Multimedia Security: Watermarking Techniques

Edin Muharemagic and Borko Furht
Department of Computer Science and Engineering
Florida Atlantic University, 777 Glades Road
Boca Raton, FL 33431-0991, U.S.A.
E-mail: {borko, edin}@cse.fau.edu

1   Introduction

A recent proliferation and success of the Internet, together with availability of relatively inexpensive digital recording and storage devices has created an environment in which it became very easy to obtain, replicate and distribute digital content without any loss in quality. This has become a great concern to the multimedia content (music, video, and image) publishing industries, because technologies or techniques that could be used to protect intellectual property rights for digital media, and prevent unauthorized copying did not exist.

While encryption technologies can be used to prevent unauthorized access to digital content, it is clear that encryption has its limitations in protecting intellectual property rights: once a content is decrypted, there's nothing to prevent an authorized user from illegally replicating digital content. Some other technology was obviously needed to help establish and prove ownership rights, track content usage, insure authorized access, facilitate content authentication and prevent illegal replication.

This need attracted attention from the research community and industry leading to a birth of Digital Watermarking. Its basic idea is to create some kind of metadata containing some information about a digital content to be protected. The metadata is called watermark, and a digital content to be protected is called a cover work. The watermark should be imperceptibly embedded into the cover work, and it should be robust enough to survive not only most common signal distortions, but also distortions caused by malicious attacks.

It is clear that digital watermarking and encryption technologies are complementing each other, and that a complete multimedia security solution depends on both. This paper describes various watermarking applications, and it provides an overview of the image watermarking solutions. It represents a complement paper to the [24] where the current achievements in multimedia encryption have been presented.

2 Applications of Digital Watermarking

Very frequently there's a need to associate some additional information with a digital content, such as music, image or video. For example, copyright notice may need to be associated with an image to identify a legal owner of that image. Or a serial number may need to be associated with a video to identify a legitimate user of that video. Or some

kind of identifier may need to be associated with a song to help find a database where more information about it can be obtained from. This additional information can be associated with a digital content by placing it in the header of a digital file, or for images, it can be encoded as a visible notice. Storing information in the header of a digital file has a couple of disadvantages. First, it may not survive a file format conversion, and second, once an image is displayed or printed, its association with the header file and information stored in it is lost. Adding a visible notice to an image may not be acceptable if it negatively affects the esthetics of the image. This could be corrected to some extent by making the notice as small as possible and/or moving it to a visually insignificant portion of the image, such as the edge. However, once on the edge, this additional information can easily be cropped off, either intentionally or unintentionally.

This is exactly what happened with an image of Lena Soderberg after its copyright notice was cropped off. The image was originally published as a Playboy centerfold in November 1972. After the image has been scanned for use as the test image, most of it has been cropped including the copyright notice which was printed on the edge of the image. The "Lena" image became probably the most frequently used test image in image processing research, and appeared in a number of journal articles without any reference to its rightful owner, Playboy Enterprises, Inc.

Figure 2-1 The Lena image used as a test image on the left, and the cropped part of the original image which identifies the copyright owner, Playboy Enterprises, Inc. on the right.

Digital watermarking seems to be suitable method for associating this additional information, the metadata, with a digital work. The metadata is imperceptibly embedded as a watermark in a digital content, the cover work, and it becomes inseparable from it. Furthermore, since watermarks will go through the same transformations as the cover work they are embedded in, it is sometimes possible to learn whether and how the content has been tampered with by looking into the resulting watermarks.

2.1 Classification of Digital Watermarking Applications

There are a number of different watermarking application scenarios, and they can be classified in a number of different ways. The following classification is based on the type of information conveyed by the watermark [33].

Application Class	Purpose of the embedded watermark	Application Scenarios
Protection of Intellectual Property Rights	Conveys information about content ownership and intellectual property rights	Copyright Protection, Copy Protection, Fingerprinting
Content Verification	Ensures that the original multimedia content has not been altered, and/or helps determine the type and location of alteration	Authentication Integrity Checking
Information hiding	Represents side-channel used to carry additional information.	Broadcast Monitoring System Enhancement

Table 2-1 Classes of watermarking applications

In the following section we'll provide a more detailed explanation of possible application scenarios involving watermarking.

2.2 Digital Watermarking for Copyright Protection

Copyright protection appears to be one of the first applications digital watermarking was targeted for. The metadata in this case contains information about the copyright owner. It is imperceptibly embedded as a watermark in the cover work to be protected. If users of digital content (music, images, and video) have an easy access to watermark detectors, they should be able to recognize and interpret the embedded watermark and identify the copyright owner of the watermarked content.

An example of one commercial application created for that purpose is Digimarc Corporation ImageBridge Solution. The ImageBridge watermark detector is made available in a form of plug-ins for many popular image processing solutions, such as Adobe PhotoShop or Corel PhotoPaint. When a user opens an image using Digimark enabled application, Digimarc's watermark detector will recognize a watermark. It will then contact a remote database using the watermark as a key to find a copyright owner and his contact information. An honest user can use that information to contact the copyright owner to request permission to use the image.

We have shown above how an invisibly embedded watermark can be used to identify copyright ownership. It would be nice if an embedded watermark could be used to prove the ownership as well, perhaps even in a court of law. We can envision the following scenario: A copyright owner distributes his/her digital content with his/her invisible watermark embedded in it. In the case of a copyright ownership dispute, a legal owner should be able to prove his ownership by demonstrating that he owns the original work, and that the disputed work has been derived from the original by embedding a watermark into it. This could be done by producing the original work together with the watermark detector, and having detector detect the owner's watermark in a disputed work. Unfortunately, it appears that the above scenario can be defeated under certain assumptions, and because of that watermarking has not been accepted yet as a technology

dependable enough to be used to prove the ownership. One potential problem is related to the availability of watermark detector. It has been demonstrated that if a detector is widely available, then it is not possible to protect watermark security. In other words, if a detector is available, it is always possible to remove an embedded watermark. This can be achieved by repeatedly making imperceptible changes to the watermarked work, until a watermark detector fails to detect the watermark. Once the watermark is removed, the original owner will not be able to prove his ownership any longer. Even if the original watermark cannot be removed, it has been demonstrated [18,19,20] that, under certain conditions, it is possible to add another watermark to an already watermarked image in such a way as to make it appear that this second watermark is present in all copies of disputed image, including the original image. This is known as an ambiguity attack, and it could be used not only to dispute the ownership claims of the rightful copyright owner, but also to make new ownership claim to the original digital content

2.3 Digital Watermarking for Copy Protection

The objective of a copy protection application is to control access to and prevent illegal copying of copyrighted content. It is an important application, especially for digital content, because digital copies can be easily made, they are perfect reproductions of the original, and they can easily and inexpensively be distributed over the Internet with no quality degradation.

There are a number of technical and legal issues that need to be addressed and resolved in order to create a working copy protection solution. Those issues are difficult to resolve in open systems, and we are not aware of the existence of an open system copy protection solution. Copy protection is feasible in closed, proprietary systems, and we will describe the Digital Versatile Disk (DVD) copy protection solution [2, 4].

DVD copy protection system has a number of components designed to provide copy protection at several levels. The Content Scrambling System (CSS) encrypts MPEG-2 video and makes it unusable to anyone who does not have a decoder and a pair of keys required to decrypt it. But, once the video has been decrypted, CSS does not provide any additional protection for the content.

Additional mechanisms have been put in place to provide extra protection for the decrypted (or unscrambled) video. For example, the Analog Protection System (APS) prevents an unscrambled video displayed on television from being recorded on an analog device, such as VCR. APS does it by modifying NTSC/PAL signals in such a way that video can still be displayed on television but it cannot be recorded on VCR.

There was also a need to support limited copying of video content. For example, a customer should be able to make a single copy of the broadcast video for later viewing (a.k.a. time shifting recording), but he should not be able to make additional copies. The Copy Control Management System (CCMS) has been designed to provide that level of copy control by introducing and supporting three rules for copying: Copy Free, Copy Never, and Copy Once. Two bits are needed to encode those rules, and the bits are embedded into the video frames in the form of watermarks.

It is obvious that this copy control mechanism will work only if every DVD recorder contains a watermark detector. How to ensure that, when there does not seem to exist a natural economic incentive for DVD manufacturers to increase a production cost of their product by incorporating watermark detectors in DVD recorders? After all, a perceived market value of a DVD recorder with a watermark detector may be lower compared with a recorder without it, because a customer would rather have a device that can make illegal copies.

One solution to this problem would be to force DVD manufacturers to add watermark detectors in their devices by law. Since such a law does not exist, and even if it did, it would be very difficult to enforce it across every country in the world, an alternative solution was needed. The solution that has been adopted for DVD systems is based on the patent license. Basically, the DVD encryption patent license makes it mandatory to use watermark detectors in the patent compliant devices.

The patent-license approach ensures that compliant devices will use watermark detectors and prevent illegal copying, but it also makes it legal to manufacture noncompliant devices, the devices which do not implement the patented decryption, and therefore do not have to implement a watermark detector. Consequently, the DVD copy control mechanism does not prevent all possible illegal copying.
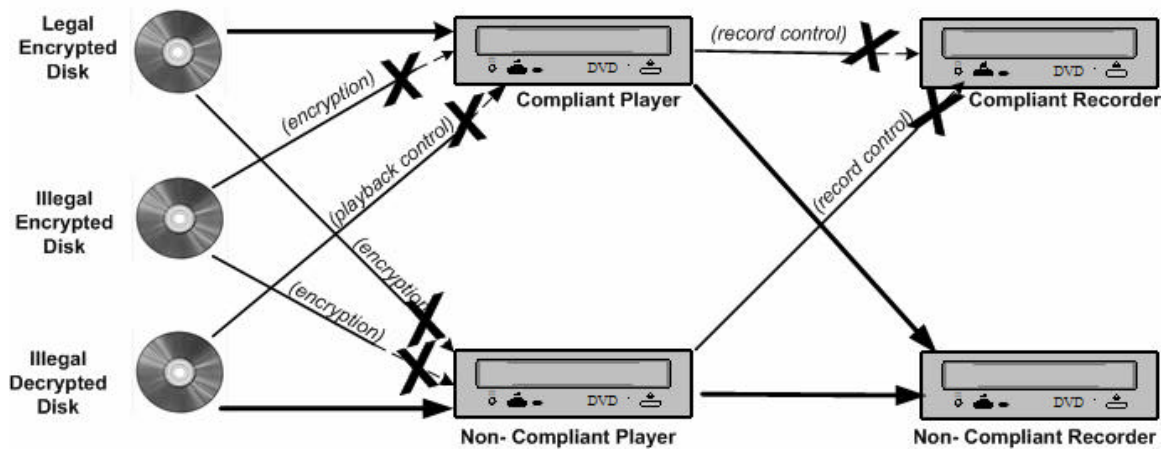

Figure 2-1 DVD copy protection systems with watermarking

Interaction of encryption and copy control, combined with the playback control, a mechanism which allows a DVD compliant device to detect illegal copies, is used to create a solution where only illegal copies can be played on noncompliant devices, and only legal copies can be played on compliant devices, as shown on Figure 2-1. The objective of this scheme is to insure that one device will not be able to play both legal and illegal content. If a customer wants to play both legal and illegal copies he will have to purchase both compliant and noncompliant devices. If one of the two has to be selected, the hope is that most customers will choose a compliant one.

2.4 Digital Watermarking for Fingerprinting

There are some applications where the additional information associated with a digital content should contain information about the end user, rather than about the owner of a

digital content. For example, consider what happens in a film making environment. During the course of film production, the incremental results of work are usually distributed each day to a number of people involved in a movie making activity. Those distributions are known as film dailies, and they are confidential. If a version is leaked out, the studio would like to be able to identify the source of the leak. The problem of identifying the source of a leak can be solved by distributing slightly different copies to each recipient, thus uniquely associating each copy with a person receiving it.

As another example, consider a digital cinema environment, an environment where films are distributed to cinemas in digital format instead of via express mail in the form of celluloid prints. Even though digital distribution of films could be more flexible and efficient and less expensive, film producers and distributors are slow to adopt it because they are concerned about potential loss of revenue caused by illegal copying and redistribution of films. Now, if each cinema receives a uniquely identifiable copy of a film, then, if illegal copies have been made, it should be possible to associate those copies with the cinema where they have been made, and initiate an appropriate legal action against it.

Associating unique information about each distributed copy of digital content is called *fingerprinting*, and watermarking is an appropriate solution for that application because it is invisible and inseparable from the content. This type of application is also known as *traitor tracing* because it is useful for monitoring or tracing illegally produced copies of digital work. Also, since watermarking can be used to keep track of multiple transactions that have taken place in the history of the copy of a digital content, the term *transaction tracking* has been used as well.

2.5 Digital Watermarking for Content Authentication

Multimedia editing software makes it easy to alter digital content. For example, Figure 2-2 shows three images. The left one is the original, authentic image. The middle one is the modified version of the original image. and the right one shows the image region which has been tampered. Since it is so easy to tamper with a digital content, there's a need to be able to verify integrity and authenticity of the content.

A solution to this problem could be borrowed from cryptography, where digital signature has been studied as a message authentication method. Digital signature essentially represents some kind of summary of the content. If any part of the content is modified, its summary, the signature, will change making it possible to detect that some kind of tampering has taken place. One example of digital signature technology being used for image authentication is the trustworthy digital camera described in [24].

Digital signature information needs to be somehow associated and transmitted with a digital content it was created from. Watermarks can obviously be used to achieve that association by embedding signature directly into the content. Since watermarks used in the content authentication applications have to be designed to become invalid if even slight modifications of digital content take place, they are called *fragile watermarks.*

Figure 2-2 Original image, tampered image, and detection of tampered regions. Courtesy of Ching-Yung Lin

Fragile watermarks, therefore, can be used to confirm authenticity of a digital content. They can also be used in applications where it is important to figure out how digital content was modified or which portion of it has been tampered with. For digital images, this can be done by dividing an image into a number of blocks and creating and embedding a fragile watermark into each and every block.

Digital content may undergo lossy compression transformation, such as JPEG image conversion. While resulting JPEG compressed image still has an authentic content, the image authenticity test based on the fragile watermark described above will fail. *Semi-fragile watermarks* can be used instead. They are designed to survive standard transformations, such as lossy compression, but they will become invalid if a major change, such as the one in Figure 2-2, takes place.

2.6 Digital Watermarking for Broadcast Monitoring

Many valuable products are regularly broadcast over the television network: news, movies, sports events, advertisements, etc. Broadcast time is very expensive, and advertisers may pay hundreds of thousands of dollars for each run of their short commercial that appears during commercial breaks of important movies, series or sporting events. The ability to bill accurately is this environment is very important. It is important to advertisers who would like to make sure that they will pay only for the commercials which were actually broadcast. And, it is important for the performers in those commercials who would like to collect accurate royalty payments from advertisers.

Broadcast monitoring is usually used to collect information about the content being broadcast, and this information is then used as the bases for billing as well as other purposes. A simple way to do monitoring is to have human observers watch the broadcast and keep track of everything they see. This kind of broadcast monitoring is expensive, and it is prone to errors. Automated monitoring is clearly better. There are two categories of automated monitoring systems: passive and active. Passive monitoring systems monitor the content being broadcast and make an attempt to recognize it by comparing it with the known content stored in a database. They are difficult to implement for a couple

of reasons. It is difficult to compare broadcast signals against the database content, and it is expensive to maintain and manage a large database of content to compare against. Active monitoring systems rely on the additional information which identifies the content and gets broadcast together with the content itself. For analog television broadcast, this content identification information can be encoded in the vertical blanking interval (VBI) of the video signal. The problem with this approach is that it is suitable for analog transmission only, and even in that case it may not be reliable because, in US, content distributors do not have to distribute information embedded in the VBI.

A more appropriate solution for active monitoring is based on watermarking. The watermark containing broadcast identification information gets embedded into the content itself, and the resulting broadcast monitoring solution becomes compatible with broadcast equipment for both digital and analog transmission.

2.7 Digital Watermarking for System Enhancement

Digital watermarking can also be used to convey a side-channel information with the purpose of enhancing functionality of the system or adding value to the content it is embedded in. This type of applications, where a device is designed to react to watermark for the benefit of the user, is also referred to as device control applications [14].

An example of an early application of watermarking for system enhancement is described in the Ray Dolby's patent application filed in 1981, where he proposed to make radio devices which would turn Dolby FM noise reduction control system on and off automatically, in response to an inaudible signal broadcast within the audio frequency spectrum. Such a signal constitutes a simple watermark, and the proposed radio device was an enhancement compared to the radio devices used at that time, where listeners had to manually turn their radio's Dolby FM decoder on and off.

More recently, Philips and Microsoft have demonstrated an audio watermarking system for music [30]. Basically, as music is played, a microphone on a PDA can capture and digitize the signal, extract the embedded watermark and based on information encoded in it, identify the song. If a PDA is network connected, the system can link to a database and provide some additional information about the song, including information about how to purchase it.

Another example of a similar application is Digimarc MediaBridge system. On content production side, watermarks representing unique identifiers are embedded into images, and then printed and distributed in magazines as advertisements. On the user side, an image from a magazine is scanned, the watermark is extracted using the MediaBridge software, and the unique identifier is used to direct a web browser to an associated web site.

3 Basic Principles of Digital Watermarking

Digital watermarking system consists of two main components: *watermark embedder* and *watermark detector*. The embedder combines the *cover work* C_O, an audio-visual signal in which data will be hidden, and the *payload P*, an input message to be added to the

cover work, and creates the *watermarked cover* C_W. This embedding operation takes place in two steps or phases. In the first phase, the watermark encoder takes the payload P and maps it into the watermark W, which has to be of the same type and dimension as the cover work C_O. For example, if the cover work C_O is an image, then the watermark encoder would produce an image pattern of the same size as the cover image. This mapping may be done with help of a watermark key K which can be used to enforce security. In the second phase, the watermark W is added to the cover work C_O to produce the watermarked cover C_W.

Watermark embedders can be classified into two categories, *blind* and *informed*, depending on whether it uses the cover work C_O or not.

Blind embedder ignores the cover work, and it can be described using the following notation:

$$C_W = E_1(C_O, W) \quad \wedge \quad W = E_0(P, K)$$

Informed embedder examines the cover work before it creates the watermark W, and it can be described using the following notation:

$$C_W = E_1(C_O, W) \quad \wedge \quad W = E_0(P, K, C_O)$$

The watermarked cover C_W may go through different types of processing yielding possibly corrupted watermarked cover $\hat{C}_W$. This corruption could be caused either by various distortions created by normal signal transformations (e.g. compression, decompression, D/A and A/D conversions) or by distortions introduced by various malicious attacks.

Watermark detector either extracts the payload P from the watermarked cover $\hat{C}_W$, or it produces some kind confidence measure indicating how likely it is for a given payload P to be present in $\hat{C}_W$. The extraction of the payload is done with help of a watermark key K.

Watermark detectors can be classified into two categories, *blind* and *informed*, depending how much of the cover work information is available to the watermark detection process.

Informed detector, also known as a non-blind detector, uses cover work C_O in a detection process, and it can be described using the following notation:

$$P = D(\hat{C}_W, C_O, K)$$

Blind detector does not use the original cover C_O, and it can be described using the following notation:

$$P = D(\hat{C}_W, K)$$

Figures 3-1 and 3-2 illustrate the two possible Digital Watermarking system configurations. Figure 3-1 shows a system using a blind embedder and an informed

detector, and Figure 3-2 shows a system using an informed embedder and a blind detector.
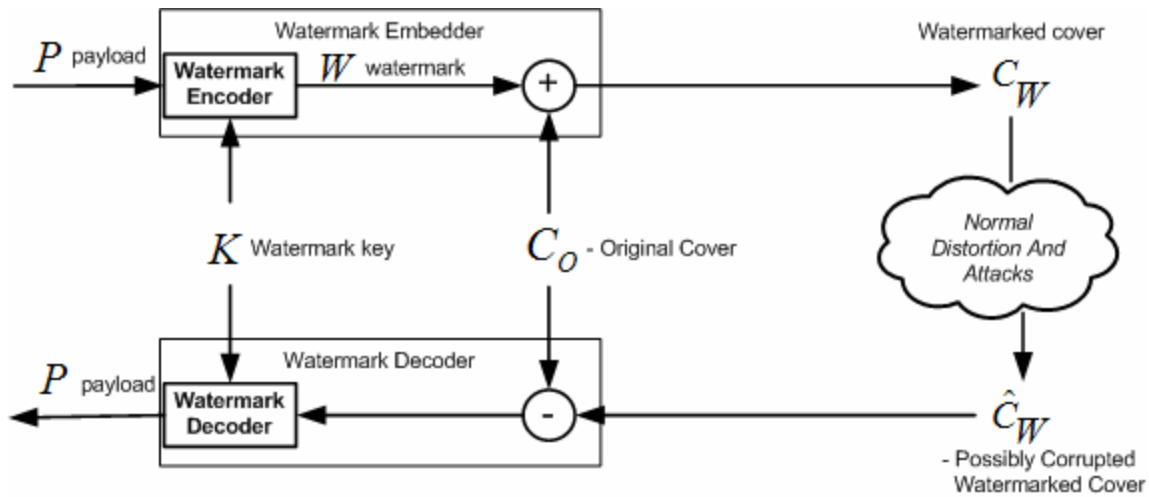

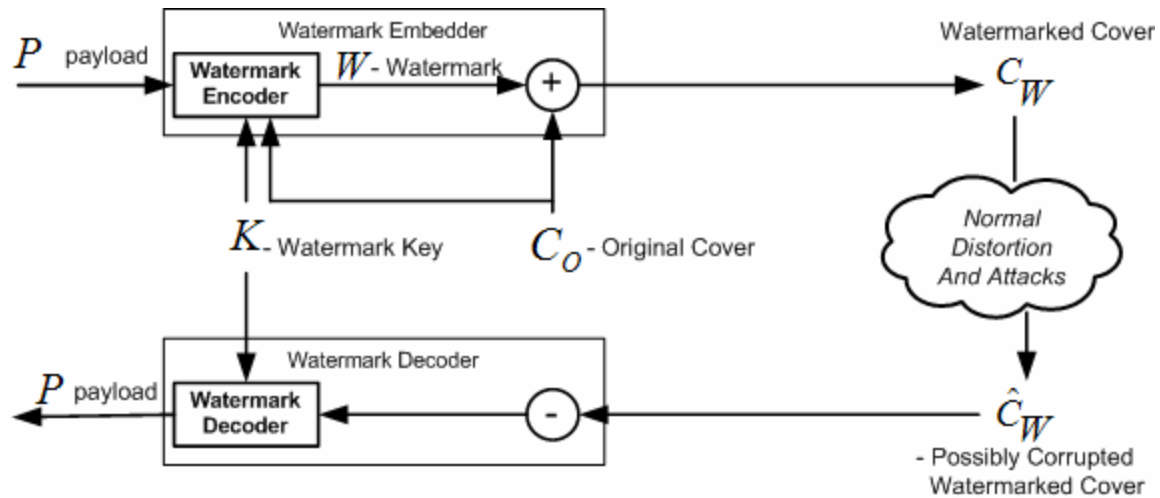Figure 3-1 Watermarking systems with blind embedder and informed detector

Figure 3-2 Watermarking system with informed embedder and blind detector

4 Evaluation of Watermarking Systems

Once a watermarking system has been designed and implemented, it is important to be able to objectively evaluate its performance. This evaluation should be done in such a way to be able to compare results against other watermarking systems designed for the same or similar purpose [29, 31, 37].

By definition, watermarking is a technique for embedding a watermark into a cover work imperceptibly and robustly. Therefore a quality of a new watermarking system can be

measured by evaluating those two properties and comparing results against an equivalent set of measures obtained by evaluating other watermarking systems.

Watermark imperceptibility can be evaluated either using subjective evaluation techniques involving human observers, or using some kind of distortion or distance metrics. Watermark robustness can be evaluated using standardized benchmark tests. Those tests are designed to create various distortions to the watermarked cover under tests, so that it is possible to measure watermark detection rate under those conditions.

4.1 Imperceptibility Measures

Imperceptibility of an embedded watermark can be expressed either as *fidelity* or *quality* measure. Fidelity represents a measure of similarity between the original and watermarked cover, whereas quality represents an independent measure of appeal or acceptability of the watermarked cover. The most accurate tests of fidelity and quality are subjective tests which involve human observers. Those tests have been developed by psychophysics, a scientific discipline whose goal is to determine relationship between the physical world and people's subjective experience of that world. An accepted measure for evaluation of the level of distortion is a *Just Noticeable Difference* (JND), and it represents a level of distortion that can be perceived in 50% of experimental trials. One JND thus represents a minimum distortion that is generally perceptible.

Watermark perceptibility can be measured using different experiments developed as a result of various psychophysics studies. One example is the Two Alternative, Forced Choice (2AFC) test. In this procedure human observers are presented with a pair of images, one original and one watermarked, and they must decide which one has higher quality. Statistical analysis of responses provides some information about whether the watermark is perceptible. For example, if the fidelity of the watermarked image is high, meaning that it is very similar to the original, the random responses will be received and we'll see approximately 50% of the observers selecting the original image as the higher quality image, and 50% of the observers selecting the watermarked image as the higher quality image. This result can be interpreted as zero JND. Variations of that test are possible, and more information about it can be found in [14]

Another, more general approach, allows observers more options in their choice of answers. Instead of selecting the higher quality image, observers are asked to rate the quality of the watermarked image under test. One example of quality scale that can be used to evaluate perceptibility of an embedded watermark is the one recommended by the ITU-R Rec.500, where a quality rating depends on the level of impairment a distortion creates. The recommended scale has 5 quality levels which go from excellent to bad, and those quality levels correspond to impairment descriptions from imperceptible distortion to very annoying distortion.

These subjective tests can provide very accurate measure of perceptibility of an embedded watermark. However, they can be very expensive, they are not easily repeatable, and they cannot be automated.

An alternative approach is to develop an automated technique for quality measure which is based on a model which tries to predict observer's responses. One such model was proposed by Watson [42], and it tries to estimate the number of JNDs between images.

Yet another alternative, and the one that is the easiest to apply, is based on measuring distortion caused by embedding a watermark. This distortion can be represented as a measure of difference or distance between the original and the watermarked signal. One of the simplest distortion measures is the mean squared error (MSE) function defined as $MSE(C_W, C_O) = \dfrac{1}{N} \sum_N (c_w[i] - c_o[i])^2$. The most popular distortion measures are the Signal to Noise Ratio defined as $SNR(C_W, C_O) = \sum_N c_o^2[i] / \sum_N (c_O[i] - c_W[i])^2$, and the Peak Signal to Noise Ration defined as $PSNR(C_O, C_W) = \max_N c_O^2[i] / \sum_N (c_o[i] - c_W[i])^2$.

For more detailed list of distortion measures see [29]

Distortion metric tests are simple and popular. Their advantage is that they do not depend on subjective evaluations. Their disadvantage is that they are not correlated with human vision. In other words, small distance between the original and the watermarked signal does not always map into the high fidelity.

4.2 Evaluation of Other Properties

Robustness property can be evaluated by applying various kinds of "normal" signal distortions and attacks that are relevant for the target application. The robustness can be assessed by measuring detection probability of the watermark after signal distortion. This is usually done using standardized benchmarking tests, and we'll provide more information about it in the next section.

Reliability can be evaluated by assessing the watermark detection error rate. This can be done either analytically, by creating models of watermarking systems under test, or empirically, by running a number of tests and counting the number of errors. As we stated before, false positive and false negative errors are interrelated and it is not possible to minimize both probabilities (or error rates) simultaneously. Because of that those two errors should always be measured and presented together, for example using a receiver operating characteristics (ROC) curve.

Capacity is an important property because it has a direct negative impact on watermark robustness. Higher capacity (the amount of information being embedded) causes lower watermark robustness. Capacity can be assessed by calculating the ratio of capacity to reliability. This can be done empirically by fixing one parameter (e.g. payload size) and determining the other parameter (e.g. error rate). Those results can then be used to estimate the theoretical maximum capacity of the watermarking system under consideration. Since a requirement for capacity depends on the application, the question is how important it is to estimate the excess capacity capability of the watermarking system under consideration. It may be important because the excess capacity can be traded for improvements in reliability. This can be done by using the excess payload bits for error detection and/or correction.

Another property that may need to be taken into consideration is the watermark access unit or granularity. It represents the smallest part of an audiovisual signal needed for reliable detection of a watermark and extraction of its payload. In the case of image watermarking for example, this property can be evaluated by using test images of different sizes.

In general, in order to obtain statistically valid results, it is important of ensure that a/ the watermarking system under consideration is tested using a large number of test inputs, b/ the set of test inputs is representative of what is expected in the operating environment (application), and c/ the tests are executed multiple times using different watermarking keys.

4.3 Benchmarking

There are a number of benchmarking tools which have been created to standardize watermarking system evaluating processes.

Stirmark [45] is a benchmarking tool for digital watermarking designed to test robustness. For a given 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. The following image alterations have been implemented in Stirmark Version 3.1: Cropping, Flip, Rotation, Rotation-Scale, FMLR, sharpening, Gaussian filtering, Random bending, linear transformations, Aspect ratio, Scale changes, Line removal, Color reduction, JPEG compression.

Checkmark [46] is a benchmarking suite for digital watermarking developed on Matlab under UNIX and Windows. It has been recognized as an effective tool for evaluation and rating of watermarking systems. Checkmark offers some additional attacks not present in Stirmark. Also, it takes the watermark application into account which means that the scores from individual attacks are weighted according to their importance for a given watermark purpose. The following image alterations have been implemented: Wavelet compression (jpeg 2000 based on Jasper), Projective transformations, Modeling of video distortions based on projective transformations, Warping, Copy, Template removal, Denoising (midpoint, trimmed mean, soft and hard thresholding, wiener filtering), Denoising followed by perceptual remodulation, Non-linear line removal, and Collage.

Optimark [47] is a benchmarking tool developed to address some deficiencies recognized in Stirmark 3.1. Some of its features are: graphical user interface, detection performance evaluation using multiple trials utilizing different watermarking keys and messages, ROC curve, detection and embedding time evaluation, payload size evaluation, and so on.

Certimark [48] is a benchmarking suite developed for watermarking of visual content and a certification process for watermarking algorithms. It has been created as a result of a large research project funded by European Union.

5 Digital Watermarking for Images: An Overview

Generally speaking, most watermarking systems are based on some variation of the following principle: On a watermark embedding side, small, pseudo-random changes

representing a watermark are applied to selected coefficients in a chosen processing domain. A watermark detector uses some kind of correlation similarity measure to identify those changes and detect the embedded watermark.

A large number of research papers and articles have been published on image watermarking over the last decade, and a number of different watermarking approaches have been presented [1, 14, 28, 29, 39, 43]. Most of those approaches are similar and they only differ in one or a few aspects related to how a watermark gets created, where in the cover it gets embedded, how it gets embedded, what domain to use for embedding, and how it gets detected.

For obvious reason, it is not possible to discuss all contributions made in the field of digital watermarking. Instead, we will classify watermarking solutions according to the defining properties mentioned above, and provide a few representative examples. More specifically, we will look into the following basic alternatives in a design of a digital watermarking system:

- Processing domain selection: A watermark can be embedded into the cover image in a *spatial domain*. Alternatively, it can be more advantageous to do it in a *transform domain*, such as discrete Fourier transform domain (DFT), discrete cosine transform domain (DCT), the Fourier-Mellin transform domain, wavelet transform domain, or the fractal transform domain.

- Cover location selection: According to the adaptation of Kerckhoff's principle to watermarking, the watermarking algorithms should be public, but the embedded watermark should be protected and it should not be easily accessible without a key. Required protection of watermark can be achieved through *random selection* of cover locations where the watermark information will be embedded. A pseudo-random number generator, initialized by the secret key (the seed), is usually used to determine those locations. This solution basically hides the locations where various bits of watermark information are embedded. An alternative approach protects the watermark information by *spreading* it across cover, so that any cover location contains some part of watermark information.

- Payload encoding: The problem can be stated as follows: given a multi-bit message payload, how to create a watermark representing it, which will have good characteristics with respect to imperceptibility, robustness, and detection error rate. Some solutions allow any multi-bit payload to be directly embedded into an image [2]. Others use *spread spectrum* or *error correcting codes* to transform a payload into an appropriate watermark before imbedding it into an image.

- Watermark embedding method selection: A watermark can simply be *added* to the cover image. The addition may be image independent or image dependent. Image dependent addition techniques could be based on common-sense rules or image-adaptive rules. The image-adaptive rules exploit masking properties of the human visual system. An alternative watermark embedding method is based on *quantization*.

- Watermark detection: In general, watermark detection is directly derived from watermark embedding.

5.1 Processing Domain Selection

A watermark can be embedded into the cover image in a spatial domain. Alternatively, this operation can be carried out in a transform domain, such as discrete Fourier transform domain, discrete cosine transform domain, or wavelet domain.

An example of a watermarking system where embedding operation is done in a spatial domain is the "*patchwork*" algorithm proposed by Bender et al. [4]. This is a statistical method used to embed only one bit of information. In other words, this technique cannot be used to embed an arbitrary message into the cover image.

The patchwork works as follows: A watermark is embedded by first selecting n pairs of pixels (a_i, b_i), and then modifying their luminance values. The pairs are selected pseudo-randomly based on a secret key K, and luminance values are modified according to the following formula: $\tilde{a}_i = a_i + d \quad \wedge \quad \tilde{b}_i = b_i - d$. Assuming that the image satisfies the following statistical property: $\sum_n (a_i - b_i) \approx 0$, the watermark can be detected if we retrieve the same n pairs of pixels based on the key K and compute: $\Delta = \sum_n (\tilde{a}_i - \tilde{b}_i)$. If $\Delta \approx 2nd$, the image is watermarked; otherwise, it is not.

As we said above, patchwork embeds only 1 bit of information. It can be modified to embed more by splitting the image into pieces and applying the patchwork to each individual piece.

Spatial domain watermarking solutions are robust to cropping and translation. However, they are less robust to lossy compressions, such as JPEG. Actually, it has been observed that the watermarking solutions implemented in specific transform domain are robust to compressions based on the same transform.

Discrete cosine transform (DCT) domain addresses the issue of robustness to JPEG compression, and watermark embedding which operates in the DCT domain is typically more robust to JPEG compression. In addition to the robustness issue, DCT domain was attractive to the watermarking research community, because DCT was widely studied in the context of JPEG and MPEG coding, and a lot of results on visual distortion of images were directly applicable to the watermarking. Therefore, a lot of DCT domain watermarking solutions have been proposed. They use either a block based or global DCT. Other transform domains that have proposed include the wavelet domain, the discrete Fourier transform domain [41], the Fourier-Mellin transform domain [36] and the fractal transform domain [26]. We will present examples of DCT and wavelet domain use.

An early solution for efficient watermarking in DCT domain was introduced by Koch at all. [2]. This solution uses relationship between DCT coefficients to embed a watermark representing an N-bit payload into the cover image. The image is first divided into the 8x8 blocks, N blocks are pseudo-randomly selected, and DCT is computed for the

selected blocks, as in JPEG compression algorithm. The N bits of information are embedded into the N pseudo-randomly selected blocks, one bit to each block, as follows: A pair of DCT coefficients is selected to represent a single bit. Let's say out of the set of DCT coefficients $(a_{11},..,a_{88})$, the selected pair is (a_{ij}, a_{mn}). The mutual relationship between two coefficients can then be used to represent the value of one bit. For example, $a_{ij} < a_{mn}$, can be interpreted as bit 1. The bit embedding process then consists of making appropriate changes to the pair of coefficients, if needed, to ensure that the relationship between coefficients is correct for the bit we want to embed. For example, assuming that the relationship $a_{ij} < a_{mn}$ represents bit value 1, the embedding algorithm can be described as follows: To embed a bit value 1 into the 8x8 block, check the relationship between coefficients in the pair. If $a_{ij} < a_{mn}$, nothing needs to be done since the relationship already indicates a correct bit value. Otherwise, modify coefficients appropriately to force $a_{ij} < a_{mn}$. In order to strike the balance between robustness and possible image degradation caused by modifications of the coefficients, the pair is selected from mid-range frequencies. This approach shows good robustness to JPEG compression down to a quality factor of 50%.

With the standardization of JPEG-2000 and a decision to use wavelet-based image compression instead of DCT-based compression, watermarking techniques operating in the wavelet transform domain have become more attractive to the watermarking research community. The advantages of using the wavelet transform domain are an inherent robustness of the scheme to the JPEG-2000 lossy compression, and possibility of minimizing computation time by embedding watermarks inside of a JPEG-2000 encoder. Additionally, the wavelet transform has some properties that could be exploited by watermarking solutions. For example, wavelet transform provides multi-resolution representation of images, and this could be exploited to build more efficient watermark detection schemes, where watermark detection starts from the low-resolution sub-bands first, and only if detection fails in those sub-bands, should it explore the higher resolution sub-bands and additional coefficients it provides.

Zhu et al. [44] propose a unified approach to digital watermarking of images and video based on the two-dimensional (2-D) and three-dimensional (3-D) discrete wavelet transform. This approach is very similar to the Cox et al. [17] we'll present in more detail later in this text. The only difference is that Zhu generates a random vector with $N(0,1)$ distribution and spreads it across coefficients of all high-pass bands in the wavelet domain as a multi-resolution digital watermark, where as Cox does it only across a small number of perceptually most important DCT coefficients. The watermark added to a lower resolution represents a nested version of the one corresponding to a higher resolution, and the hierarchical organization of the wavelet representation allows detection of watermarks at all resolutions except the lowest one. The ability to detect lower resolution watermarks reduces computational complexity of watermarking algorithms because fewer frequency bands are involved in computation. It also makes this watermarking scheme robust to image/video down sampling operation by power of two in either space or time.

5.2 Cover Location Selection

5.2.1 Hiding Watermark Location

Early watermarking techniques were based on using the least significant bit of the image representation as the carrier for watermark. This technique has been improved by pseudo-randomly selecting pixels to be used as carriers of watermark information bits.

The solution introduced by Koch at all. we described above [2], is another example of a secret key based technique for selection of the cover location where the watermark information bits are embedded.

5.2.2 Spreading Watermark Information

One way to spread the watermark information is to embed it into the statistics of the luminance of the pixels, like in the patchwork solution we described earlier. Recall that the patchwork watermark carries only 1 bit of information. This one bit of information is spread across randomly selected set of n pairs of pixels.

The patchwork statistical technique can be thought of as some kind of primitive spread spectrum modulation. General spread spectrum system spreads a narrow band signal over a much wider frequency band so that the signal to noise ratio (SNR) in a single frequency band is low and appears like noise to an outsider. However, a legitimate receiver with precise knowledge of the spreading function should be able to extract and sum up the transmitted signals so that the SNR of the received signal is strong.

Since it is a common practice to model watermarking as a communications channel where the cover image is treated as noise and the watermark is viewed as a signal that is transmitted through it, it become obvious that techniques that worked in communications may work in watermarking as well. That was a motivation for Cox et al. [17] to apply the spread spectrum techniques to watermarking. The basic idea was to spread the watermark over many frequency bands, so that the energy in any one band is small and undetectable. But, knowing the location and content of the watermark, makes it possible to concentrate those many weak watermark signals into a single output with high SNR. Here is a high-level overview of this watermarking technique.

A watermark consists of a sequence of real numbers $W = \{w_i\}_1^n$ drawn from normal distribution $N(0,1)$. The watermark is embedded using the formula $\tilde{v}_i = v_i(1 + \boldsymbol{a}w_i)$, where $V = \{v_i\}_1^n$ represents n most perceptually significant components of an image's DCT. These values are selected to provide greater robustness to JPEG compression. Watermark detection is performed using the following similarity measure: $sim(W,W') = \dfrac{W \bullet W'}{\sqrt{W' \bullet W'}}$, where W' is the extracted watermark. The watermark is said to be present if $sim(W,W')$ is greater than the given threshold. The original image is needed to check for the presence of watermark, so this system falls into the category of informed detectors.

Note that the length n does not represent capacity of the payload. Instead, it represents the degree to which the watermark is spread out among the relevant components of the image. In general, as n increases, the extent of required alteration of v_i as part of the embedding process decreases, resulting in better fidelity of the watermarked image.

This scheme, like the patchwork, embeds only 1 bit of information. More bits can be embedded by placing multiple watermarks into the image, but at the cost of reduced robustness.

Robustness tests showed that this scheme is robust to JPEG compression to the quality factor of 5%, dithering, fax transmission, printing-photocopying-scanning, multiple watermarking, and collusion attacks.

5.3 Payload Encoding

A watermark designed to carry only one bit of information is typically created as a pseudo-random noise drown from Gaussian or uniform distribution. The detector extracts the embedded bit by verifying whether the watermark is present or not. Most watermarking applications, however, require more than one bit of information to be embedded.

The information rate of the watermarking system can be increased by introducing additional watermarks, and mapping each individual watermark to different bit string (multi-bit message). For example, to support 4-bit messages, one would need $2^4 = 16$ different watermarks, each one mapping to a different 4-bit message. The message is detected by computing a detection value for each of 16 watermarks, and selecting the one with the highest detection value. This technique is known as *direct message coding*. It works well for short messages, but it is not practical for longer bit strings. For example, in order to embed 16 bits of information, the watermarking system would need $2^{16} = 65536$ different watermarks. Those watermarks would have to be created with the maximum possible separation to avoid a situation where a small corruption of the watermarked image would lead to erroneous watermark detection. Ensuring that 65536 watermarks are far apart from one another is not easy. Additionally, the detector would have to compare a test image against 65536 different watermarks even if it only had to check for the watermark absence.

An alternative to direct message coding is a technique where a different watermark represents each individual bit of the multi-bit message. A multi-bit message can be embedded into a cover image by adding watermarks representing individual bits of the multi-bit message to the cover, one by one. This is the approach used in [2] we described before. More generally, this technique can be presented as the one where watermarks representing individual bits of a multi-bit message are first combined together into a single watermark representing the whole message, and then added into the cover image.

Watermarks can be combined together in a couple of different ways. For example, they could be tiled together in such a way that any individual tile is a watermark representing individual message bit. This is equivalent to the space division multiplexing. Alternatively, an approach equivalent to frequency division multiplexing could be used

where watermarks representing individual message bits would be placed into disjoint frequency bands. Or, most generally, an approach analogous to code division multiplexing in spread spectrum communications could be used. This approach exploits the fact that several uncorrelated watermarks can be combined together without interfering with one another.

5.3.1 Spread-Spectrum

Once again, we have a multi-bit message (payload) we would like to embed into an image. We can do that by creating different watermark for each individual message bit, and then we can combine all those watermarks together into one master watermark to be embedded into the image. The master watermark can be created by tiling or concatenating individual watermarks, or by placing individual watermarks into different frequency bands. The most efficient watermark combining technique, however, can be created based on the spread spectrum communication technology. Since watermarking systems can be modeled as communication systems, where the watermark represents a message and the image represents communications channel, it is only natural to revisit all techniques which have been applied to communications systems successfully, and see whether and how they can be applied to watermarking systems.

Spread spectrum technique is based on spreading the message energy over a bandwidth much larger than the minimum bandwidth required. This technique has two major advantages: low power density and redundancy. Low power density relates to the fact that the transmitted energy is spread over a wide band, and consequently the amount of energy for any specific frequency band is low. The effect is that such a signal will not interfere with other signals that share the same frequency band. Redundancy relates to the fact that the message is present on different frequency bands, so that if there's an error in one band, the message could still be recovered from other bands.

Both properties are very beneficial to watermarking as well. Assuming that a watermark represents a message, the low power density means that the watermark will be introducing very small changes to the image and therefore the embedded watermark should be imperceptible. Redundancy maps to robustness, and means that a watermark will be recoverable even if it suffered certain level of intentional or unintentional distortion.

Hartung and Girod [32] proposed a watermarking system based on the direct-sequence spread spectrum communications techniques. This solution has been proposed for video watermarking, but it is also applicable to images. A watermark, representing an individual message bit $a_j \in \{-1,1\}$ is created in two steps. The bit is first spread by a large spreading factor cr, in an analogy to spread spectrum communications equivalent called the chip-rate. The purpose of spreading is to distribute that one bit of information across many pixels of an image. The spread bit is then modulated with a pseudo-noise sequence, yielding one watermark. This procedure is repeated for each information bit of a message, and the created watermarks are added together yielding a final watermark which represents the whole message. The recovery of the multi-bit message is accomplished by correlating the watermarked image with the same pseudo-noise sequence that was used on the message encoding side, where correlation can be thought

of as demodulation followed by summation over the correlation window, where the width of the correlation window for each information bit is the chip-rate cr. If the peak of the correlation is positive, then the current information bit is $+1$, and if the peak of the correlation is negative, then the current information bit is -1. After decoding of one bit, the next cr pixels are processed the same way to recover the next bit. This scheme will work only if both message encoder and message decoder use the same pseudo-noise sequence. In other words, both sides have to use the same key (seed) for the pseudo-random number generator. Note also that the original (un-watermarked) image is not used in the message recovery process, so this watermarking system belongs to the category of blind detection systems.

5.3.2 Error-correcting codes

As we said above, in direct message coding where an individual watermark is created to represent the whole message, the number of different watermarks has to match the number of messages, and in order to minimize watermark detection error, individual watermarks have to be designed to have maximum separation. In the multi-bit coding system, a watermark representing a multi-bit message is created by somehow combining together watermarks representing individual message bits. Good separation of watermarks is still important, but it can not be guarantied. If we assume that every possible sequence of bits represents a distinct message, and that watermarks representing those messages are created using a multi-bit coding approach, then there's a possibility that some of those watermarks will have poor separation. That means a small signal distortion could cause the system to erroneously detect presence of the wrong watermark.

This problem could be solved using error correcting codes. The basic idea is to define a system where not every possible sequence of bits corresponds to a message. Bit sequences that correspond to messages are called *code words*. This scheme requires the number of bits representing messages to be increased. For example, if we have 16 possible messages, we need only 4 bits to represent them. However, we can use 7 bits instead, and we can select only 16 out of possible 128 7-bit combinations to represent the 16 messages. Those 16 7-bit combinations (code words) should be selected in such a way that any two differ in three bits. In other words, if we start from one code word, we would need to change at least three bits to obtain a codeword which represents different message.

There are many error correction codes available. For example, the old and famous Hamming code ensures that any two coded messages differ in at least three bits. It allows correction of single bit errors, and it handles random errors well. Other codes, such as BCH and Trellis codes allow a greater number of burst errors to be corrected. The class of turbo codes [7] is known for its good performance, and it has been used to encode watermark messages [27]

5.4 Watermark Embedding Method Selection

A watermark can be embedded into the cover image using the following techniques: *addition* and *quantization*.

5.4.1 Addition

The addition techniques have evolved over time, and they differ on how they exploit frequency sensitivity, luminance sensitivity and masking capabilities of the human visual system (HVS).

A lot of research has been done over the years, to understand how HVS responds to frequency and luminance changes. The frequency sensitivity refers to the eye's response to spatial, spectral, or time frequency changes. Spatial frequencies are perceived as patterns or textures, and spatial frequency sensitivity is usually described as the eye's sensitivity to luminance changes [14]. It has been found that the eye is the most sensitive to luminance changes in the mid-range spatial frequencies, and that sensitivity decreases at lower and higher spatial frequencies. The pattern orientation affects sensitivity as well and the eye is most sensitive to vertical and horizontal lines and edges and it is least sensitive to lines and edges with 45-degree orientation. Spectral frequencies are perceived as colors, and it has been found that the eye is least sensitive to changes in blue color. Based on that, Hurtung and Kutter [28] proposed a solution where the watermark is added to the blue channel of an RGB image. Temporal frequencies are perceived as motion or flicker, and it has been found that eye sensitivity decreases very quickly as temporal frequencies exceed 30 Hz. It has also been found that the eye is less sensitive to higher luminance levels, and that this sensitivity is not linear.

A number of solutions have been proposed where frequency sensitivity of HVS is exploited to ensure that the watermark is imperceptible [16, 17, 38, 41, 42]. Those solutions use transform domain (e.g. DCT, FDT, wavelet), and the watermark is added directly into the transform coefficients of the image. Some of those solutions do not use the original image, and therefore belong to a class of blind embedders. This can be formally described using the following formula: $\tilde{c}_i = c_i + \boldsymbol{a}w_i$, where $W = \{w_i\}$ is the watermark, $C_O = \{c_i\}$ is the cover image, $C_W = \{\tilde{c}_i\}$ is the watermarked image, and $\boldsymbol{a}$ represents a global scaling parameter which determines the W embedding strength.

This embedding formula may not be appropriate if c_i values vary a lot. For example, adding 10 to the large value of c_i may not be sufficient to establish a mark, whereas adding 10 to the small value of c_i may introduce an unacceptable distortion. It may be more appropriate to make the amount of change dependant on characteristics of the cover image C_O. This can be achieved using the following watermark embedding formula: $\tilde{c}_i = c_i(1 + \boldsymbol{a}w_i)$. Here the watermark embedding depends on the image. However, this dependence is simple and straightforward and it does not take full advantage of characteristics of the HVS.

It is known that different spectral components may have different levels of tolerance to modification, and also it is known that the presence of one signal can hide or mask the presence of another signal. Those characteristics of the HVS can be exploited as well to create an efficient image-adaptive solution. A single scaling parameter $\boldsymbol{a}$ will not be appropriate in that case. Instead, more general watermark embedding formula $\tilde{c}_i = c_i(1 + \boldsymbol{a}_i w_i)$ should be used. Different image-adaptive solutions select multiple

scaling parameters a_i different ways. Walfgang et al. [42] present a couple of image-adaptive watermarking solutions.

5.4.2   Quantization

Chen and Wornell [10] have proposed watermark embedding based on quantization. Their method called quantization index modulation (QIM) is based on the set of N-dimensional quantizers. The quantizers satisfy a distortion constraint and are designed such that the reconstruction values from one quantizer have a good separation from the reconstruction points of every other quantizer. The message to be transmitted is used as an index for quantizer selection. The selected quantizer is then used to embed the information by quantizing the image data in either special or DCT domain. In the decoding process, a distance metric is evaluated for all quantizers and the index of the quantizer with the smallest distance identifies the embedded information. The watermarking system based on QIM was shown to have better performance than other watermarking systems based on the standard spread-spectrum modulation which are not image-adaptive.

5.5 *Watermark Detection*

Watermark detection is usually done using some kind of correlation technique. This works well as long as there's no cross correlation between the watermark and the cover image. However, since the watermark is frequently designed independent of the cover image, a possibility of high cross correlation exists and it represents a common problem in watermarking. Some proposed solutions for this problem require the original, un-watermarked image, to subtract it before the watermark extraction. Those techniques belong to the class of informed detectors. Other proposed methods apply a pre-filter [23] instead of subtracting the original. Yet other proposed methods do not deal with cross correlation at all [38]. Watermark detection is usually done in the domain that corresponds to the domain used for watermark creation and embedding.

6 Conclusions

In this paper we presented an overview of digital watermarking. First we looked at the range of applications that could benefit from applying digital watermarking technology. Protection of intellectual property is very important nowadays because digital multimedia content can be copied and distributed quickly, easily, inexpensively, and with high quality. Watermarking has been accepted as a complementary technology to multimedia encryption, providing some additional level of protection of intellectual property rights. Other applications, such as fingerprinting, content authentication, copy protection and device control have also been identified. We also presented a general model of the watermarking system, and identified its two main components: embedder and detector. Depending on whether the original content, or cover work, is needed for embedding or detection, we classified watermarking systems into blind or informed embedders, and blind or informed detectors. We then discussed the issues related to evaluation of watermarking systems. At the end we presented an overview of image watermarking

techniques, where we classified various watermarking solutions based on a/ what domain is being used (spatial vs. transform), b/ how to select image locations where to embed a watermark (random vs. spreading), c/ how to encode a payload for robustness (spread-spectrum and/or error correcting codes), d/ how to embed a watermark (addition vs. quantization), and e/ how to detect a watermark.

7 References

[1] *Arnold, M.; Schmucker, M;Wolthusen, S.D.* ; "Techniques and Applications of Digital Watermarking and Content Protection", Artech House, 2003

[2] *Burgett, S.; Koch, E.; Zhao, J.;* "Copyright labeling of digitized image data", Communications Magazine, IEEE , Volume: 36 Issue: 3 , March 1998, Pages:94-100

[3] *Bell, A.E.;* "The dynamic digital disk", Spectrum, IEEE , Volume: 36 Issue: 10 , Oct. 1999, Page(s): 28 -35

[4] *Bender, W.;Gruhl, D.;Morimoto, N.*;"Techniques for Data Hiding" in Proc.SPIE, vol 2420, San Jose, CA, Feb 1995, p.40

[5] *Bloom, J.A.; Cox, I.J.; Kalker, T.; Linnartz, J.-P.M.G.; Miller, M.L.; Traw, C.B.S.;* "Copy protection for DVD video", Proceedings of the IEEE , Volume: 87 Issue: 7 , July 1999, Page(s): 1267 -1276

[6] *Boneh, D.; Shaw, J.;* "Collusion-secure fingerprinting for digital data", IEEE Transactions on Information Theory, Volume: 44 Issue: 5 , Sept. 1998, Page(s): 1897 -1905

[7] *Berrou, C.; Glavieux, A.;* "Near optimum error correcting coding and decoding: turbo-codes", Communications, IEEE Transactions on , Volume: 44 Issue: 10 , Oct. 1996 Page(s): 1261 -1271

[8] *Chen, B.; Sundberg, C.-E.W.;* "Digital audio broadcasting in the FM band by means of contiguous band insertion and precanceling techniques", IEEE Transactions on Communications, Volume: 48 Issue: 10 , Oct. 2000, Page(s): 1634 -1637

[9] *Chen, B.; Wornell, G.W.;* "An information-theoretic approach to the design of robust digital watermarking systems", 1999 IEEE International Conference on Acoustics, Speech, and Signal Processing, 1999. ICASSP '99. Proceedings., Volume: 4 , 15-19 March 1999, Page(s): 2061 -2064 vol.4

[10] *Chen, B.; Wornell, G.W.;* "Quantization index modulation: a class of provably good methods for digital watermarking and information embedding**", IEEE Transactions on Information Theory, Volume: 47 Issue: 4 , May 2001, Page(s): 1423 -1443

[11] *Pradhan, S.S.; Chou, J.; Ramchandran, K.;* "Duality between source coding and channel coding and its extension to the side information case", IEEE Transactions on Information Theory, Volume: 49 Issue: 5 , May 2003, Page(s): 1181 -1203

[12] *Chou, J.; Pradhan, S.S.; El Ghaoui, L.; Ramchandran, K.;* "Watermarking based on duality with distributed source coding and robust optimization principles", 2000. Proceedings. 2000 International Conference on Image Processing, Volume: 1 , 10-13 Sept. 2000, Page(s): 585 -588 vol.1

[13] *Costa, M.;* "Writing on dirty paper (Corresp.)", , IEEE Transactions on Information Theory, Volume: 29 Issue: 3 , May 1983, Page(s): 439 -441

[14] I.J. Cox, M.L.Miller, and J.A.Bloom, "Digital Watermarking", Morgan Kaufmann, 2001

[15] *Cox, I.J.; Miller, M.L.;* "Electronic watermarking: the first 50 years", 2001 IEEE Fourth Workshop on Multimedia Signal Processing, 3-5 Oct. 2001, Page(s): 225 - 230

[16] *Cox, I.J.; Miller, M.L.; McKellips, A.L.;* "Watermarking as communications with side information", Proceedings of the IEEE , Volume: 87 Issue: 7 , July 1999, Page(s): 1127 -1141

[17] *Cox, I.J.; Kilian, J.; Leighton, F.T.; Shamoon, T.;* "Secure spread spectrum watermarking for multimedia", IEEE Transactions on Image Processing, Volume: 6 Issue: 12 , Dec. 1997, Page(s): 1673 -1687

[18] *Cox, I.J.; Linnartz, J.-P.M.G.;* "Some general methods for tampering with watermarks", IEEE Journal on Selected Areas in Communications, Volume: 16 Issue: 4 , May 1998, Page(s): 587 -593

[19] *Craver, S.; Memon, N.; Yeo, B.-L.; Yeung, M.M.;* "Resolving rightful ownerships with invisible watermarking techniques: limitations, attacks, and implications", IEEE Journal on Selected Areas in Communications, Volume: 16 Issue: 4 , May 1998, Page(s): 573 -586

[20] *Craver, S.; Memon, N.; Boon-Lock Yeo; Yeung, M.M.;* "On the invertibility of invisible watermarking techniques", Image Processing, 1997. Proceedings., International Conference on , Volume: 1 , 26-29 Oct. 1997, Page(s): 540 -543 vol.1

[21] *Craver, S.A.; Min Wu; Liu, B.;* "What can we reasonably expect from watermarks?", Applications of Signal Processing to Audio and Acoustics, 2001 IEEE Workshop on the, 21-24 Oct. 2001, Page(s): 223 -226

[22] *Decker, S.;* "Engineering considerations in commercial watermarking", IEEE Communications Magazine, Volume: 39 Issue: 8 , Aug. 2001 , Page(s): 128 -133

[23] *Depovere, G.; Kalker, T.; Linnartz, J.-P.;* "Improved watermark detection reliability using filtering before correlation", Image Processing, 1998. ICIP 98. Proceedings. 1998 International Conference on , Volume: 1 , 4-7 Oct. 1998, Page(s): 430 -434 vol.1

[24] *Friedman, G.L.,* "The Trustworthy Digital Camera: Restoring Credibility to the Photographic Image," IEEE Transaction on Consumer Electronics, Vol. 39, No. 4, November 1993, pp.905-910

[25] *Furht,B.; Socek,D.;* "Multimedia Security: Encription Techniques," IEC Comprehensive Report on Information Security, International Engineering Consortium, Chicago, IL, 2003.

[26] *Dugelay, J.-L.; Roche, S.;* "Fractal transform based large digital watermark embedding and robust full blind extraction" Multimedia Computing and Systems, 1999. IEEE International Conference on , Volume: 2 , 7-11 June 1999 Page(s): 1003 -1004 vol.2

[27] *Eggers, J.J.; Su, J.K.; Girod, B.;* "Robustness of a blind image watermarking scheme", Image Processing, 2000. Proceedings. 2000 International Conference on , Volume: 3 , 10-13 Sept. 2000, Page(s): 17 -20 vol.3

[28] *Hartung, F.; Kutter, M.;* "Multimedia watermarking techniques", Proceedings of the IEEE , Volume: 87 Issue: 7 , July 1999, Page(s): 1079 -1107

[29] *S. Katzenseisser and F.A.P Petitcolas*, "Information Hiding Techniques for Steganography and Digital Watermarking", Artech House, Boston – London 2000

[30] *Kirovski, D.; Malvar, H.;* "Robust spread-spectrum audio watermarking", 2001. Proceedings. (ICASSP '01). 2001 IEEE International Conference on Acoustics, Speech, and Signal Processing, Volume: 3 , 7-11 May 2001, Page(s): 1345 -1348 vol.3

[31] *Kutter, M;Petitcolas, F.A.P.;* "A Fair Benchmark for Image Watermarking Systems," Security and Watermarking of Multimedia Contents, SPIE-3657:226-239, 1999

[32] *Hartung, F.; Girod, B;* "Digital Watermarking of MPEG-2 Coded Video in the Bitstream domain,", Proceedings of the IEEE International Conference on Acoustics, Speech and Signal Processing, Vol. 4, Munich, Germany, Apr. 1997, pp 2621-2624

[33] *Moulin, P.; O'Sullivan, J.A.;* "Information-theoretic analysis of information hiding", IEEE Transactions on Information Theory, Volume: 49 Issue: 3 , March 2003, Page(s): 563 -593

[34] *Nikolaidis, A.; Tsekeridou, S.; Tefas, A.; Solachidis, V.;* "A survey on watermarking application scenarios and related attacks", Image Processing, 2001. Proceedings. 2001 International Conference on , Volume: 3 , 7-10 Oct. 2001, Page(s): 991 -994 vol.3

[35] *O'Ruanaidh, J.J.K.; Pun, T.;* "Rotation, scale and translation invariant digital image watermarking" Image Processing, 1997. Proceedings., International Conference on , Volume: 1 , 26-29 Oct. 1997 Page(s): 536 -539 vol.1

[36] *Papadopoulos, H.C.; Sundberg, C.-E.W.;* "Simultaneous broadcasting of analog FM and digital audio signals by means of precanceling techniques",1998. ICC 98. Conference Record.1998 IEEE International Conference on Communications, Volume: 2 , 7-11 June 1998, Page(s): 728 -732 vol.2

[37] *Petitcolas, F.A.P.;* "Watermarking schemes evaluation", Signal Processing Magazine, IEEE , Volume: 17 Issue: 5 , Sept. 2000, Page(s): 58 -64

[38] *Piva, A.; Barni, M.; Bartolini, F.; Cappellini, V.;* "DCT-based watermark recovering without resorting to the uncorrupted original image", Image Processing, 1997. Proceedings., International Conference on , Volume: 1 , 26-29 Oct. 1997, Page(s): 520 -523 vol.1

[39] *Podilchuk, C.I.; Delp, E.J.;* "Digital watermarking: algorithms and applications" Signal Processing Magazine, IEEE , Volume: 18 Issue: 4 , July 2001, Page(s): 33 -46

[40] *Podilchuk, C.I.; Wenjun Zeng;* "Image-adaptive watermarking using visual models", IEEE Journal on Selected Areas in Communications, Volume: 16 Issue: 4, May 1998, Page(s): 525 -539

[41] *Ramkumar, M.; Akansu, A.N.; Alatan, A.A.;* "A robust data hiding scheme for images using DFT", Image Processing, 1999. ICIP 99. Proceedings. 1999 International Conference on , Volume: 2 , 24-28 Oct. 1999 Page(s): 211 -215 vol.2

[42] *Watson,A.B.;*"DCT Quantization Matrices Optimized for Individual Images", Human Vision, Visual Processing, and Digital Display IV, SPIE-1913:202, 1993

[43] *Wolfgang, R.B.; Podilchuk, C.I.; Delp, E.J.;* "Perceptual watermarks for digital images and video", Proceedings of the IEEE , Volume: 87 Issue: 7 , July 1999, Page(s): 1108 -1126

[44] *Wenwu Zhu; Zixiang Xiong; Ya-Qin Zhang;* "Multiresolution watermarking for images and video: a unified approach" Image Processing, 1998. ICIP 98. Proceedings. 1998 International Conference on , Volume: 1 , 4-7 Oct. 1998, Page(s): 465 -468 vol.1

[45] www.watermarkingworld.org

[46] http://watermarking.unige.ch/Checkmark/index.html

[47] http://poseidon.csd.auth.gr/optimark

[48] www.certimark.org