. 688-689):

- Robustez: A marca d'água deve ser detectável após alterações ocorridas no conteúdo que a contém. Robustez significa que a marca d'água deve ser de difícil retirada ou destruição. O ideal é que seja impossível violar uma marca d'água sem degradar o conteúdo severamente ou tão severamente que o conteúdo não seja mais útil ou não tenha mais valor comercial;
- Imperceptibilidade ou um baixo grau de impertinência: esta característica visa preservar a qualidade do documento que contém a marca d'água, sendo que a marca d'água inserida no conteúdo não pode distorcer visivelmente o conteúdo original (ou não pode alterar a audibilidade ou inteligibilidade de conteúdos musicais). Idealmente, os documentos, original e com marcas d'água, devem ser perceptivelmente idênticos;
- Segurança: Partes não autorizada não devem ser capaz de ler ou alterar a marca d'água. Idealmente, a marca d'água não deve ser detectável por pessoas não autorizadas;
- Não referência ao documento original: dependendo da aplicação é necessário recuperar a marca d'água sem a necessidade de se possuir o documento original não marcado;
- Múltiplas marcas d'água: Pode ser interessante incorporar mais de uma marca d'água ao conteúdo. Por exemplo, em uma determinada música pode-se inserir diferentes

melodias em diferentes trechos da gravação do áudio que contém direitos autorais reservados. Outro exemplo, aplicado em imagens digitais, é a inserção de uma nova marca d'água a cada *download* do conteúdo;

- Não ambigüidade: A marca d'água deve transmitir informações inequívocas sobre o legítimo proprietário, ponto de distribuição (por exemplo, se a imagem foi baixada do *site A* ou do *site B*), entre outras informações. As informações veiculadas na marca d'água não podem gerar confusão e devem garantir a verificação de autoria.

Tais características podem aferir às marcas d'água a segurança necessária, procurando evitar alterações para uso indevido ou não autorizado, por exemplo, quando o interesse é remover uma marca d'água visível para então utilizar o conteúdo como se fosse de própria autoria. O mesmo pode ocorrer, com marcas invisíveis, por meio da aplicação de algoritmos que busquem pela marca d'água. Este procedimentos não são simples, visto existirem diversas técnicas de marcação de autoria as quais podem ser implementadas com variações nos algoritmos.

Os algoritmos de marcação de autoria tem por base o conceito da inserção, ou seja, iserem, por exemplo, nos bits que são ruídos e pré-existem em conteúdos digitais por um texto ou outra imagem. A Figura 02 mostra como estes algoritmos funcionam marcando (a) ou recupernado (b) uma marca em um determinado conteúdo.

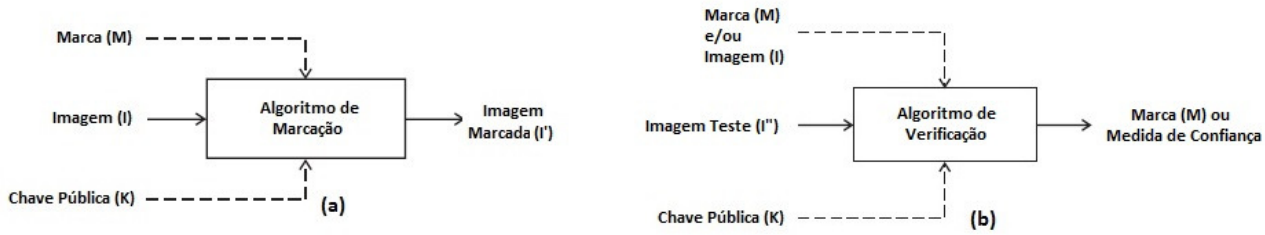

Figura 02: Esquema de Algoritmos de Marcação Robusta

As técnicas mais conhecidas de inserção para marcação de autoria em imagens digitais, apresentadas por Johnson e Jajodia (1998, p. 28) são as seguintes: Inserção no bit menos significativo (*least significant bit insertion - LSB*); técnicas de filtragem e mascaramento (*masking and filtering*) e algoritmos e transformações (*algorithms and transformations*). Não é objetivo do artigo explicar tecnicamente como cada uma destas técnicas funcionam, mas ressaltar que outros pesquisadores e trabalhos podem ser consultados para um melhor entendimento (BANDYOPADHYAY et al., 2010) (CHANNALLI e JADHAV, 2009).

Em termos de classificação, de acordo com Petitcolas et al. (1999, p. 1064), pode-se ainda subdividir as marcas de autoria em três subcategorias: sem chave, com chave simétrica

e com chave assimátrica ou par de chaves (privada e pública) (EFING e FREITAS, 2008, p.132-136).

Uma marca de autoria sem chave é aquela que não precisa de chave para ser utilizada. Pode ser útil para detectar as alterações não intencionais em imagens, por exemplo, erros de transmissão ou de armazenamento. Caso o algoritmo de verificação esteja disponível publicamente, qualquer pessoa pode inserir este tipo de marca em qualquer imagem e, ainda, qualquer pessoa pode verificar se uma imagem contém uma marca válida.

A marca de autenticação com chave simétrica é usada para detectar alterações intencionais ou maliciosas. Este tipo de marca é similar ao mecanismo aplicado em assinaturas digitais com chave simétrica para cifragem de conteúdo, por exemplo, emails e documentos. Chaves simétricas são aplicadas tanto para cifrar quanto para decifrar conteúdos. A diferença é que para marcação de inagens digitais o código de autenticação está inserido na imagem ao invés de ser armazenado separadamente. Os algoritmos para inserção e verificação deste tipo de marca podem ser disponibilizados publicamente.

Finalmente, as marcas de autoria basedas em chaves assimétricas utilizam om emso mecanismo da criptografia com base em um par de chaves: uma privada e outra pública. Este tipo de chave permite que a autoria e autencidade de uma imagem digital possam ser verificadas sem que nenhuma informação privada seja revelada, portanto, constituem o mecanismo mais seguro para aplicar em marcação de autoria em imagens digitais.

3.2. Ataques sobre Marcas d'Àgua

Qualquer sistema ou técnica computacional não é 100% seguro. Todo procedimento está sujeito a falhas, sendo que no caso específico de marcação de autoria por meio de marcas d'água pode-se entender que, apesar da grande variedade de técnicas, algumas técnicas são mais seguras e robustas que outras. Portnato, os problemas surgem desde falhas inerentes aos procedimentos de marcação de autoria, ou seja, falhas computacionais até a aplicação de marcas d´água que podem ser quebradas ou detectadas.

A quebra ou detecção de uma marca d'água permite que os conteúdos digitais sejam utilizados para fins comerciais ou outros interesses sem que se tenha a alteração ou destruição das marcas d'água. ou não mesmo sem autorização.

A literatura científica apresenta diversas classicações para os procedimentos de quebra de marcas d'água, tecnicamente denominados de ataques (*attacks*) (CRAVER et al., 1998) (VOLOSHYNOVSKIY et al., 2001) (BOUNKONG et al., 2003).

De um modo geral, em um primeiro nível consdierando a intenção, os ataques são classificados em maliciosos ou não. Os ataques não maliciosos constituem métodos comuns de processamento de imagens e não estão destinados a eliminar ou interferir na marca d'água. Por outro lado, os ataques maliciosos, são tentativas deliberadas de remover e/ou desativar a marca d'água, sendo que na muitas vezes são aplicados os mesmos algoritmos de inserção das marcas. Cabe destacar que alguns tipos de ataques não maliciosos também podem ser usados como ataques maliciosos, especialmente se o processo de marca d'água é fraco e não resistente ao ataque.

Outra classificação tem por base explorar falhas nas características das marcas d'água, já apresentadas anteriormente. Assim, os ataques podem ser ditos de: robustez, apresentação, interpretação. O ataque de robustez visa diminuir ou eliminar a presença de uma marca de água digital. O ataque de apresentação modifica o conteúdo de maneira que o método de verificação não mais consegue localizar a marca d'água. E, o ataque de interpretação atua de maneira que o atacante concebe uma situação, a qual passa a impedir a confirmação da autoria e, consequentemente, da propriedade.

Em casos de litígio em que a propriedade de determinada imagem digital é questionada, deve-se como boa prática analisar se a imagem possui algum procedimento de marcação de autoria para então analisar se houve ou não ataque sobre a marca d'água e que alterações foram geradas na imagem original, muitas vezes com a intenção de disfarçar tanto o ataque quanto o uso e aplicação da imagem em outro contexto.

A aplicação de marcas d'água tem múltiplos usos, entre estes usos a prova de propriedade e a autenticação e verificação da integridade do conteúdo são os que mais se destacam, visto que uma marca d'água íntegra revela que o conteúdo não foi modificado.

4. A LEGISLAÇÃO PERTINENTE E AS IMAGENS DIGITAIS

Pergunta-se, então: A quem pertence à autoria de uma imagem digital? Inicialmente deve-se retroceder no tempo e analisar a fotografia, a qual é protegida pela Lei de Direito Autoral, Lei N^{o} 9.610 de 1998 (BRASIl, 1998), sendo que no art. 7º, inciso VII, tem-se que:

> Art. 7º São obras intelectuais protegidas as criações do espírito, expressas por qualquer meio ou fixadas em qualquer suporte, tangível ou intangível, conhecido ou que se invente no futuro, tais como:
> ...

> VII - as obras fotográficas e as produzidas por qualquer processo análogo ao da fotografia;

E o legislador já prevendo que os avanços tecnológicos também influenciariam o modo como são registradas as imagens, considerou a expressão "processo análogo ao da fotografia" equiparando, portanto, o negativo ao cartão de memória, seja em câmera digital ou em celular ou *smartphone*. Sobre a utilização da obra fotográfica, o art. 79º, dispõe que:

> Art. 79. O autor de obra fotográfica tem direito a reproduzi-la e colocá-la à venda, observadas as restrições à exposição, reprodução e venda de retratos, e sem prejuízo dos direitos de autor sobre a obra fotografada, se de artes plásticas protegidas.

O parágrafo 1º deste artigo indica que "A fotografia, quando utilizada por terceiros, indicará de forma legível o nome do seu autor". É o que se observa nos jornais veiculados pela Internet, nos quais ao lado da imagem é mostrado o nome do autor da imagem seguido do nome do meio de comunicação para qual a imagem foi gerada, criada ou capturada.

O parágrafo 2º esclarece que "É vedada a reprodução de obra fotográfica que não esteja em absoluta consonância com o original, salvo prévia autorização do autor". Portanto, toda obra somente pode ser reproduzida com alterações se o autor assim autorizar.

Os direitos inalienáveis do autor são denominados de direitos morais e de acordo com o art. 24º da lei de Direito Autoral (BRASIL, 1998), o autor de obra intelectual tem os seguintes direitos resguardados:

> I – o de reivindicar, a qualquer tempo, a autoria da obra;
> II – o de ter seu nome, pseudônimo ou sinal convencional indicado ou anunciado, como sendo o do autor, na utilização de sua obra;
> III – o de conservar a obra inédita;
> IV – o de assegurar a integridade da obra, opondo-se a quaisquer modificações ou à prática de atos que, de qualquer forma, possam prejudicá-la ou atingi-lo, como autor, em sua reputação ou honra;
> V – o de modificar a obra, antes ou depois de utilizada;
> VI – o de retirar de circulação a obra ou de suspender qualquer forma de utilização já autorizada, quando a circulação ou utilização implicarem afronta à sua reputação e imagem;
> VII – o de ter acesso a exemplar único e raro da obra, quando se encontre legitimamente em poder de outrem, para o fim de, por meio de processo fotográfico ou assemelhado, ou audiovisual, preservar sua memória, de forma que cause o menor

> inconveniente possível a seu detentor, que, em todo caso, será indenizado de qualquer dano ou prejuízo que lhe seja causado.
>
> § 1º Por morte do autor, transmitem-se a seus sucessores os direitos a que se referem os incisos I a IV.
>
> § 2º Compete ao Estado a defesa da integridade e autoria da obra caída em domínio público.
>
> § 3º Nos casos dos incisos V e VI, ressalvam-se as prévias indenizações a terceiros, quando couberem.

Depreende-se deste artigo, portanto, que os créditos ao autor devem sempre mencionados. Além disto, ao se proceder a venda de imagens em mídia eletrônica (CD, DVD, site na Internet), os autores devem assegurar-se da integridade da obra informando se a obra pode ou não ser modificada, bem como, esclarecendo que o uso da obra não poderá prejudicar ou atingir o autor em sua reputação ou honra. Ressalta-se, de acordo com o inciso VI, que o autor pode solicitar a retirada de imagem de sua autoria cujo o uso não esteja de acordo com seus objetivos. Por exemplo, se alguém utilizar uma imagem em site de pornografia infantil ou site de apologia ao racismo ou nazismo, sendo que o autor desconhecia esta finalidade, o autor pode solicitar a retirada de veiculação da imagem.

Como mencionado, os direitos inalienáveis do autor são denominados de direitos morais e estão garantidos no art. 27º, a saber: "Art. 27. Os direitos morais do autor são inalienáveis e irrenunciáveis". Direitos morais não podem ser vendidos, repassados ou qualquer outra modalidade à pessoa alguma. Tais direitos são do autor e não pertencem ou poderão pertencer a mais ninguém. Portanto, os direitos patrimoniais estão estabelecidos nos arts. 28º ao 45º, sendo que somente o autor tem o direito de "utilizar, fruir e dispor da obra literária, artística ou científica". Utilizar, reproduzir, editar, adaptar, traduzir, ou distribuir depende de autorização prévia e expressa do autor. Nesta mesma condição está "a inclusão em base de dados, o armazenamento em computador, a microfilmagem e as demais formas de arquivamento do gênero" (art. 29º, inciso IX). No art. 44º fica estabelecido que "O prazo de proteção aos direitos patrimoniais sobre obras audiovisuais e fotográficas será de setenta anos, a contar de 1° de janeiro do ano subseqüente ao de sua divulgação".

A lei estabelece também, no art. 46°, as condições em que a reprodução, a citação, o apanhado, a utilização de obras, a representação teatral, a execução musical e a utilização para produzir prova judiciária ou administrativa; não constituem ofensa aos direitos autorais.

Outra preocupação é o Direito de Imagem, quando a imagem contém pessoas ou objeto de autoria conhecida. Tanto a pessoa quanto o responsável ou autor do objeto necessitam

permitir o uso da imagem, por meio de uma licença de uso de imagem, especificando o meio (onde) e o tempo (período) em que a imagem será utilizada ou veiculada (AFFORNALLI, 2007, p.55-58). O direito de imagem encontra-se assegurado e protegido pela Constituição Federal da República de 1988 no art. 5º, incisos X e XXVIII, tratado dentre os Direitos e Garantias Fundamentais e como um Direito de Personalidade (BRASIL, 1988). E, ainda, pelo Código Civil de 2002, Lei Nº 10.406/2002, como um direito de personalidade autônomo (art. 11º e seguintes), visto tratar-se da projeção da personalidade física da pessoa, incluindo traços fisionômicos, o corpo, atitudes, gestos, sorrisos, indumentárias, entre outros (BRASIL, 2002).

O direito de imagem possui as seguintes características: irrenunciabilidade, inalienabilidade, intransferibilidade; todas interligadas e decorrentes do caráter da indisponibilidade**.** Significar que a imagem da pessoa ou sua personalidade física jamais poderá ser vendida, renunciada ou cedida em definitivo, porém, poderá, sim, ser licenciada por seu titular a terceiros. Além disto, o direito de imagem possui a característica da imprescritibilidade, ou seja, não se extingue com o passar do tempo (AFFORNALLI, 2007, p. 50-55).

5. CONCLUSÃO

O uso de imagens digitais é crescente e as empresas possuem nas imagens capital intelectual de interesse econômico, social e ambiental, ao qual cabe proteção. O artigo apresentou o uso das marcas d'água em imagens digitais como meio para evitar o uso indevido e não autorizado das imagens, principalmente quando ocorrem alterações ou modificações visando descaracterizar a imagem original e não permitir a comprovação do uso indevido e/ou não autorizado.

Foi apresentada a terminologia técnico-científica correta, de modo a diferenciar esteganografia, criptografia e marcação de autoria. Entende-se que a aplicação de marcas d'água não pode por si só impedir a cópia, modificação e redistribuição de conteúdos digitais. No entanto, se os procedimentos de criptografia falharem, as marcas d'água permitem que o conteúdo seja verificado e constatado o uso indevido e/ou não autorizado.

Finalmente, entende-se que a combinação de técnicas podem auxiliar na marcação de autoria e garantir às empresas que as imagens criadas, geradas ou capturadas por elas não sejam alteradas ou modificadas para fins comerciais de outrem ou de degradação intencional a fim de atingir a empresa. "Uma imagem vale por mil palavras", é o que diz o provérbio chinês

do pensador Confúcio e, portanto, deve ser protegida visto que os danos decorrentes do uso indevido ou não autrorizado pode gerar danos à propria imagem da empresa.

REFERÊNCIAS

AFFORNALLI, Maria Cecília Naréssi Munhoz. Direito à Própria Imagem. 1a. ed. (2003) 5ª. Tir., Curitiba: Juruá. 2007.

BANDYOPADHYAY, Samir Kumar; PAUL, Tuhin Utsab; RAYCHOUDHURY, Avishek. **Invisible Digital Watermarking Through Encryption**. International Journal of Computer Applications (0975 – 8887), Vol. 4, Nº 8, aug., 2010. p. 18-20.

BARBOSA, Denis Borges. **Tratado da Propriedade Intelectual**. Tomo III. Editora Lumen Juris: Rio de Janeiro, 2010.

BOWEN, Pauline; HASH, Joan; WILSON, Mark. **Information Security Handbook: A Guide for Managers**. Recommendations of the National Institute of Standards and Technology, NIST Special Publication 800-100, oct., 2006.

BOUNKONG, Stéphane; TOCH, Borémi; SAAD, David; LOWE, David. **ICA forWatermarking Digital Images**. Journal of Machine Learning Research, Vol. 4, 2003. p.1471-1498.

BRASIL, Senado Federal. **Constituição Federal da República do Brasil**. 1988. Disponível em <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm> Acesso em 30 jul. 2015.

BRASIL, Senado Federal. Lei No. 9.610/1998. **Lei de Direitos Autorais**. 1998. Disponível em <http://www.planalto.gov.br/ccivil_03/leis/l9610.htm> Acesso em 30 jul. 2015.

BRASIL, Senado Federal. Lei No. 10.406/2002. **Código Civil Brasileiro**. 2002. Disponível em <http://www.planalto.gov.br/ccivil_03/leis/2002/L10406.htm> Acesso em 30 jul. 2015.

CHANNALLI, Shashikala; JADHAV, Ajay. **Steganography An Art of Hiding Data**. International Journal on Computer Science and Engineering, Vol.1(3), 2009, p.137-141.

CRAVER, Scott; YEO, Boon-Lock; YEUNG, Minerva. **Technical Trials and Legal Tribulations**. Communications of the A.C.M., Vol. 41, Nº 7, jul., 1998. p. 44-54.

EFING, Antonio C., FREITAS, Cinthia O. de A. **Direito e Questões Tecnológicas Aplicados ao Desenvolvimento Social**. Curitiba: Juruá, 2008.

FREITAS, Cinthia Obladen de Almendra; EFING, Antônio Carlos; Santin, Altair Olivo. **A Nuvem e o Agravamento dos Riscos: Necessidade de Reforço na Aferição da Irrefutabilidade**. In: Anais do V Congresso de Direito de Autor e Interesse Público (V CODAIP), 2011, Florianópolis. Livreto do V Congresso de Direito de Autor e Interesse Público. Florianópolis-SC: UFSC - Universidade Federal de Santa Catarina, Vol. 1, 2011. p.161-179.

GONZALEZ, Rafael C.; WOODS, Richard E. **Processamento de Imagens Digitais**. São Paulo: Edgard Blücher Ltda., 2000.

JOHNSON, Neil F.; JAJODIA, Sushil. **Exploring Steganography: seeing the unseen**. Journal Computer. Computing Practice, Vol. 31, Issue 2, February, 1998. p. 26-34.

MARCON JR., Arlindo; LAUREANO, Marcos; SANTIN, Altair; MAZIERO, Carlos. **Aspectos de segurança e privacidade em ambientes de computação em nuvem**. In: SIMPÓSIO BRASILEIRO EM SEGURANÇA DA INFORMAÇÃO E DE SISTEMAS COMPUTACIONAIS. MINICURSOS DO SBSEG. 10, 2010, Porto Alegre. Anais... Porto Alegre, RS: SBC, 2010. Disponível em: <http://dainf.ct.utfpr.edu.br/~maziero/lib/exe/fetch.php/research:2010-sbseg-mc.pdf> Acesso em 30 jul. 2015.

MACAHDO, André. Por ano, 125 bilhões de imagens são compartilhadas na rede. 2013. Disponível em <http://oglobo.globo.com/sociedade/tecnologia/por-ano-125-bilhoes-de-imagens-sao-compartilhadas-na-rede-8301345>Acesso em 30 jul. 2015.

MARQUES FILHO, Ogê; VIEIRA NETO, Hugo. **Processamento Digital de Imagens**, Rio de Janeiro:Brasport, 1999.

PETITCOLAS, Fabien A. P.; ANDERSON, Ross J.; KUHN, Markus G.. **Information Hiding: A Survey**. Proceedings of the IEEE: Special Issue on Protection of Multimedia Content, 87(7), July, 1999, p.1062-1078.

SU, Jonathan K.; HARTUNG, Frank; GIROD, Bernd. **Digital Watermarking of Text, Image, and Video Documents**. Computers & Graphics, Volume 22, Issue 6, December 1998, p. 687–695.