Global Information Assurance Certification Paper

Copyright protection and copy control when distributing and publishing digital information

Peter Bonne
GSEC Practical Version 1.4b, Option 1

Abstract

Lack of sufficiently strong copyright protection and copy control is one of the hindrances for increased use of Internet for publishing information where protection of copyright is a requirement and for distribution of information where copy control is a requirement.

What is the status of available of methods, techniques and products that may give protection and control, and what is the level of protection and control they can offer?

The current status of watermarking for copyright protection and Digital Right Management for copy control will be described and discussed.

Introduction

A number of elements to support the electronic society are already in place. Both companies and private individuals have these days access to networks with an ever-growing bandwidth and network infrastructure. This allows them to access large amounts of information and services on the web and via e-mail. Use of cryptographic techniques in PKI ensures confidentiality, authenticity and integrity in electronic transactions. This is used by many people worldwide on a daily basis to perform things like bank transactions and payments of goods electronically.

Common for many of these transactions are that they are carried out between parties where there already is established a level of trust (e.g. a bank and its customers) and where the main problem is to ensure safe communication between parties trusting each other. Here safe refers to that confidentiality, authenticity, integrity and non-repudiation is handled.

In other types of transactions there is not, and will not be established the level of trust as between a bank and its customer (Alice doesn't trust Bob and/or Alice wants to enforce limitations on what Bob can do with the information). However, it is still important that there is a level of control on what one of the parties is doing with the information received or made available from the other. The information may represent text, images, sound and movies. We will focus on text and images in this paper, but variants of the methods and techniques used for text and images are also often used for other digital information like sound and movies.

Examples of these kinds of transactions are purchase of information (e.g. e books) downloaded via Internet in digital representation and therefore easily manipulated and duplicated with computers or other devices that can read, copy and transform the received information unless there is some mechanism that control what the user can do with the information. Often there will be an intellectual property right and a commercial issue connected to the information, and the publisher and distributor therefore need to have influence and control over what the buyer is doing with the delivered digital information.

Another important area is when the information is not delivered from one part to the other but is published on the Internet available for anybody with access to Internet. Still there may be connected intellectual property rights to the published information, so the publisher needs to be able to trace and prove use that violates the intellectual property rights and copyrights.

Electronic invoice is another example. Existing techniques can take care of the integrity, authenticity and confidentiality of the electronic invoice when transmitted from supplier to customer, but in accounting there is also a requirement that all claimed expenses shall be documented with original invoices, not copies of invoices. The purpose is to prevent the same expense being accounted for in more than one organization's books. With paper invoices it is fairly difficult to make a copy that is not easily recognized as a copy, while a copy of an electronic invoice may be very difficult to distinguish from the original unless special precautions are taken or copying is prevented.

What does a potential publisher of images on the Internet and publisher/distributor of documents over the Internet have to assess before she/he can decide which techniques, methods and security products she/he should employ to ensure protection of copyrights of published information and control over copying of distributed documents?

There are two approaches used to ensure security and control when distributing and publishing information where intellectual right protection and copy control are major concerns:

1. Use of watermarking for copyright protection of information published on Internet
2. Establishing Digital Right Management Systems for copy control of distributed information.

This document gives an overview of watermarking and describes how different applications of watermarking and fingerprinting can be used to protect intellectual property rights when distributing and publishing information. Furthermore description of systems that are used for distribution of information when copy control is of critical importance. These systems are often referred to as Digital Right Management Systems - DRMS.

Use of watermarking for copyright protection of information published on Internet

When publishing on the Internet you cannot have a relationship with every possible person that will view or read your information. You are publishing in an open environment and you have to use methods that work under these circumstances.

Watermarks and fingerprinting can be regarded as an application of steganography techniques.

Steganography is another way than "traditional" cryptography of communicating and ensuring that unauthorized people do not get access to the information, i.e. handles confidentiality. In cryptography the strategy is to make it very difficult for unauthorized people to decrypt the information, while in steganography the strategy is to hide that there is anything for unauthorized people to pay an interest in. In traditional steganography the hidden or embedded text or information is the important one while the visible part (for example a picture) called the *cover,* only is a

disguise for the important information. When using steganography techniques for watermarking it is the other way around. The cover is the important and valuable information and the hidden information is there to make it possible to tell something about the cover, e.g. to prove the origin or ownership, or to ensure that change of the cover can be discovered.

Watermarking has a number of applications. Some examples of applications where watermarking can be used are:

1. Ownership assertion or copyright protection
2. Fingerprinting
3. Copy prevention or control
4. Image authentication for tamper and fraud control
5. Security of ID cards or other identification papers

Ownership assertion or copyright protection can be done by embedding information about the source and the copyright owner of the data as a watermark in the data. For this application it is important with a robust watermark that is difficult to erase or distort so it can't be recognized.

Fingerprinting aims at identifying each legally distributed copy of the data with a different watermark, a fingerprint, and thereby enabling tracing of illegal copying and distribution. If an illegal copy is found the fingerprint will help to identify whom the traitor is.

Copy prevention and control is about controlling what can be done with a distributed copy of the data. This is difficult to obtain in open environment, [4, 5, 7], and will require control over both the data with the embedded watermark and the device or software used to read the data and act according to the instructions in the watermark.

Image authentication. Watermarking can be used to verify if multimedia content used for example for legal purposes, news reporting and commercial transactions have been changed and if its origin is from a specific source. By embedding a watermark with low robustness (i.e. a watermark that will change at the slightest modification of the multimedia content) it can be controlled if the multimedia content has been tampered with.

ID card security. ID card consists in principle of two parts. One is the picture (could also be another biomedical identification) used to connect the ID card to an individual and the other giving some information about the individual like name, address or right to enter certain premises. By adding a watermark to the picture including the information in the other part of the ID card it can be verified if one of the ID card's parts has been changed or substituted.

For the type of transaction we have discussed in the introduction, the three first examples of using watermarks are the most likely alternatives to solve the problem we are focusing on in this paper.

Basic watermarks terminology, principles and hiding methods.

The information to be hidden (the watermark, fingerprint or in the general case of steganograhy, the secret message) is embedded in a *cover* object (e.g. a cover CD, a cover video, a cover text) giving a *stego* object, which in the context of copyright may also be called the *marked* object. The embedding will often be performed using a secret *key* normally known to the *cover* object's owner or a public/private key system. In addition the watermark may be encrypted before it is embedded in the cover object.

Visible watermarks are visual patters inserted into an image in a way that makes them visible in the same way as e.g. logos on paper images, an artist's signature on a painting.

Imperceptible watermarks are watermarks inserted in the cover object in a way that makes them imperceptible for the human senses. Imperceptible watermarks are the most interesting for the applications we will focus on in this paper.

Some of the properties that are of importance to evaluate a watermark's usefulness for the different applications are [4,5,7]:

Imperceptibility. The changes in the cover object caused by the embedded watermark should be below the threshold for what the human senses can distinguish.

Robustness. The robustness of a watermark is the watermark's ability to remain intact and detectable after the cover image has been modified i.e. exposed to image processing like compressing, cropping, blurring or to malicious attacks.

Redundancy. Redundant embedding of the watermarking in the cover is one method of improving the robustness of the watermark.

Security or Key restrictions. Normally the embedding of the watermark in the cover will include use of a secure cryptographic key to ensure the protection against manipulation or removal of the watermark. The key may be a single key for both encoding and decoding or public/private key system where one key is used for encoding and the other for decoding dependent of the application.

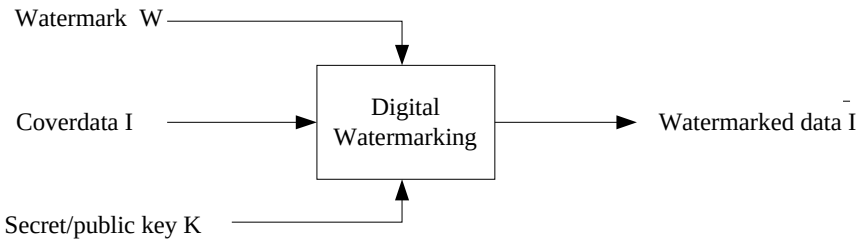
Computational cost. For many applications it is important how much processing the embedding and recovering of the watermark requires. The embedding only happens once for a specific cover while the recovery may have to occur many times and for some applications in real time. Hence, the computational cost for recovery will often be of greater importance than the computational cost for embedding.

Data payload. The payload is the amount of data (bits) that a watermark may consist of. Dependent of the application the need for watermark size will vary. The numbers of bits in watermarks are normally fairly limited.

All watermarking systems share the same generic building blocks [4]:

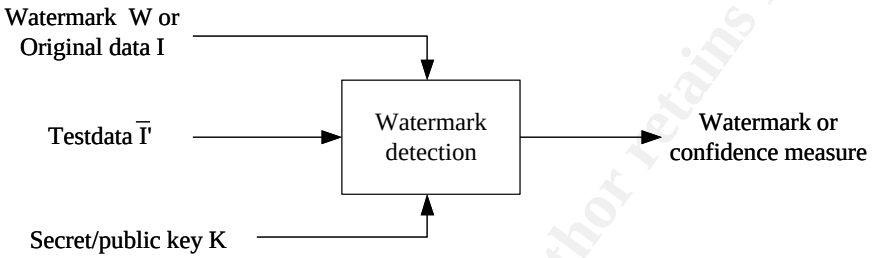
- Watermark embedding system or watermark encoding system
- Watermark recovery system or watermark decoding system

The watermark embedding system is the process of embedding the watermark in the cover using the key as shown in the following figure.



Generic digital watermarking scheme, Stefan Katzenbeisser, Fabien A.P. Petitcolas [4]

The watermark recovery system is the process of recovery or decoding of the watermark to be able to read the content or to verify that the watermark exists in the information to be tested as shown in the following figure.



Generic watermark recovery scheme, Stefan Katzenbeisser, Fabien A.P. Petitcolas [4]

Types of watermarking algorithms can be defined from the following properties and characteristics:

- What information must be available to recover or detect the watermark - blind/non-blind watermarking
- Who can detect the watermark? Only authorized readers or the public - Private/public watermarking
- Can the content of the watermark be extracted and read or can it only be detected if the watermark is there - Readable/detectable watermark
- Can the watermark be removed once it has been read or detected - Reversibility/non reversibility

Blind/non-blind/semi-blind watermarks. These concepts refer to which information must be available when recovering the watermark. Watermarking is said to be non-blind if it requires the original data to extract the information contained in the watermark. Another type of non-blind watermarking also requires a copy of the embedded watermark to be able to answer if the watermark exist in the watermarked data or not. Blind watermarking requires neither the original data or the embedded watermark to recover or detect the watermark in the watermarked data. Semi-blind watermarking does not use the original data but a copy of the embedded watermark to detect if it exist in the watermarked data.

Watermarking techniques

There exists a large number of techniques for embedding watermarks in digital information, and there is a comprehensive amount of research going on to improve existing techniques and to find new techniques and new combinations of existing techniques. The research often emphasizes on improving the robustness of watermarking because this is regarded as being the most important area for enhancements to watermarking. Thus making it more useful for copyright protection, currently the most prominent application of watermarking.

In [7] the following structure of watermarking techniques is proposed based on domain of insertion. This overview is not exhaustive:

- Spatial Domain
  - Patchwork's Algorithm
  - Public key cryptography and public watermark recovery
  - Predictive coding for psychovisual watermark management
- Transform domain
  - Discrete Fourier Transform (DFT)
  - Discrete Cosine Transform (DCT)
  - Mellin-Fourier Transform
  - Discrete Wavelet Transform
  - Spread Spectrum

The techniques are described in [1,3,4,5,7,15]. For each of the techniques there exists a number of variants having different values on parameters that are used by the techniques. This will influence the properties of the resulting watermark and hence the suitability for a specific application.

As there is an ongoing activity and research to find new and improved techniques to embed watermarks in images, there are also ongoing activities to develop new attacks on watermarks. In [21] the following classification of some of the known attacks is presented:

- Removal and Interference Attacks
  - Denoising
  - Lossy compression
  - Quantization
  - Remodulation
  - Collution
  - Averaging
  - Noise Storm
- Geometrical Attacks
  - Global, local warping
  - Global, local transforms
  - Jittering
- Cryptographic Attacks
  - Brute force key search
  - Oracle
- Protocol Attacks
  - Watermark inversion
  - Copy Attacks

Further description of attacks can be found in [4,6,21].

Watermarking tools must ensure that watermarks are not removed or made undetectable by these attacks. Implementing watermark techniques to accomplish this is a great challenge. A good implementation should be able to adapt to the image that is watermarked. It has for example been demonstrated that watermarks hidden in the perceptually significant parts of an image are more robust to attacks than watermarks hidden in less significant parts of the image. Hence the implementation ought to be able to adapt to this.

As seen from this brief presentation of watermarking the area is comprehensive and complex and there are many possible choices - e.g. type of algorithm in terms of blind/non-blind, public/private, readable/detectable and technique(s) - to make, to select the best combination for an application.

For the potential user to make up her/his mind, by reading and understanding the mathematics behind the different techniques, their robustness to different attacks and to select the right techniques for her/his application and requirements, is not an easy task.

In [4,5,7] there are some general descriptions on the properties of the different techniques with regard to their inherited robustness in term of ability to resist and survive different attacks from normal image processing to more malicious attacks. However, the robustness is not only dependent on the technique but also on the implementation in the watermarking product.

There are a large number of companies offering watermarking products like Digimark, Signum Technologies and many more (for a more comprehensive list see [20]). There are partnerships established between watermark companies and companies delivering image processing applications like Corel with Coreldraw and Photo-Paint and Adobe with Photoshop. These products are delivered with watermarking products included.

Benchmark tools like Stirmark, Checkmark and Optimark can help to evaluate and test an actual watermarking product and technique with regard to its robustness to withstand different types of attacks. However it requires fairly good understanding of the different techniques and attack types to perform a benchmark relevant for a potential users application and requirements.

Stirmark is a benchmarking tool for digital watermarking technologies. Given a watermarked input image, Stirmark generates a number of modified images which can then be used to verify if the embedded watermark can still be detected. Stirmark also proposes a procedure to combine the different detection results and compute an overall score ranging between 0 and 1.

Checkmark is a benchmarking suite for digital watermarking technologies. Running on Matlab under UNIX and Windows, it provides tools to evaluate and rate watermarking technologies. Checkmark contains some attacks not present in Stirmark. Moreover, it takes the watermark application into account which means that the scores from individual attacks are weighed according to their importance for a given watermark usage.

Optimark is a benchmarking tool for still image watermarking algorithms that was developed in the Artificial Intelligence and Information Analysis Laboratory at the Department of Informatics, Aristotle University of Thessaloniki, Greece. Optimark was partially supported by EU Projects CERTIMARK and INSPECT.

The following table shows some results from a Stirmark benchmark, Fabien A.P. Petitcolas, Ross J. Anderson [13]:

	Digimarc	Unige	SureSign	SCMark
Signal enhancement				
Gaussian filter	100	100	100	100
Median filter	100	100	100	100
Sharpening	100	100	100	100
F.M.L.R.	100	67	100	100
Compression				
J.P.E.G.	65	63	87	100
GIF/Colour quantisation	100	1	100	20
Scaling				
Without J.P.E.G. 90	81	86	97	0
With J.P.E.G. 90	72	83	83	0
Cropping				
Without J.P.E.G. 90	100	83	94	2
With J.P.E.G. 90	98	83	91	2
Shearing				
X	50	38	42	0
Y	50	21	42	0
Rotation				
Auto-crop	98	98	37	2
Auto-scale	97	98	51	26
Other geometrical transformations				
Lines and columns removal	100	83	89	7
Horizontal flip	100	100	100	0
Random geometric distortions (StirM	17	0	0	0

The table shows some results from a benchmark performed with Stirmark 3.1 in 1999 (4.0 is now the current version). The numbers indicate the percentage of successful watermark detection after the distortions. The benchmark gives a good comparison of the tested products on how they perform when exposed to different distortions of the watermarked images. But it also shows that a potential user of watermarks will need some expert assistance to interpret the results to select the product best suited for the actual applications based on this type of benchmark.

All the products have lack of robustness for some of the distortions. So none of them could resist attacks from experts.

One of the directions for further watermark research deals with providing potential users of watermark systems information about a watermarking system's performance. Research is being conducted to develop an internationally recognized watermark benchmarking system [15]. If this can be achieved it will help the potential user of watermarks to evaluate different watermarking product's suitability for an application. Helen Wollan [14] points out that "before watermarking can be commonplace, standards need to be developed. Without standards, the industry has no reference when it says a technique provides good protection", i.e. we need standards to compare with, when we test a watermarking product using a benchmark system. We need standards telling what requirements we should put on the watermark system's robustness against the different attacks when we are going to use it for a specific application.

Watermarking status and prospects

Digital watermarking is a fairly new discipline and there is comprehensive research going on to improve the robustness of watermarking so it can give better protection for copyright and other applications. So fare there is no satisfactory watermarking system, but work is still being done to find a truly robust, blind, public, transparent-image watermarking algorithm.

However, there are watermarking products on the market that can provide fairly robust watermarking. Though they can't resist attacks from experts they may together with new legislation (described later) provide adequate copyright protection for a number of applications.

Digital Right Management Systems for copy control of distributed information

Because of the difficulties in enforcing copy control in open system environments distribution of documents e.g. e-books are mainly using closed solutions developed by some of the major players in the market like Microsoft and Adobe.

These systems include some if not all of the elements described in [11] as the Digital Rights Management for e-books - DRM.

The components of a DMR system are:

- DRM e-book server
- Reading and searching system
- Transmission facilities. Any communication network may be used to transmit the e-book from the e-book server to the consumer's reader.

The e-book content, metadata and information of DRM and e-book numbering are stored on the e-book server. There are three types of metadata. Discovery metadata are public data including title, author and description of the e-book to make it possible for consumers to identify it and decide if they want to buy it. Core metadata are also public data, but are aimed at people organizing digital libraries. In addition to title, author etc. it includes category, file size and other necessary information for creating and administrating of digital libraries. The private metadata are data to help publishers, distributors and retailers in the process of selling and delivering the e-book. Private metadata is as the name indicates not for public use. Private metadata includes information about the rights, terms and condition of use of the delivered e-book. The rights are specified in RSL, Right Specification Language, and may specify the rights to print, copy, lend etc. The rights, spesified in RSL, are included in the ePackage delivered to the customer buying an e-book.

The reading and searching system is the software on the user's PC that enables the customer to read the delivered e-book. The e-book will normally be delivered encrypted and the reading and searching system utilize the information in the delivered ePackage and the information exchanged during the process of initiating the reader to give the customer the possibilities specified in the rights following the e-book.

The information transferred from the e-book server to the reader is normally encrypted. In addition fingerprinting may be used to give possibilities to trace unauthorized copies.

Adobe is, together with Microsoft, Palm and others, one of the major players in delivering DRM systems for e-books.

Adobe PDF has for several years offered the possibility to protect documents by encryption and passwords, one user password and one owner password. When the document is opened with owner password it is possible to define restrictions that will be in effect when the document is opened with the user password. Restrictions can for example be on modifying the document's content, copying text and graphics from the document, printing the document. In Acrobat 5 new user password restrictions has been introduced [18].

These mechanisms have given the owner of documents a certain level of control over what users of documents could do. It doesn't prevent copying the document because all necessary information is in the document and the standard Acrobat reader. Knowing either password is sufficient to decrypt the document.

In 2001 a Russian cryptoanalyst presented Adobe's Acrobat e-book reader security mechanisms and the security flaws that he found in Adobe's Acrobat e-book reader [18].

In addition the company he worked for made available on the Internet software that could remove all restrictions on encrypted Adobe PDF documents. This initiated a lot of actions from Adobe to get the cryptoanalyst arrested and to close down the site where the software was available. We are in this paper not going to discuss that part of the event but look at the basic driving forces and principles behind it.

There have also been reports on exploitation of security flaws in Microsoft's e-book LIT format [16,17]

There will always be professionals, putting effort into solving any available, interesting problem as for example cracking the protection of an Adobe document.

However, there is also a market that mainly is interested in getting access to documents and books on fair conditions. They acknowledge the value of the author's and publisher's contribution to make interesting and valuable information available to the market.

So one of the basic problems is that there is no agreement between owners/publishers and customers of e.g. an e-book about what should be possible for the customer to do with it. Should it be possible to read on different computers, printing for personal use etc? Some e-books, including the reference [4] for this paper, are distributed with very limited possibilities for the customer, without any notice when the e-book is marketed and purchased. The distributor has utilized to the maximum the possibilities in the e-book distribution and reading system to limit what the customer can do with the e-book. It is not possible to print. It can only be read on the computer it initially was downloaded to. It is not possible to transfer and read on another computer. If you change disk or cpu in the computer you have downloaded the e-book to you can't read it any more. The user manual for the reader says you have to call support because the reader checks for disc and cpu configuration.

This kind of limitation most customers would regard as unfair and many would be tempted to support effort to break these limitations including buying software that can be used to remove limitations regarded as unfair. So the publisher has created a market for the hacker and the software that can remove the limitations.

For the benefit of the e-book marked it is important that publishers and owners of e-book rights don't put unfair limitations on the customer's possibilities to use what they have purchased because the technology enables these possibilities. It may end up with an e-book marked where the publishers have extremely good control on possible misuse of the e-books, but with very few customers or an e-book market where hackers and their software to break limitations have a prosperous time.

In standard crypto terms the Basic problem is that Alice doesn't trust Bob and Alice and Bob disagree on the rights he should have over the documents he has paid for. She doesn't want Bob to get full control over the documents she sent him. So she sent him the documents encrypted with additional information embedded in the documents and certificates or vouchers that tells what Bob is allowed to do with the documents. In addition she delivers a proprietary device, the reader, that can decrypt the documents combining all the information.

So on Bobs computer all information, keys, methods and how to combine them exist.

So we are back to one of the basic rules for security, "Security by Obscurity is no security" (Kerchoffs prinsiple [4], ref. SANS GSEC lesson 4.1)

This, combined with many e-book buyers possible feeling they haven't got fair rights to utilization of the documents they have paid for, will inspire people to find out how to break the system, and will most likely lead to that many, otherwise law obedient people, will get tempted to download software that can decrypt the documents and give them full control for own use. The Adobe case illustrates this.

Status of DRM

DRM systems are available from major companies like Microsoft and Adobe. Some of the larger publishers and distributors of e-books, like Penguin and Amazon, use these types of systems.

Though they can't resist attacks from experts they may together with new legislation (described later) provide adequate copy control for a number of applications.

Legislation

Both in the US and EU the awareness of the technology's lack of ability to ensure a strong protection of copyright and copy control has contributed to legislation initiatives to compensate for this.

In the US the Digital Millenium Copyright Act of 1998 (DMCA) [19] makes it a crime to offer for sale products that circumvent digital copy protections, including encryption schemes. Other provisions create penalties for creating and distributing such tools.

In the EU [8], the " Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on Harmonization of Certain ASPECTS OF Copyrights and Related Rights in the Information Society" (called the "Information Society Directive") explicitly requires, in Article 6, member states to provide "adequate legal protection" against circumvention of "effective technological measures" designed to prevent or restrict acts not authorized by the copyright holder, including the trafficking in devices, products or services which may be used to circumvent such technology. Article 7 of the Directive imposes similar obligations with respect to electronic rights-management information.

It still remains to see how the different EU member countries will implement the Information Society Directive, but there is no doubt that new legislation will support the protection that may be obtained with technological measures.

Summary

For publishers and distributors of electronic documents, e-books and information on the Internet there are possibilities to protect intellectual property rights by using different technological measures.

For copy control of distributed electronic documents like e-books, available DRM systems provide an adequate level of protection and several large publishers and distributors of e-books have chosen to base their business on these systems. The protection the systems offer against e.g. copying and printing, may be removed by experts, but if the publishers and distributors allow fair use of the distributed e-books it is likely that this only will have a marginal influence on their business.

For copyright protection there are several products available that provide fairly robust watermarking of e.g. images published on the Internet. However, none of the existing watermarking techniques can withstand attacks from experts. There is a comprehensive ongoing research to find new and improved techniques. It is expected that these efforts in the future will result in techniques providing more robust watermarking. To select the right watermarking product for an application it is likely that a potential user may need some expert assistance.

New legislation support the protection and control that may be obtained with technological measures as they make it a crime to sell and distribute products aimed at circumvention of the technical measures.

References

[1] Elizabeth Ferrill, Matthew Moyer, "A survey of Digital Watermarking, February 25, 1999. URL:
http://elizabeth.ferrill.com/papers/watermarking.p df

[2] Deepa Kundur and Dimitrios Hatzinakos, "Towards Robust Logo Watermarking using Multiresolution Image Fusion Principles", URL:
http://ee.tamu.edu/~deepa/pdf/mm10324.pdf

[3] Saraju P. Mohanty, "Digital Watermarking: A Tutorial Review", URL:
http://www.csee.usf.edu/~smohanty/research/Reports/WMSurvey1999Mohanty.pdf

[4] Stefan Katzenbeisser, Fabien A.P. Pe titcolas, editors, "InformationHiding Techniques for Steganography and Digital Watermarking", 2000, ARTECH HOUSE, INC.

[5] R. Chandramouli, Nasir Memon, Majid Rabbani, "Digital Watermarking", URL:
http://faculty.ist.unomaha.edu/pdasgupta/courses/csci8980/papers/collberg02watermarking.p df

[6] Fabien A.P. Petitcolas, Ross J. Anderson, Markus G. Kuhn, "Attacks on Copyright Marking Systems", URL:
http://downloads.securityfocus.com/library/ih98 -attacks.pdf

[7] Stanley R.M. Oliveira, Mario A. Nascimento, Osmar R. Zaïane, "Digital Watermarking: Status, Limitation and Prospects", Janu ary 2002, URL:
http://www.cs.ualberta.ca/~oliveira/techreport/ TR02-01.pdf

[8] Brian W. Esler, "Technological Self -Help: Its Status under European Law and Implications for U.K. Law", April 2002, URL:
http://www.bileta.ac.uk/02papers/esler.html

[9] Mary E. Carter, "Protecting Your Copyrights on the Web", URL
http://www.ef use.com/Plan/copyright3.html

[10] Arnaud Sahuguet, "Piracy: The Dark Side of Electronic Commerce", May 1998, URL:
www.cis.upenn.edu/~sahuguet/PLAN/piracy.ps.gz

[11] Guoyou He, "Analysis of E-book Security", 2001, URL:
http://www.tml.hut.fi/Studies/T -110.501/2001/papers/he.pdf

[12] Bryan Guignard, "How Secure Is PDF?", URL:
http://www-2.cs.cmu.edu/~dst/Adobe/Gallery/PDFsecurity.pdf

[13] Fabien A.P. Petitcolas, Ross J. Anderson, "Evaluation of copyright marking systems", june 1999, URL:
http://www.cl.cam.ac.uk/~fapp2/publications/ieeemm99 -evaluation.ppt

[14] Helen Wollan, "Digital Watermarking in Still Images", URL:
http://mrs.umn.edu/~lopez dr/seminar/spring2000/wollan.pdf

[15] Changhua Wu and Rebecca Cathey, "Digital Watermarking: An Comparative Overview of Several Digital Watermarking Schemes", December 20002, URL:
http://www.csam.iit.edu/~cs549/cs549/project/presentation_report.pdf

[16] "Microsofts E-Book-Verschlüsselung", 02.01.2003, URL:
http://www.golem.de/0301/23292.html

[17] "Microsoft e-book securi ty in doubt", August 2001, URL:

http://news.com.com./2100-1023-272506.html?legacy=cnet&tag=rltdnws

[18] "eBooks security - theory and practice", July 2001, URL:

http://www-2.cs.cmu.edu/~dst/Adobe/Gallery/ds-defcon2/ds-defcon.html

[19] U.S. Copyright Office Summary, "The Digital Millennium Copyright Act of 1998", URL:

http://www.loc.gov/copyright/legislation/dmca.pdf

[20] Watermarking world, Digital watermarking companies

http://www.watermarkingworld.org/companies.html

[21] S. Pereira, S. Voloshynovskiy, M. Madueno, S. Marchand-Maillet and T. Pun, "Second generation benchmarking and application oriented evaluation", URL:

http://vision.unige.ch/publications/postscript/2001/PereiraVoloshynovskiyMaduenoMarchandPun_ihw2001.pdf

Last Updated: October 18th, 2017

Upcoming Training

SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201710,	Oct 23, 2017 - Nov 29, 2017	vLive
San Diego Fall 2017 - SEC401: Security Essentials Bootcamp Style	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	vLive
SANS Seattle 2017	Seattle, WA	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS San Diego 2017	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS Gulf Region 2017	Dubai, United Arab Emirates	Nov 04, 2017 - Nov 16, 2017	Live Event
Community SANS Vancouver SEC401^	Vancouver, BC	Nov 06, 2017 - Nov 11, 2017	Community SANS
Community SANS Colorado Springs SEC401~	Colorado Springs, CO	Nov 06, 2017 - Nov 11, 2017	Community SANS
SANS Miami 2017	Miami, FL	Nov 06, 2017 - Nov 11, 2017	Live Event
SANS Sydney 2017	Sydney, Australia	Nov 13, 2017 - Nov 25, 2017	Live Event
SANS Paris November 2017	Paris, France	Nov 13, 2017 - Nov 18, 2017	Live Event
SANS San Francisco Winter 2017	San Francisco, CA	Nov 27, 2017 - Dec 02, 2017	Live Event
Community SANS St. Louis SEC401	St Louis, MO	Nov 27, 2017 - Dec 02, 2017	Community SANS
SANS London November 2017	London, United Kingdom	Nov 27, 2017 - Dec 02, 2017	Live Event
Community SANS Portland SEC401	Portland, OR	Nov 27, 2017 - Dec 02, 2017	Community SANS
SANS Khobar 2017	Khobar, Saudi Arabia	Dec 02, 2017 - Dec 07, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Dec 04, 2017 - Dec 09, 2017	Community SANS
SANS Austin Winter 2017	Austin, TX	Dec 04, 2017 - Dec 09, 2017	Live Event
SANS Munich December 2017	Munich, Germany	Dec 04, 2017 - Dec 09, 2017	Live Event
SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201712,	Dec 11, 2017 - Jan 24, 2018	vLive
SANS Bangalore 2017	Bangalore, India	Dec 11, 2017 - Dec 16, 2017	Live Event
SANS Cyber Defense Initiative 2017	Washington, DC	Dec 12, 2017 - Dec 19, 2017	Live Event
SANS Cyber Defense Initiative 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Dec 14, 2017 - Dec 19, 2017	vLive
Community SANS Nashville SEC401^	Nashville, TN	Jan 08, 2018 - Jan 13, 2018	Community SANS
Community SANS Hawaii SEC401	Honolulu, HI	Jan 08, 2018 - Jan 13, 2018	Community SANS
SANS Security East 2018	New Orleans, LA	Jan 08, 2018 - Jan 13, 2018	Live Event
Mentor Session - SEC401	Memphis, TN	Jan 09, 2018 - Mar 13, 2018	Mentor
Northern VA Winter - Reston 2018	Reston, VA	Jan 15, 2018 - Jan 20, 2018	Live Event
SANS Amsterdam January 2018	Amsterdam, Netherlands	Jan 15, 2018 - Jan 20, 2018	Live Event
Mentor Session - SEC401	Minneapolis, MN	Jan 16, 2018 - Feb 27, 2018	Mentor
Las Vegas 2018 - SEC401: Security Essentials Bootcamp Style	Las Vegas, NV	Jan 28, 2018 - Feb 02, 2018	vLive
SANS Las Vegas 2018	Las Vegas, NV	Jan 28, 2018 - Feb 02, 2018	Live Event