Digital Watermarking : A Tutorial Review

Saraju P. Mohanty *
Dept of Comp Sc and Eng.
Unversity of South Florida
Tampa, FL 33620
smohanty@csee.usf.edu

Abstract

The growth of high speed computer networks and that of Internet, in particular, has explored means of new business, scientific, entertainment, and social opportunities. Ironically, the cause for the growth is also of the apprehension - use of digital formatted data. Digital media offer several distinct advantages over analog media, such as high quality, easy editing, high fidelity copying. The ease by which a digital information can be duplicated and distributed has led to the need for effective copyright protection tools. Various software products have been recently introduced in attempt to address these growing concerns. It is done by hidding data (information) within digital audio, images and video files. One way such data hidding is **digital signature**, **copyright label** *or* **digital watermark**, *that completely characterizes the person who applies it and, therefore, marks it as being his intellectual property.* **Digital Watermarking** *is the process that embeds data called a watermark into a multimedia object such that watermark can be detected or extracted later to make an asertion about the object. Watermarking is either "visible" or "invisible". Although visible and invisible are visual terms watermarking is not limited to images, it can also be used to protect other types of multimedia object. This work is a tutorial review of the digital watermarking techniques appreared in the literature.*

1 Information Hiding Techniques

In this section, we briefly discuss the historical development of steganography / watermarking. We also introduce various data hiding terminologies used in current literature and attempt have clear distinction of them.

*This report was written in 1999 when the author was at the Indian Institute of Science, Bangalore

1.1 History of Information Hiding

The idea of communicating secretely is as old as communication itself. The earliest allusion to secret writing in the West appears in Homer's Ilaid [9]. Steganographic methods made their record debut a few centuries later in several tales by Herodotus, the father of history [10]. Some of them can also be found in [7, 19, 23]. Kautilya's Arthasa'stra and LalitaVista'ra, and Vatsa'yana's Ka'masu'tra are few famous examples of the Indian literature in which secret writting / steganography have been used.

Few other examples of steganography can be found in [7, 19, 23]. An important technique was the use of sympathetic inks. Ovid in his "Art of Love" suggests using milk to write invisibly. Later, chemically affected sympathetic inks were developed. This was used in World Wars 1 and 2. The origin of steganography is biological and physiological. The term "steganography" came into use in 1500's after the appearance of Trithemius' book on the subject "Steganographia". A whole other branch of steganography, "linguistic steganography", consists of linguistic or language forms of hidden writing. These are the "semagrams" and the "open code" [16, 19, 23]. A semagram is a secret message that is not in a written form. For example, a system can use long blades of grass in a picture as dashes in Morse code, with short blades for dots. People have also used musical notes for letters -but it doesn't look anything at all like music and it doesn't sound like music. Open codes use illuions or code words. In World War 1, for example, German spies used fake orders for cigars to represent various types of British warships-cruisers and destroyers. Thus 5000 cigars needed in Portsmouth meant that five cruisers were in Portsmouth.

Watermarking technique has eveloved from steganography. The use of watermarks is almost as old as paper manufacturing [32]. Our ancients poured their half-stuff slurry of fiber and water on to mesh molds to collect the fiber, then dispersed the slurry within deckle frames to add shape and uniformity, and finally applied great pressure to expel

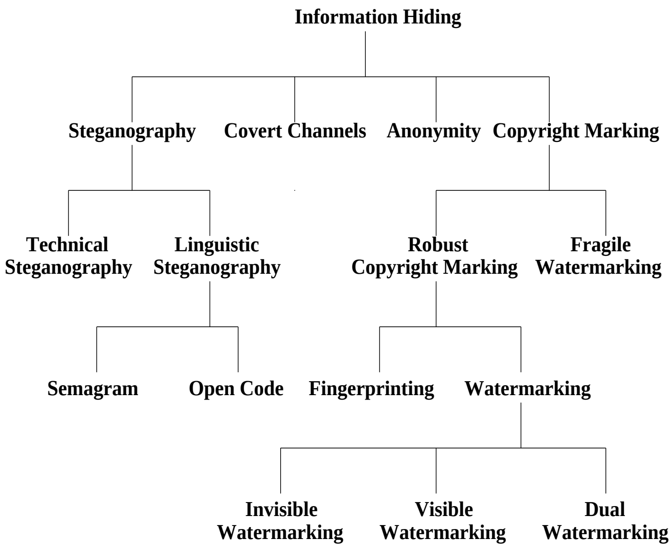


Figure 1: Information Hiding Techniques

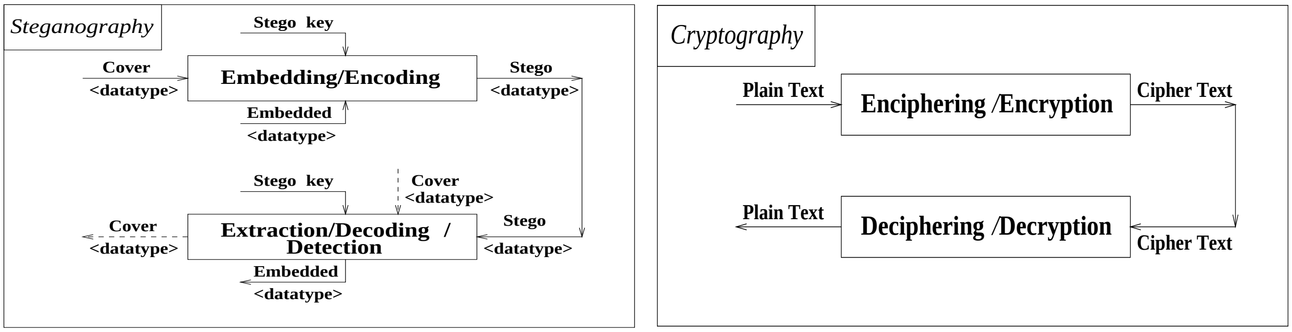
the water and cohere the fiber. This process hasn't changed too much in 2000 years. One by-product of this process is the watermark- the technique of impressing into the paper a form of image, or text derived from the negative in the mold, as the paper fibers are squeezed and dried. Paper Watermarks have been in wide use since the late Middle Ages. Their earliest use seems to have been to record the manufacturer's trademark on the product so that the authenticity could be clearly established without degrading the aesthetics and utility of the stock. In more recent times, watermarks have been used to certify the composition of paper, including the nature of the fibers used. Today most developed countries also watermark their paper, currencies and postage stamps to make forgery more difficult.

The digitization of our world has expanded our concept of watermarking to include immaterial digital impressions for use in authenticating ownership claims and protecting proprietary interests. However, in principle digital watermarks are like their paper ancestors. They signify something about the token of a document or file in which they inherit. Whether the product of paper press or discrete cosine transformations, watermarks of varying degree of visibility are added to presentation media as a guarantee of authenticity, quality ownership and source.

1.2 Information Hiding Terminology

In this section we will discuss diffrent information hiding terminology. The various information hiding techniques can be classified as given in Fig. 1.

- **Steganography** Steganogrphy is the art / science / study / work of communicating in a way which hides a secret message in the main information. Various steganography terminology is given in [16]. The model of steganography is given in Fig. 2(a).
  - **Embedded-<datatype>** Something to be hidden in something else.
  - **Stego-<datatype>** The output of hidding process; something that has the embedded message hidden in it.
  - **Cover-<datatype>** An inout which is an "original" form of the stego-<datatype>.
  - **Stegokey** Additional secret data that may be needed in the hiding process. The standard case where the same key is used in embedding and extracting is called symmetric.
  - **Embedding** The process of hiding the embedded message is called embedding.
  - **Extracting** Getting the embedded message out of the stegomessage again is called extracting.
  - **Stegoanalyst** The party from whom the embedded message is hidden is called the stegoanalyst.
  - **Embeddor/Extractor** An entity or person that embeds and extracts is called an embeddor or an extractor, respectively.
- **Steganography Vs Cryptography** To have a better understanding of the terms we compare "steganography" with "cryptography" (Fig. 2). The term steganography means "cover writing" whereas cryptography means "secret writing". Cryptography is the study of methods of sending messages in distinct form so that only the intended recipients can remove the disguise and read the message. The message we want to send is called plain text and disguised message is called cipher text. The process of converting a plain text to a cipher text is called enciphering or encryption, and the reverse process is called deciphering or decryption. Encryption protects contents during the transmission of the data from the sender to receiver. However, after receipt and subsequent decryption, the data is no longer protected and is the clear. Steganography hides messages in plain sight rather than encrypting tha message, it is embedded in the data (that has to be protected) and doesn't require secret transmission. The message is carried inside data. Steganography is therefore broader than cryptography. The schematic representation of the cryptography is given in Fig. 2(b).
- **Digital Watermarking** Watermarking is the process that embeds data called a watermark, tag or label into a



(a) Steganography

(b) Cryptography

Figure 2: Steganography Vs Cryptography

multimedia object such that watermark can be detected or extracted later to make an assertion about the object. The object may be an image or audio or video. It may also be text only

- **Steganography Vs Digital Watermarking** They primarily differ by intent of use. A watermark can be perceived as an attribute of the carrier (cover). It may contain information such as copright, license, trackning and authorship etc. Whereas in case of steganography, the embedded message may have nothing to do with the cover. In steganography an issue of concern is bandwidth for the hidden message whereas robustness is of more concern with watermarking.

- **Fingerprinting and Labelling** Fingerprints are also called labels by some authors. Digital watermarking differs from ”digital fingerprinting” [176]. Fingerprinting are characteristics of an object that tend to distinguish it from other similar objects. Fingerprinitng is the process of adding fingerprints to an object and recording them, or identifying and recording fingerprints that are already intrinsic to the object. Digital fingerprinting produces a metafile that describe the contents of the source file.

- **Digital Signature Vs Digital Watermark** There are conflicting view points about the ”digital signature”. Some authors use digital signature and digital watermark synonymously, whereas some authers distinguish between the digital signature and digital watermark. A digital signature is based upon the idea of public key encryption. A private key is used to encrypt a hashed version of the image. This encrypted file then forms a unique ”signature” for the image since only the entity signing the image has knowledge of the private key used. An assoiciated public key can be used to decrypt the signature. The image under question can be hashed using the same hashing function as used originally. If these hashes match then the image is authentic. Digital signature can be used for more than just image authentication. In particular when combined with secure timestamp, a digital signature can be used as a proof of first authorship. A watermark, on the other hand, is a code secretly embedded into the image. The watermark allows for verification of the origin of an image. However, a watermark alone is not enough to prove first authorship, since an image could be marked with multiple watermarks. It has also been pointed out in [18] that digital watermarks are not well suited to protect the authenticity of an image. The term ”embedded signature” has been used instead of ”watermarking” in early publications. Because it potentailly leads to confusion with cryptographic ”digital signatures”, it is not used anymore.

- **Electronic Stamp Vs Digital Watermark**

- **Covert Channel / Subliminal Channel**

  Details can be found in [178, 179, 180, 181] and many more works.

- **Anonymity**

  The readers are refferred to [177].

2 Introduction to Digital Watermarking

Digital watermarking technology is an emerging field in computer science, cryptography, signal processing and communications. Digital Watermarking is intended by its developers as the solution to the need to provide value added protection on top of data encryption and scrambling for content protection. Like other technology under development, digital watermarking raises a number of essential questions as follows.

- What is it?
- How can a digital watermark be inserted or detected?
- How robust does it need to be?
- Why and when are digital watermarks necessary?
- What can watermarks achieve or fail to achieve?
- How should digital watermarks be used?
- How might they be abused?
- How can we evaluate the technology?
- How useful are they, that is, what can they do for content protection in addition to or in conjunction with current copyright laws or the legal and judicial means used to resolve copyright grievances?
- What are the business opportunities?
- What roles can digital watermarking play in the content protection infrastructure ?
- And many more ...

3 General Framework for Watermarking

Watermarking is the process that embeds data called a watermark or digital signature or tag or label into a multimedia object such that watermark can be detected or extracted later to make an assertion about the object. The object may be an image or audio or video. A simple example of a digital watermark would be a visible ”seal” placed over an image to identify the copyright. However the watermark might contain additional information including the identity of the purchaser of a particular copy of the material.

In general, any watermarking scheme (algorithm) consists of three parts.

- The watermark.
- The encoder (insertion algorithm).
- The decoder and comparator (verification or extraction or detection algorithm).

Each owner has a unique watermark or an owner can also put different watermarks in different objects the marking algorithm incorporates the watermark into the object. The verification algorithm authenticates the object determining both the owner and the integrity of the object.

3.1 Encoding Process

Let us denote an image by I, a signature by $S = s_1, s_2, ...$ and the watermarked image by $\hat{I}$. E is an encoder function, it takes an image I and a signature S, and it generates a new image which is called watermarked image $\hat{I}$, mathematically,

$$E\left(I, S\right) = \hat{I} \quad (1)$$

It should be noted that the signature S may be dependent on image I. In such cases, the encoding process described by Eqn. 1 still holds. Following figure illustrates the encoding process.

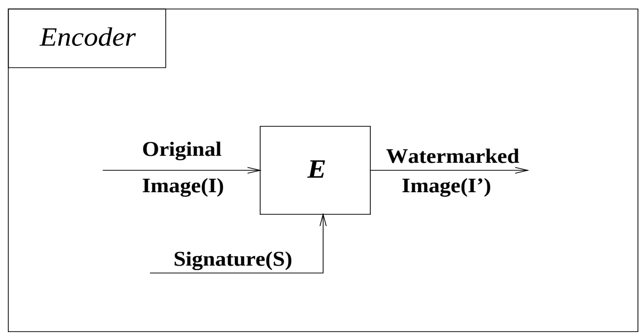


Figure 3: Encoder

3.2 Decoding Process

A decoder function D takes an image J (J can be a watermarked or un-watermarked image, and possibly corrupted) whose ownership is to be determined and recovers a signature S' from the image. In this process an additional image I can also be included which is often the original and un-watermarked version of J. This is due to the fact that some encoding schemes may make use of the original images in the watermarking process to provide extra robustness against intentional and unintentional corruption of pixels. Mathematically,

$$D\left(J, I\right) = S' \quad (2)$$

The extracted signature S' will then be compared with the owner signature sequence by a comparator function C_δ

and a binary output decision generated. It is 1 if there is match and 0 otherwise, which can be represented as follows.

$$C_\delta\left(S', S\right) = \begin{cases} 1, & \text{c} \leq \delta \\ 0, & \text{otherwise} \end{cases} \tag{3}$$

Where C is the correlator, $x = C_\delta\left(S', S\right)$. c is the correlation of two signatures and δ is certain thresold. Without loss of generality, watermarking scheme can be treated as a three-tupple (E, D, C_δ). Following figures demonstrate the decoder and the comparator.

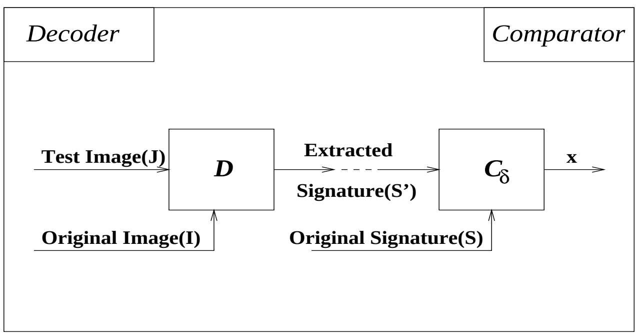


Figure 4: Decoder

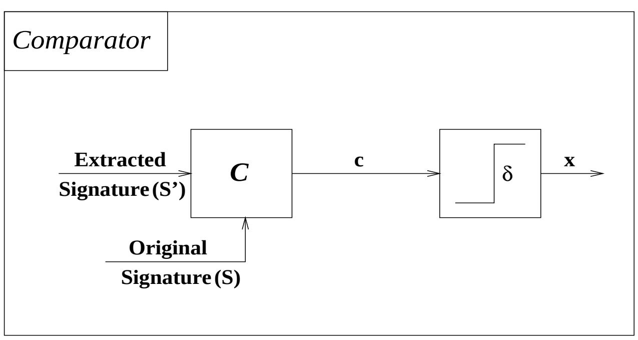


Figure 5: Comparator

A watermark must be detectable or extractable to be useful. Depending on the way the watermark is inserted and depending on the nature of the watermarking algorithm, the method used can involve very distinct approaches. In some watermarking schemes, a watermark can be extracted in its exact form, a procedure we call watermark extraction. In other cases, we can detect only whether a specific given watermarking signal is present in an image, a procedure we call watermark detection. It should be noted that watermark extraction can prove ownership whereas watermark detection can only verify ownership.

4 Types of Digital Watermarks

Watermarks and watermarking techniques can be divided into various categories in various ways. The watermarks can be applied in **spatial domain**. An alternative to spatial domain watermarking is **frequency domain** watermarking. It has been pointed out that the frequency domain methods are more robust than the spatial domain techniques. Different types of watermarks are shown in the figure below.

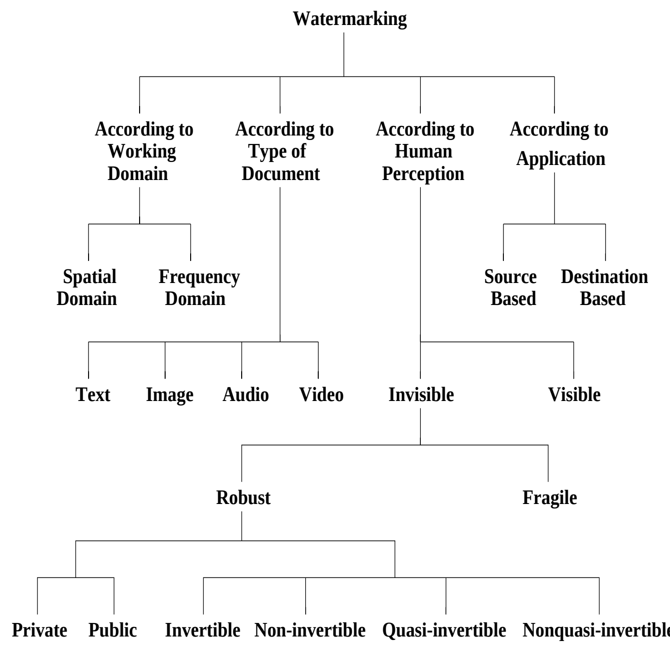


Figure 6: Types of watermarking techniques

Watermarking techniques can be divided into four categories according to the type of document to be watermarked as follows.

- Image Watermarking
- Video Watermarking
- Audio Watermarking
- Text Watermarking

According to the human perception, the digital watermarks can be divide into three different types as follows.

- Visible watermark
- Invisible-Robust watermark
- Invisible-Fragile watermark
- Dual watermark

Visible watermark is a secondary translucent overlaid into the primary image. The watermark appears visible to a casual viewer on a careful inspection. The **invisible-robust** watermark is embed in such a way that alternations made to the pixel value is perceptually not noticed and it can be recovered only with appropriate decoding mechanism. The **invisible-fragile** watermark is embedded in such a way that any manipulation or modification of the image would alter or destroy the watermark. Dual watermark is a combination of a visible and an invisible watermark [78]. In this type of watermark an invisible watermark is used as a back up for the visible watermark as clear from the following diagram.

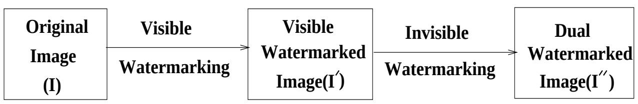


Figure 7: Schematic representation of dual watermarking

An invisible robust **private** watermarking scheme requires the original or reference image for watermark detection; whereas the **public** watermarks do not. The class of invisible robust watermarking schemes that can be attacked by creating a "counterfeit original" (to be discussed in later sections) is called **invertible** watermarking scheme. Using mathematical notations from Sec.3, an invisible robust watermarking scheme (E, D, C_δ) is called **invertible** if, for any watermarked image $\hat{I}$, there exits a function E^{-1} such that (1) $E^{-1}(\hat{I}) = (I', S')$, (2) $E(I', S') = (\hat{I})$ and (3) $C_\delta(D(\hat{I}), S') = 1$, where E^{-1} is a computationally feasible function, S' belongs to the set of allowable watermarks, and the images I and I' are perceptually similar. Otherwise, the watermarking scheme is **non-invertible**.

A watermarking scheme (E, D, C_δ) is called **quasi-invertible** if, for any watermarked image $\hat{I}$, there exits a function E^{-1} such that (1) $E^{-1}(\hat{I}) = (I', S')$, (2) $C_\delta(D(\hat{I}), S') = 1$, where E^{-1} is a computationally feasible function, S' belongs to the set of allowable watermarks, and the images I and I' are perceptually similar. Otherwise, the watermarking sheme is **nonquasi-invertible**.

From application point of view digital watermark could be as below.

- source based or
- destination based.

Source-based watermark are desirable for ownership identification or authentication where a unique watermark identifying the owner is introduced to all the copies of a particular image being distributed. A source-based watermark could be used for authentication and to determine whether a received image or other electronic data has been tampered with. The watermark could also be **destination-based** where each distributed copy gets a unique watermark identifying the particular buyer. The destination -based watermark could be used to trace the buyer in the case of illegal reselling.

5 Application of Digital Watermarks

5.1 Visible Watermark

Visible watermarks can be used in following cases :

- Visible watermarking for enhanced copyright protection. In such situations, where images are made available through Internet and the content owner is concerned that the images will be used commercially (e.g. imprinting coffee mugs) without payment of royalties. Here the content owner desires an ownership mark, that is visually apparent, but which does not prevent image being used for other purposes (e.g. scholarly research).

- Visible watermarking used to indicate ownership originals. In this case images are made available through the Internet and the content owner desires to indicate the ownership of the underlying materials (library manuscript), so an observer might be encouraged to patronize the institutions that owns the material.

5.2 Invisible Robust Watermark

Invisible robust watermarks find application in following cases.

- Invisible watermarking to detect misappropriated images. In this scenario, the seller of digital images is concerned, that his, fee-generating images may be purchased by an individual who will make them available for free, this would deprive the owner of licensing revenue.

- Invisible watermarking as evidence of ownership. In this scenario, the seller that of the digital images suspects one of his images has been edited and published without payment of royalties. Here, the detection of the seller's watermark in the image is intended to serve as evidence that the published image is property of seller.

5.3 Invisible Fragile Watermarks

Following are the applications of invisible fragile watermarks.

- Invisible watermarking for a trustworthy camera. In this scenario, images are captured with a digital camera for later inclusion in news articles. Here, it is the desire of a news agency to verify that an image is true to the original capture and has not been edited to falsify a scene. In this case, an invisible watermark is embedded at capture time; its presence at the time of publication is intended to indicate that the image has not been attended since it was captured.

- Invisible watermarking to detect alternation of images stored in a digital library. In this case, images (e.g. human fingerprints) have been scanned and stored in a digital library; the content owner desires the ability to detect any alternation of the images, without the need to compare the images to the scanned materials.

6 Attacks on Watermarks

A watermarked image is likely to be subjected to certain manipulations, some intentional such as compression and transmission noise and some intentional such as cropping, filtering, etc. They are summarized in Fig.8.

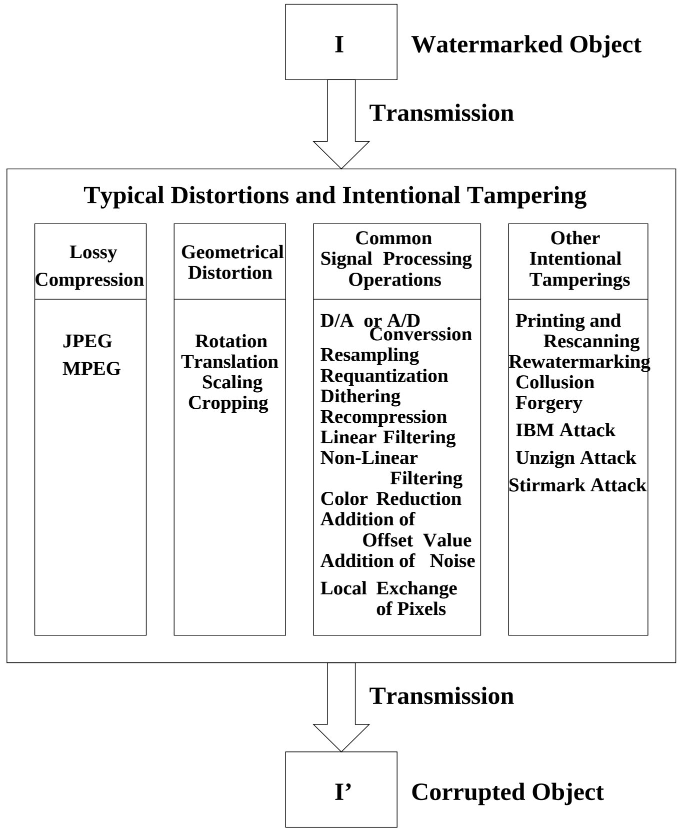


Figure 8: Attacks on watermarks

- Lossy Compression: Many compression schemes like JPEG and MPEG can potentially degrade the data's quality through irretrievable loss of data.

- Geometric Distortions: Geometric distortions are specific to images videos and include such operations as rotation, translation, scaling and cropping.

- Common Signal Processing Operations: They include the followings.
  - D/A conversion
  - A/D conversion
  - Resampling
  - Requantization
  - Dithering distortion
  - Recompression
  - Linear filtering such as high pass and low pass filtering
  - Non-linear filtering such as median filtering
  - Color reduction
  - Addition of a constant offset to the pixel values
  - Addition of Gaussian and Non Gaussian noise
  - Local exchange of pixels

- Other intentional attacks:
  - Printing and Rescanning
  - Watermarking of watermarked image (rewatermarking)
  - Collusion: A number of authorized recipients of the image should not be able to come together (collude) and like the differently watermarked copies to generate an un-watermarked copy of the image (by averaging all the watermarked images).
  - Forgery: A number of authorized recipients of the image should not be able to collude to form a copy of watermarked image with the valid embedded watermark of a person not in the group with an intention of framing a 3rd party.
  - IBM attack [155, 157] : It should not be possible to produce a fake original that also performs as

well as the original and also results in the extraction of the watermark as claimed by the holder of the fake original.

– The Unzign and Stirmark have shown remarkable success in removing data embedded by commercially available programs.

7 Desired Characteristics of Watermarks

7.1 Desired Characteristics of Visible Watermarks

- A visible watermark should be obvious in both color and monochrome images.
- The watermark should spread in a large or important area of the image in order to prevent its deletion by clipping.
- The watermark should be visible yet must not significantly obscure the image details beneath it.
- The watermark must be difficult to remove. Rather, removing a watermark should be more costly and labor intensive than purchasing the image from the owner.
- The watermark should be applied automatically with little human intervention and labor.

7.2 Desired Characteristics of Invisible Robust Watermarks

- The invisible watermark should neither be noticeable to the viewer nor should degrade the quality of the content.
- An invisible robust watermark must be robust to common signal distortions and must be resistant to various intentional tamperings solely intended to remove the watermark.
- Retrieval of watermark should unambiguously identify the owner.
- It is desirable to design a watermark whose decoder is scalable with each generation of computer.
- While watermarking high qulaity images and art works the amount of pixel modification should be minimum.
- Insertion of watermark should require little human intervention or labor.

7.3 Desired Characteristics of Invisible Fragiles Watermarks

- The invisible watermark should neither be noticeable to the viewer nor should degrade the quality of the content.
- An invisible fragile watermark should be readily modified when the image pixel values have been altered.
- The watermark should be secure. This means that it is impossible to recover the changes, or regenerate the watermark after image alternations, even when the watermarking procedure, and/or the watermark itself is known.
- For high quality images, the amount of individual pixel modification should be as small as possible.

7.4 Desired Characteristics of Video Watermarks

- The presence of watermark should not cause any visible or audible effects on the playback of the video.
- The watermark should not afftect the compressibilty of the digital content.
- The watermark should be detected with high degree of reliability. The probablity of false detection should be extremely small.
- The watermark should be robust to various intentional and unintenional attacks.
- The detection algorithm should be implemented in circuitry with small extra cost.

8 Image Watermarking

There are plenty of image watermarking techniques algorithms available in current literature. In this section we will discuss a few of them. We focuse on one visible watermarking scheme, few invisible watermarking scheme and the dual watermarking scheme in [78].

M.Kankanhalli, et al. [77] have developed a visible watermarking technique. They divide the host image into different blocks, find the DCT of each block. Then they classify the blocks into six different classes in the increasing order of noise sensitivity, such as edge block, uniform with moderate intensity, uniform with high or low intensity, moderate busy, busy and very busy. Each block is then assigned

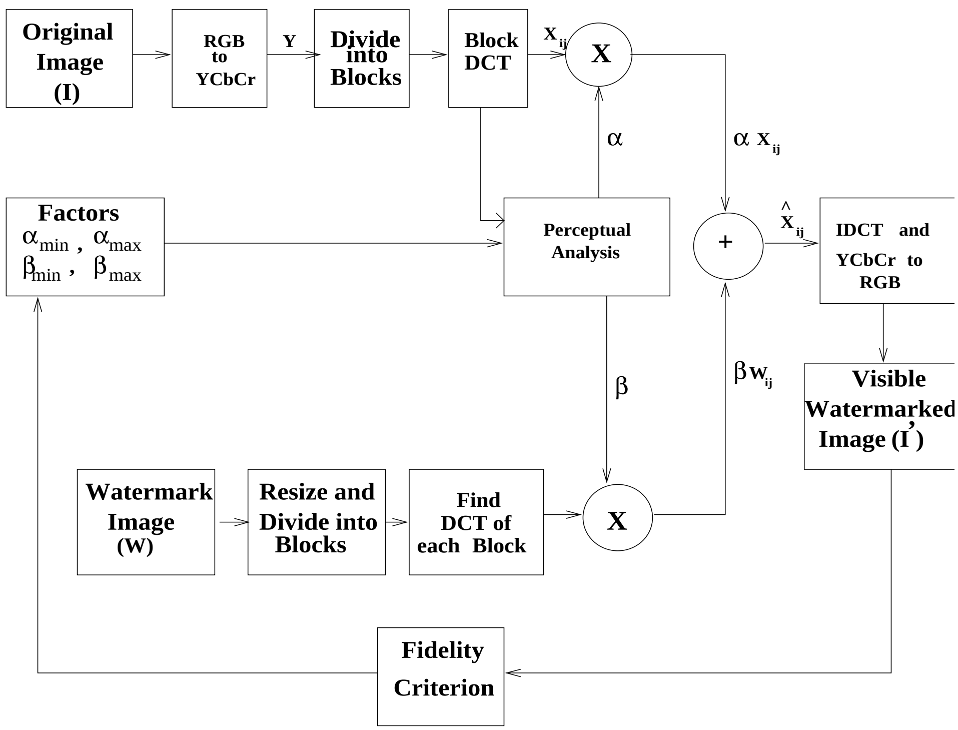


Figure 9: Schematic representaion of visible watermarking algorithm of [77]

different α and β values. The host image blocks are then modified as follow:

$$\hat{X}_{ij} = \alpha X_{ij} + \beta W_{ij} \tag{4}$$

where $\hat{X}_{ij}$ is the i, j DCT co-efficient of the watermarked image, X_{ij} is the corresponding DCT co-efficient of the original image and W_{ij} is the DCT co-efficient of the watermark image. Fig. 9 gives the schematic representation of the technique and Fig. 10 show various results.

I.J.Cox et al. [84, 85, 98] propose an invisible robust watermarking technique. They insert the watermark into the spectral components of the image using technique analogous to spread spectrum communication. The argument is that the watermark must be inserted in the perceptually significant components of a signal if it os to be robust to common signal distortions and malicious attacks. However, the modification of these components may lead to perceptual degradation of the signal. The watermark insertion consists of following steps:

- DCT of the entire original image is computed assuming as on block.
- The perceptually significant regions of the image are found out. The authors have used 1000 largest coefficients.
- The watermark $X = x_1, x_2, ..., x_n$ is computed where each x_i is chosen according to $N(0, 1)$, where $N(0, 1)$ denotes a normal distribution with mean 0 and variance 1.
- The watermark is inserted in the DCT domain of the image by setting the frequency components v_i in the original image to v'_i using the following eqn.

  $$v'_i = v_i\,(1 + \alpha x_i) \tag{5}$$

  where α is a scalar factor.

The author has chosen $\alpha = 0.1$. A Gaussian type of wateramark is used because it is more robust to tampering than uniform type. Extraction of watermark consists of following steps:

- DCT of the entire watermarked image is computed assuming as one block.

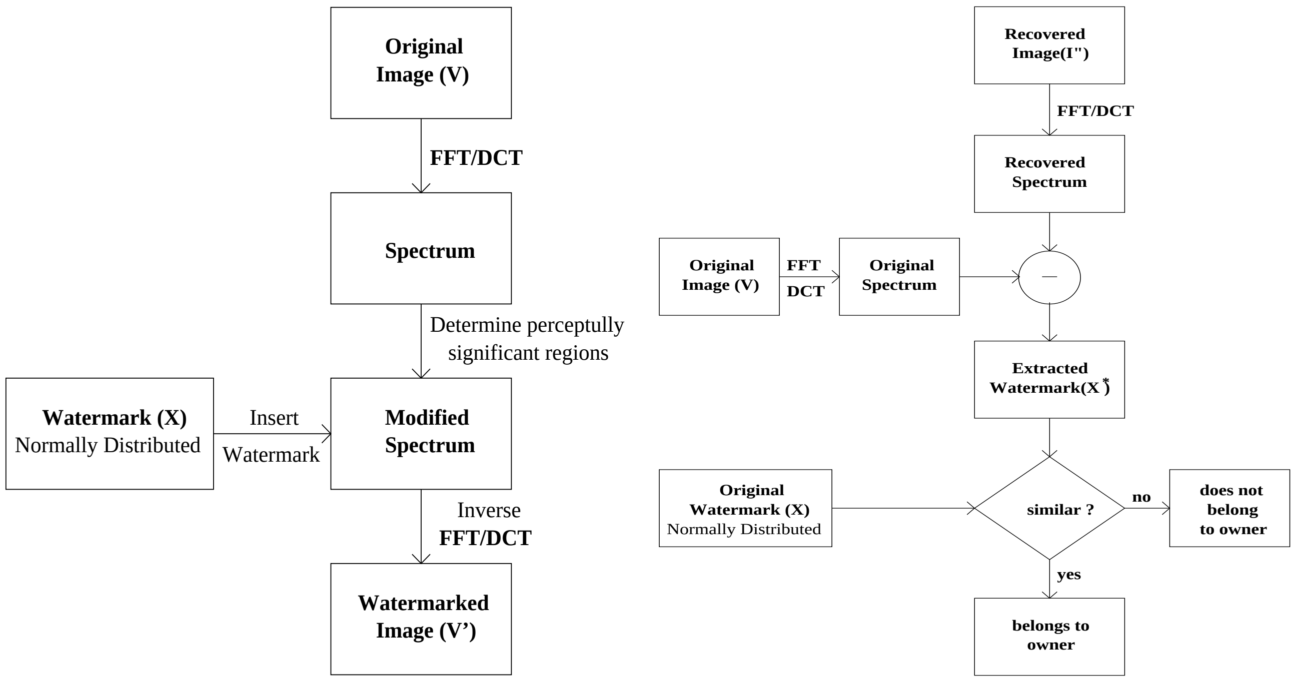
(a) Original image

(b) Watermark images

(c) Bigger watermark

(d) Smaller watermark

Figure 10: Visible watermarked ”Lena” [77]



(a) Insertion process

(b) Extraction process

Figure 11: Schematic representaion of watermarking scheme of [84, 85, 98]

- DCT of the entire original image is computed assuming as one block.
- The difference of the two is the watermark X^*.

The extracted watermark X^* is compared with the original watermark X using similarity function given in eqn.6.

$$sim\left(X, X^*\right) = \frac{\left(XX^*\right)}{sqrt\left(XX^*\right)} \tag{6}$$

The watermark is robust to common signal and geometric distortion such as A/D and D/A conversion, resampling, quantization, compression, rotation, translation, cropping and scaling. The watermark is universal in the sense that it can be applied to all three media. Retrieval of the watermark unambigously identifies the owner and the watermark can be constructed to make counterfeiting almost impossible. The watermarking technique has the disadvantage that it needs the original image for its exatraction. It is also not clear whether the watermark is robust to photocopying. Fig. 11(a) and Fig. 11(b) give the schematic represenation of the insertion and extraction process, respectively. The original image and the watermarked images are given in Fig. 12.

R.B.Wolfgang and E.J.Delp [101, 102] have developed one invisible watermarking technique that works in the spatial domain. Fig.13 shows image watermarked using this algorithm. The watermark insertion proces has following steps:

- The watermark is created by arranging a longer m-sequence row by row into two dimenional blocks.
- The watermark is then added to the image. The size of the watermark should be same as the size of the image.
- The authers define the spatial cross-correlation function of the images X and Y as:

$$R_{xy}\left(\alpha, \beta\right) = \sum_i \sum_j X\left(i, j\right) Y\left(i - \alpha, j - \beta\right) \tag{7}$$

Let X be the original image block, W be the watermark block, Y be the watermarked image block and Z be the watermarked image that might be forged. The test statistics for a block is defined as:

$$\delta = R_{yw}\left(0, 0\right) - R_{zw}\left(0, 0\right) \tag{8}$$

The mean δ for all blocks is found as follows:

$$E\left[\left|\delta_k\right|\right] = \frac{1}{N}\sum_{i=1}^{N} \delta_k \tag{9}$$

(a) Original

(b) Watermarked

Figure 12: Original and watermarked ”shuttle” [84, 85, 98]

(a) Original

(b) Watermarked

Figure 13: Original and watermarked ”bird” [101, 102]

where δ_k is the value of δ for the k^{th} block and N is the number of 8×8 blocks in the image.

- A testing paradigm is found out with different ranges of $E[|\delta_k|]$. The image is declared to be fully authentic, authentic but forged, possible authentic and completely inauthentic using this testing paradigm.

W.Zhu, et al. [118, 119] propose an invisible wateramrking technique which is very much similar to that of [84, 85, 98], but the watermark is inserted to wavelet co-efficients. The diffrence between this algorithm and that of [84, 85, 98] is that in later case the watermark (gussian random number) has been added to the small number of percetually significant co-efficients whereas in former case the watermark is added to the every high-pass wavelet co-efficients.

I.Pitas, et al. [42, 103, 104, 105] use an approach that allows slightly more information to be embedded. A binary signature that consists of equal number of zeros and ones is embedded in an image by assigning pixels into one of the two sets. The intensity levels of pixels in one of the sets are altered. The intensity levels are not changed in the other set. Signature detection is done by comparing mean intensity value of the marked pixels againast that of the not marked pixels. Statistical hypothesis testing is used for this purpose. The signature can be designed in such a way that it is resistant to JPEG compression and low pass filtering. According to the authers, the degree of certianty can be as low as 84% and as high as 92%, which would likely not stand up as evidence in a court of law for copyright protection. But, the algorithm has the advantage that it doesn't need the original image for wateramark detection.

S.P.Mohanty, et al. [78] propose a new watermarking technique called *dual watermarking*. The dual watermarking is combination of a visible watermark and an invisible watermark. The invisible watermark is used as protection or back up for the visible watermark. The dual watermark insertion process has the following steps:

i. Both host image (one to be watermarked) I and the watermark (image) W are divided into blocks of equal sizes (the two images may be of unequal size).

ii. Let i_n denote the n^{th} block of the original image I and ω_n denote the n^{th} block of the watermark W. For each block (i_n), the local statistics; mean μ_n and variance σ_n are computed. The image mean gray value μ is also found out.

iii. The watermarked image block is obtained by modifying i_n as follows.

$$i'_n = \alpha_n i_n + \beta_n \omega_n \quad n = 1, 2... \tag{10}$$

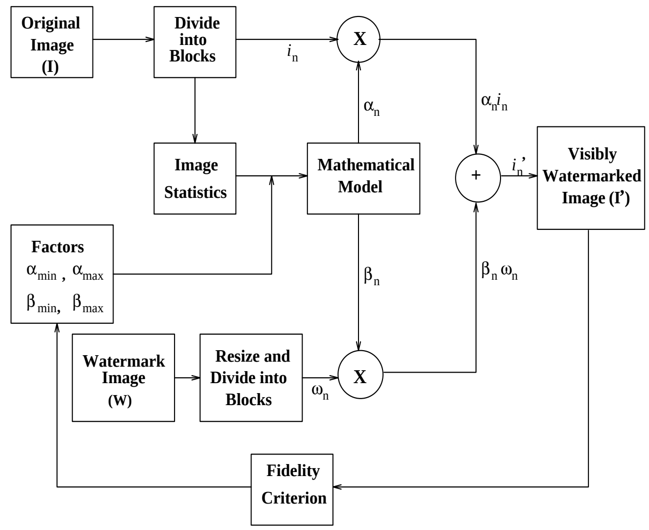


Figure 14: Schematic representation of visible watermark insertion process [78]

where α_n and β_n are scaling and embedding factors respectivley, depending on μ_n and σ_n of each block. The α_n and β_n are obtained as follows:

- The α_n and β_n for edge blocks are taken to be α_{max} and β_{min} respectively.
- The α_n and β_n are found out using the following eqns.

$$\alpha_n = \frac{1}{\hat{\sigma_n}} exp\left(-(\hat{\mu_n} - \hat{\mu})^2\right) \tag{11}$$

$$\beta_n = \hat{\sigma_n}\left(1 - exp\left(-(\hat{\mu_n} - \hat{\mu})^2\right)\right) \tag{12}$$

  where $\hat{\mu_n}$, $\hat{\mu}$ are normalised values of μ_n and μ, and $\hat{\sigma_n}$ are normalised logarithm values of σ_n.

- The α_n and β_n are scaled to the ranges (α_{min},α_{max}) and (β_{min}, β_{max}) respectively, where α_{min} and α_{max} are minimum and maximum values of scaling factor, and β_{min} and βmax minimum and maximum values of embedding factor. These are the parameters determining the extent of watermark insertion.

The image thus obatained is visible watermarked image I'.

iv. Pseudo-random binary-sequence {0,1} of period N is generated using linear shift register [55, 56]. The period N is equal to the number of pixels of the image.

v. The watermark is generated by arranging the binary sequence into blocks of size 4×4 or 8×8. The size of the watermark is same as the size of the image.

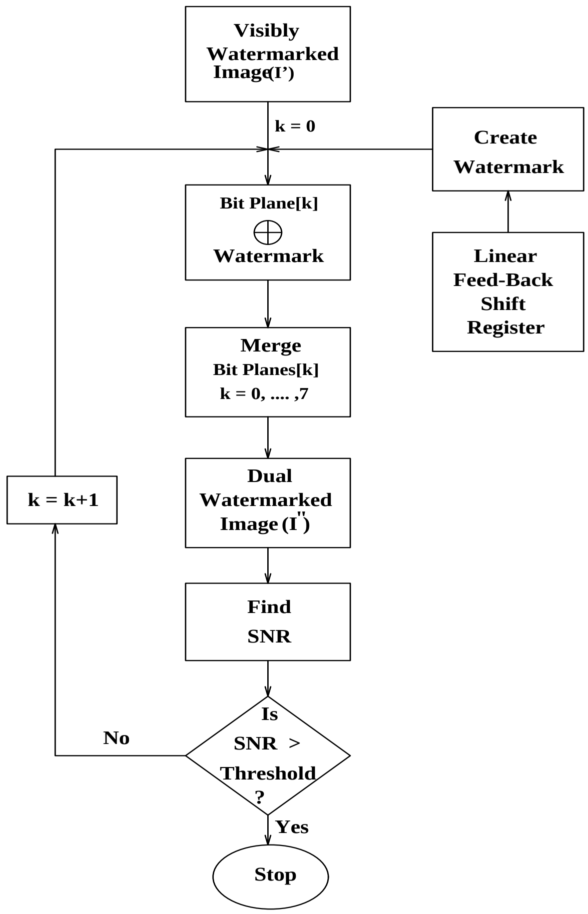


Figure 15: Schematic representation of Invisible watermark insertion process [78]

vi. We start with bit-plane $k = 0$ (MSB) of the image I'.

vii. The watermark is EX-ORed with the k^{th} bit-plane of the image.This gives the k^{th} bit-plane for watermarked image.

viii. The above watermarked k^{th} bit-plane and the remaining bit-planes of the image I' are merged to find the final watermarked image I''.

ix. The SNR is found out. If SNR $>$ theshold, then we stop; otherwise we go to (vii) with k incremented by 1 (for next lower bit-plane). The dual watermarked image I" is finally obtained.

The shematic represenatation of the watermarking insertion steps are given in Fig.14 and Fig.15. Fig.16 shows dual watermarked "Lena" and "bird". For watermark detection a testing paradigm similar to [101, 102] is used.

9 Video Watermarking

In this section we will discuss some of the video watermarking techniques available in current litearture. I.J.Cox et al. [84, 85, 98] algorithm also works for video if watermarking is done framewise.

F.Hartung and B.Girod [136, 137, 138, 139, 140] present a scheme for robust watermarking of MPEG-2 video. The watermark is either embedded into the encoded video or into the MPEG-2 bit streams and can be retreived from the codec video. The basic idea of *watermarking for raw video* is addition of pseudo-random signal to the video that is below the threshold of perception that can't be identified and thus removed without knowledge of the parameters of the watermarking algorithm. The approach to accomplish this is a direct extension from direct-sequence spread spectrum communications. The marking of raw video data v_i to produce a modified signal v'_i is described by eqn.13.

$$v'_i = v_i + \alpha b_i p_i \tag{13}$$

where p_i is the pseudo-noise sequence, b_i is the embedded bit and α is amplitude-scaling factor. The information bit recovered by a matched filter. Given several sequences with differnent watermarks, it is easier to figure out the watermarked pixel values if the watermark consists only of the -1's and 1's. In the *bit stream domain* it is more difficult to embed a watermark into video, especially when the requirement is imposed that the bit reat may not be incersed. For each signal block, the watermarking procedure consists of the folloing steps:

i. The DCT of the watermark data (of the spread information bits modulated by the pseudo-noise sequence) is calculated for 8×8 block. A zigzag scan is done to get a 1×16 vectro of rescanned DCT co-efficients. The DCT co-efficients are denoted by W_n with W_0 being DC co-efficient and W_{63} being the AC co-efficients. The DCT co-efficients of the unwatermarked signal are denoted by V_n and that of the watermarked signal by V'_n.

ii. For DC co-efficients, the mean value of the watermark block is added to the mean value of the signal block, i.e.

$$V'_n = V_0 + W_0 \tag{14}$$

iii. For the AC co-efficients, the bit stream of the coded signal is searched for the next VLC codeward, the (run-level) pair (r_m, l_m) belongs to that codeword is identified and thus the position and amplitude of the AC DCT co-efficients represneted by the VLC codeword.

(a) Lena

(b) Bird

Figure 16: Dual watermarked ”Lena” and ”bird” [78]

iv. $V'_m = V_m + W_m$ is the candidate DCT co-efficient for the watermarked signal. However, V'_m should not increase the bit-rate.

v. Let R be the number of bits used for transmitting the codeword for (r_m, l_m) (i.e. for V_m) and R' be the number of bits used for transmitting the codeword for (r_m, l'_m) (i.e. V'_m. If $R \geq R'$ the codeword for (r_m, l'_m) else the codeword for (r_m, l_m) transmitted.

vi. Steps (iii)-(v) are repeated until end of block (EOB) codeword is encountered.

Due to bit rate constraint, usually only few DCT coefficients of the watermark can be incorprated per 8×8 block. As a result, **the watermarking sheme in bit stream domain is less robust than its counterpart in the pixel domain**. But the scheme working on encoded video is of mush lower complexity than a complete decoding process followed by watermarking inn the pixel and recording. Although an existing MPEG-2 bitstream is partly altered the scheme avoids drift problems. The authors have suggested schemes for drift compensation in [139]. The embedded watermark can be retreived from the watermarked video without knowledge of the original video. The watermark is robust agianst the linear and non-linear operations like further transform coding, filtering, quantization, modest rotation etc.

M.D.Swanson, et al. [141] propose an object based watermarking technique for video, Individual watermarks are created for objects within the video. Each watermark is created by shaping an author and video dependent pseudorandom sequence according to the perceptual masking characteristics of the video. The insertion procedure has following steps :

- The spatial (S) and frequency (M) masking values for the current frames are computed. The frequency masking values are obtained from DCT co-efficeints of 8×8 blocks in the frame.
- The frame segmented to block (B) to ensure that masking estimates are localized.
- Each block of frequency masking values is then multilpied by part of pseudo-random author representation.
- The inverse DCT of the product (P) is computed.
- The result is multiplied by the spatial masking values for the frame, creating the perceptually shaped pseudonoise (W).
- The pseudo-noise is added to the blocks of the frame to get watermarked block B'.
- The watermark for a macroblock in the current frame is replaced for the watermark for the macroblock from

the previous frame if the distortion $D(V)$ is less than threshold T.

Detection of watermark is accomplished via generalized likelihood ration test. The watermark is statistically undetectable. The watermark also resolves multiple ownership claims. The watermark algorithm may be easily incorporated into the MPEG-4 object based coding framework. The watermarking procedure is robust to video degradations that result from noise, MPEG compression, cropping, printing and scanning.

C.T.Hsu and J.L.Wu [144] present a DCT based watermarking technique for video sequences. The steps for watermarking insertion are given below.

- The original image is divided into 8×8 blocks and the 2-D DCT is applied independently to each block.
- The middle frequency range co-efficients are picked up.
- A 2-D sub-block is used in order to compute the residual pattern from the chosen middle frequency coefficeints.
- The watermark is a binary image. A fast 2-D pseudorandom number traversing method is used to permute the watermark so as to disperse its spatial relationship.
- Bith variances of image block and watermark blocks are sorted and mapped accordingly so that the inisiblity of the watermarked image will improve.
- After binary residual patterns of the transoform intraframe are obtained, for each marked pixel of the permuted watermark, the DCT co-efficeints are modified according to the residual mask so that corresponding polarity of the residual value is reversed.
- Inverse DCT value of the associated result is calculated to obtian the watermarked image. For P-frame, modifying the temporal relationship between the current P-frame and its reference frame embeds the watermark.
- For B-frame, the residual mask is designed between the current B-frame and its past and future reference frame. The polarity of the residual frame is also reveersed to embed the watermark.

The extraction procedure is simply the reverse operation of insertion procesure. This requires the original frame, then watermarked frame and also the digital watermark, which is a disadvantage of this watermarking scheme. The scheme is robust to cropping operation and MPEG compression.

10 Audio Watermarking

The author didn't work in this area, but will address the schemes whenever time permits.

11 Text/Document Watermarking

The author didn't work in this area, but will address the schemes whenever time permits.

12 VLSI Implmentation of Watermarking Schemes

Hopefully some work will appear in future.

13 Limitation of Watermarks

There are plenty of works available in the reference.

14 Conclusions

The watermarking research is progressing very fast and numerous researcher from various fields are focussing to develop some workable scheme. Different companies also working to get commercial products. We hope some commercial and effective schemes will be available in future.

References

[1] A.Papoulis, ”Probability, Random Variables and Stochastic Processes”, McGraw Hill Inc., 3rd Edn., 1991.

[2] R.C.Gonzalez and R.E.Woods, ”Digital Image Processing”, Addison-Wesley Publishing company, Inc., 1993.

[3] A.K.Jain, ”Fundamentals of Digital Image Processing”, Prentice-Hall of India Pvt. Ltd., 1995

[4] Neal Koblitz, ”A Course in Number Theory and Cryptography”, Springer-Verlag.

[5] V. K. Rohatgi, ”An Introduction to Probability Theory and Mathematical Statistics”, Wiley Eastern Ltd., 1993.

[6] A.M.Tekalp, ”Digital Video Processing”, Printice Hall, Englewood Cliffs, NJ, 1995.

[7] David Kahn, ”Codebreakers : Story of Secret Writting”, Macmillan 1967.

[8] F.L.Bauer, ”Decrypted Secrets-Methods and Maxims of Cryptology”, Berlin, Heidelberg, Germany: Springer-Verlag, 1997.

[9] Homer, ”The Iliad” (trans. R. Fragels), Middlesex, England: Penguin 1972.

[10] Herodotus, ”The Histories” (trans. R. Selincourt), Middlesex, England: Penguin 1972.

[11] R. G. Gallager, ”Information Theory and Reliable Communication”, Wiley, 1968.

[12] J. G. Proakis, ”Digital Communications”, McGraw-hill 1995, 3rd ed.

[13] A. J. Viterbi, ”CDMA Principles of Spread Spectrum Communications”, Addison-Wesley Inc., 1995.

[14] Rajmohan, ”Watermarking of Digital Images”, ME Thesis Report, Dept. Electrical Engineering, Indian Institute of Science, Bangalore, India, 1998.

[15] S.P.Mohanty, ”Watermarking of Digital Images”, Masters Project Report, Dept. of Electrical Engineering, Indian Institute of Science, Bangalore - 560 012, India, Jan 1999.

[16] B.Pfitzmann, ”Information Hiding Terminology”, *Proc. of First Int. Workshop on Information Hiding*, Cambridge, UK, May30-June1, 1996, Lecture notes in Computer Science, Vol.1174, Ross Anderson(Ed.), pp.347-350.

[17] W. Bendor, et. al., ”Techniques for Data Hiding”, *IBM Systems Journal*, Vol.35, No.3 and 4, pp. 313-336, 1996.

[18] B.M.Macq and J.J.Quisquater, ”Cryptography for Digital TV Broadcasting”, *Proc. of the IEEE*, Vol.83, No.6, June 1995, pp. 944-957.

[19] David Kahn, ”The History of Steganography”, *Proc. of First Int. Workshop on Information Hiding*, Cambridge, UK, May30-June1 1996, Lecture notes in Computer Science, Vol.1174, Ross Anderson(Ed.), pp.1-7.

[20] R.J. Anderson and Fabien A.P. Petitcolas, ”On the Limits of Steganography”, *IEEE Journal on Selected Areas in Comm.*, Vol.16, No.4, May 1998, pp.474-481.

[21] R.J. Anderson, ”Stretching the Limits of Steganography”, *Proc. of First Int. Workshop on Information Hiding*, Cambridge, UK, May30-June1 1996, Lecture notes in Computer Science, Vol.1174, Ross Anderson(Ed.).

[22] E. Franz, et. al., ”Computer Based Steganography”, *Proc. First Intl. Workshop on Information Hiding*, Cambridge, UK, May 30 - June 1, 1996, Lecture notes in Computer Science, Vol.1174, Ross Anderson(Ed.).

[23] F.A.P.Petitcolas, et al., ”Information Hiding - A Survey”, *Proceedings of the IEEE*, Vol.87, No.7, July 1999, pp.1062-1078.

[24] C.Cachin, ”An Information-Theoritic Model for Steganography”, Proc. of the 2nd International Workshop on Information Hiding, Portland, Oregon, USA, 15-17 Apr 1998, Lecture notes in CS, Vol.1525, Springer-Verlag.

[25] S.Craver, ”On Public-Key Steganography in the Presence of an Active Warden”, Proc. of the 2nd International Workshop on Information Hiding, Portland, Oregon, USA, 15-17 Apr 1998, Lecture notes in Comp Sc, Vol.1525, Springer-Verlag.

[26] N.F.Johnson and Sushil Jajodia, ”Exploring Steganography: Seeing the Unseen”, IEEE Computer, Vol.31, No.2, pp.26-34, feb.1998.

[27] N.Paskin, ”Towards Unique Identifiers”, *Proceedings of the IEEE*, Vol.87, No.7, July 1999, pp.1208-1227.

[28] K.Hill, ”A Perspective: The Role of Identifiers in Managing and Protecting Intellectual Property in the Digital Age”, *Proceedings of the IEEE*, Vol.87, No.7, July 1999, pp.1228-1238.

[29] P.B.Schneck, ”Persistent Access Control to Prevent Piracy of Digital Information”, *Proceedings of the IEEE*, Vol.87, No.7, July 1999, pp.1239-1250.

[30] D.Augot, et al., ”Secure Delivery of Images over Open Network”, *Proceedings of the IEEE*, Vol.87, No.7, July 1999, pp.1251-1266.

[31] M.D.Swanson, et al., ”Multimedia data Embedding and Watermarking Technologies”, *Proc. of the IEEE*, Vol.86, No.6, June 1998, pp.1064-1087.

[32] Hal Berghel, ”Watermarking Cyberspace”, *Communications of the ACM*, Nov.1997, Vol.40, No.11, pp.19-24.

[33] M.M.Yeung, "Digital Watermarking",*Communications of the ACM*, Jul.1998, Vol.41, No.7, pp.31-33.

[34] N.Memon and P.W.Wong, "Protecting Digital Media Content", *Communications of the ACM*, July 1998, Vol.41, No.7, pp.35-43.

[35] M.M Yeung, et al. "Digital Watermarking for High-Quality Imaging", *IEEE First Workshop on Multimedia Signal Processing*, June23-25 1997, Princeton, New Jersey, pp. 357-362.

[36] F. Mintzer, et.al., "Effective and Ineffective Digital Watermarks", *IEEE Intl. Conference on Image Processing, ICIP-97*, Vol.3, pp.9-12.

[37] J. Zhao, et. al., "In Business Today and Tommorrow", *Communications of the ACM*, July 1998, Vol.41, No.7, pp.67-72.

[38] J. M. Acken, "How Watermarking Value to Digital Content?", *Communications of the ACM*, July 1998, Vol.41, No.7, pp.75-77.

[39] S. Craver, et. al., "Technical Trials and Legal Tribulations", *Communications of the ACM*, July 1998, Vol.41, No.7, pp.45-54.

[40] I. J. Cox and M. Miller, "A Review of Watermarking and Importance of Perceptual Modelling", *Proc. SPIE Human Vision and Imaging*, SPIE-3016, Feb 1997.

[41] F. Mintzer, et. al., "Opportunities for Watermarking Standards", *Communications of the ACM*, July 1998, Vol.41, No.7, pp.57-64.

[42] G.Voyatzis and I.Pitas, "Protecting Digital Image Copyrights: A Framework", *IEEE Computer Graphics & Applications*, Jan/Feb 1999, pp.18-24.

[43] C.Busch, et al., "Digital Watermarking: From Concepts to Real-Time Video Applications", *IEEE Computer Graphics & Applications*, Jan/Feb 1999, pp.25-35.

[44] F.Bartolini, et al., "Mask Building for Perceptually Hiding Frequency Embedded Watermarks", *Proc. IEEE International Conference on Image Processing, ICIP-98*, Vol.1, pp.450-454.

[45] R.Barnett, "Digital Watermarking : application, techniques, and challengs", *IEE Electronics and Communication Engineering Journal*, August 1999, pp.173-183.

[46] Ton Kalker, et al., "Watermark Estimation Through Detector Analysis", *Proc. IEEE International Conference on Image Processing, ICIP-98*, Vol.1, pp.425-429.

[47] F.Mintzer, et al., "Safegaurding Digital Library Contents and Users : Digital Watermarking", D-Lib Magazine, December 1997, http://www.dlib.org/dlib/december97/ibm/12lotspiech.html

[48] C. F. Osborne, et al., "Image and Watermark Registration for Monochrome and Coloured Images", Digital Image Computing, Technology and Applications, Wellington New Zealand, 1997, pp.59-64

[49] A.Z.Tirkel, et al., "Image and Watermark Registration", Signal Processing, Vol.66, No.3, May 1998, pp.373-384.

[50] Jian Zhao, "Look, Its Not Therae", *BYTE Magazine*, January, 1997, pp.401-407, http://www.byte.com/art/9701/sec18/art1.htm

[51] F.Hartung and M.Kitter, "Multimedia Watermarking Techniques", *Proceedings of the IEEE*, Vol.87, No.7, July 1999, pp.1079-1107.

[52] R.B.Wolfgang, et al., "Perceptual Watermarking for Digital Images and Video", *Proceedings of the IEEE*, Vol.87, No.7, July 1999, pp.1108-1126.

[53] G.Voyatzis and I.Pitas, "The Use of Watermarks in the Protection of Digital Multimedia Products", *Proceedings of the IEEE*, Vol.87, No.7, July 1999, pp.1197-1207.

[54] J.Lacy, et al., "Intellectual Property Systems & Digital Watermarking", *Proc. of the 2nd International Workshop on Information Hiding*, Portland, Oregon, USA, 15-17 Apr 1998, Lecture Notes in Computer Science, Vol.1525, Springer-Verlag, David Aucksmith (Ed.).

[55] F. J. MacWilliam and N. J. A. Sloane, "Pseudorandom Sequences and Arrays", *Proc. of the IEEE*, Vol. 64, No. 12, Dec 1976, pp 1715-1729.

[56] D.V. Sarwate and M. B. Pursley, "Cross-correlation of Pseudorandom and Related Sequences", *Proc. of the IEEE*, Vol.68, No.5, May 1980, pp 593-619.

[57] K. N. Ngan, et. al., "Adaptive Cosine Transform Coding of Images in Perceptual Domain", *IEEE Trans. Acoustics, Speech and Signal Processing*, Vol.37, No.11, Nov. 1989, pp.1743-1750.

[58] D. J. Granrath, "The Role of Human Visual Models in Image Processing", *Proc. of the IEEE*, Vol.69, No.5, May 1981, pp.552-561.

[59] C. E. Shannon, ”A Mathematical Theory of Communication”, *Bell Systems Technical Journal*, 1948, 27, pp.379-423, 623-656.

[60] J. L. Mannas and D. J. Sakrison, ”The Effects of a Visual Fidelity Criterion on the Encoding of Images”, *IEEE Trans. Information Theory*, Vol.IT-20, No.4, July 1974.

[61] R. C. Reminger and J. D. Gibson, ”Distribution of the 2D DCT Coefficients for Images”, *IEEE Trans. Communication*, Vol.COM-31, No.6, June 1983.

[62] A.D.Wyner, ”Fundamental Limits in Information Theory”, Proc. of IEEE, Vol.69, No.2, Feb 1981.

[63] J.R.Smith and B.O.Comiskey, ”Modulation and Information Hiding in Images”, *Proc. of First International Workshop on Information Hiding*, University of Canbridge, UK, May 30-June 1 1996, Lecture Notes in Comp. Sc., Vol.1174, Ross Anderson (Ed.).

[64] S.D.Servette, et.al., ”Capacity Issues in Digital Watermarking”, *IEEE Intl. Conference on Image Processing, ICIP-98*, Vol.1, pp.445-449.

[65] G.Depovre, et al., ”Improved Watermark Detection Reliability Using Filtering Before Correlation”,*IEEE International Conference on Image Processing, ICIP-98*, Vol.1, pp.430-434.

[66] J.R.Hernandez, et. al., ”Performance Analysis of a 2-D Multipulse Amplitude Modulation Scheme for Data Hiding and Watermarking of Still Images”, *IEEE Journal on Selected areas in Communications*, Vol.16, No.4, May 1998, pp.510-524.

[67] M.Ramkumar and A.N.Akansu, ”Information Theoritic Bounds for Data Hiding in Compressed Images”, *Electronic Proceedings of IEEE Signal Processing Society 1998 Workshop on Multimedia Signal Processing*, 7-9 Dec 1998, Los Angeles, California, USA.

[68] R. van Schyndel, et al., ”Algebraic Construction of a New Class of Quasi-Orthogonal Arrays in Steganography”, SPIE Electronic Imaging 1999, Vol 3657, pp. 354-364, San Jose, USA, January, 1999

[69] A.Z.Tirkel, et al., ”Secure Arrays for Digital Watermarking”, *Proc. of International Conference on Pattern Recognition*, Brisbane, Australia, August 1998, pp.1643-1645.

[70] I.J.Cox, et al., ”Watermarking as Communications with Side Information”, *Proceedings of the IEEE*, Vol.87, No.7, July 1999, pp.1127-1141.

[71] J.R.Hernandez, et al., ”Statistical Analysis of Watermarking Schemes for Copyright Protection of Images”, *Proceedings of the IEEE*, Vol.87, No.7, July 1999, pp.1142-1166.

[72] J.R.Hernandez, et al., ”Throwing More Lights on Image Watermarks”, *Proc. of the 2nd International Workshop on Information Hiding*, Portland, Oregon, USA, 15-17 Apr 1998, Lecture Notes in Computer Science, Vol.1525, Springer-Verlag, David Aucksmith (Ed.).

[73] J.M.G.Linnartz and M.van Dijk, ”Analysis of Sensitivity Attack Against Electronic Watermarks in Images”, *Proc. of the 2nd International Workshop on Information Hiding*, Portland, Oregon, USA, 15-17 Apr 1998, Lecture Notes in Computer Science, Vol.1525, Springer-Verlag, David Aucksmith (Ed.).

[74] J.M.G.Linnartz, et al., ”Modelling the False Alarm and Missed Detection Rate for Electronic Watermarks”, *Proc. of the 2nd International Workshop on Information Hiding*, Portland, Oregon, USA, 15-17 Apr 1998, Lecture Notes in Computer Science, Vol.1525, Springer-Verlag, David Aucksmith (Ed.).

[75] F. C. Mintzer, et al., ”Towards online Worldwide Access to Vatican Library Materials”, *IBM Jou. of Research and Development*, Vol.40, No.2, Mar. 1996, pp.139-162,
http://www.software.ibm.com/is/diglib/vatican.html,
http://www.ibm.com/IBM/ibmgives/diglib.html,
http://www.research.ibm.com/image_apps.

[76] G. W. Braudaway, et. al., ”Protecting Publicly Available Images with a Visible Image Watermark”, *Proc. SPIE Conf. Optical Security and Counterfiet Deterrence Technique*, Vol. SPIE- 2659, pp.126-132,

[77] M. Kankanahalli, et. al., ”Adaptive Visible Watermarking of Images”, *Proc. of IEEE Int. Conf. on Multimedia Computing Systems, ICMCS-99*, Cento Affari, Florence, Italy, June 1999.

[78] S.P.Mohanty, et al., ”A Dual Watermarking Technique for Images”, *Proc. 7th ACM International Multimedia Conference, ACM-MM'99*, Part 2, pp. 49-51, Orlando, USA, Oct. 1999.

[79] J.J.K O'Ruanaidh, et al., ”Watermarking Digital Images for Copyright Protection”, *IEE Proc. Vision Image and Signal Processing*, Vol.143, No.4, Aug. 1996.

[80] J.J.K. O'Ruanaidh, et al., ”Phase Watermarking on Digital Images”, *Proc. IEEE International Conf. on Image Processing, ICIP-96*, Vol.3, pp 239-242.

[81] J.J.K O'Ruanaidh and T. Pun , "Rotation, Scale and Translation Invariant Digital Image Watermarking", *Proc. IEEE International Conf. on Image Processing, ICIP-97*, Vol.1, pp.536-539.

[82] J.J.K. O'Ruanaidh and T.Pun, "Rotation, Scale and Translation Invariant Spread Spectrum Digital Image Watermarking", *Signal Processing*, Vol.66, No.3, May 1998, pp.303-317.

[83] M.D.Swanson, et al., "Transparent Robust Image Watermarking", *Proc IEEE International Conf. on Image Procesing, ICIP-96*, Vol.3, pp 211-214.

[84] I.J.Cox et. al., "Secure Spread Spectrum Watermarking of Images, Audio and Video", *Proc IEEE International Conf on Image Processing, ICIP-96*, Vol.3, pp 243-246,
http://www.neci.nj.nec.com/tr/neci_tr_95_10.ps

[85] I.J.Cox, et. al., "A Secure Robust Watermarking for Multimedia", *Proc. of First International Workshop on Information Hiding*, Lecture Notes in Comp. Sc., Vol.1174, pp.185-206, Speinger-Verlag, 1996.

[86] C.T.Hsu and J.L.Wu., "Hidden Singatures in Images", *Proc. IEEE International Conf. on Image Processing, ICIP-96*, Vol.3, pp.223-226.

[87] C.T.Hsu and J.L.Wu, "Hidden Digital Watermarks in Images", *IEEE Trans. on Image Processing*, Vol.8, No.1, Jan.1999, pp.58-68.

[88] A.G.Bors and I. Pitas, "Image Watermarking using DCT Domain Constraints", *Proc. IEEE International Conf. on Image Processing, ICIP-96*, Vol.3, pp.231-234.

[89] C.Podilchuk and W.Zeng, "Perceptual Watermarking of Still Images", *IEEE First Workshop on Multimedia signal Processing*, June 23-25 1997, Priceton, New Jersy, USA, pp.363-368.

[90] C.I.PodilChuk and W.Zeng, "Image Adaptive Watermarking using Visual Models", *IEEE Journal on Selected Areas in Communications*, Vol.16, No.4, May 1998, pp.525-539.

[91] A.Piva et. al., "DCT Based Watermark Recovery Without Resorting to the Uncorrupted Original Signal", *Proc. IEEE International Conf. on Image Processing, ICIP-97*, Vol.1, pp.520-523.

[92] D.J.Fleet and D.J.Heeger, "Embedding Invisible Information in color Images", *Proc. IEEE International Conf. on Image Processing, ICIP-97*, Vol.1, pp.532-535.

[93] G.W.Barudaway, "Protecting Publicly available Images with Invisible Watermark", *Proc. IEEE International Conf on Image Processing, ICIP-97*, Vol.1, pp.524-527.

[94] M.Barni, et al., "A DCT-Domain System for Robust Image Watermarking", *Signal Processing*, Vol.66, No.3, May 1998, pp.357-372.

[95] B.Tao and B.Dickinson, "Adaptive Watermarking in DCT Domain", *Proc. IEEE International Conf on Accoustics, Speech and Signal Processing, ICASSP-97*, Vol.4, pp.2985-2988.

[96] M. Kankanahalli, et al., "Content Based Watermarking for Images", *Proc. 6th ACM International Multimedia Conference, ACM-MM 98*, Bristol, UK, pp.61-70, Sep. 1998.

[97] M. Kankanahalli, et al., "Perceptual Content Analysis Based Digital Image Watermarking", *Proc. National Seminar on Cryptography*, July 9-10 1998, Delhi, India.

[98] I.J.Cox, et al., "Secure Spread Spectrum Watermarking for Multimedia", *IEEE Trans. on Image Processing*, Vol.6, No.12, Dec 1997, pp.1673-1687.

[99] A.Herrigel, et al., "Secure Copyright Protection Techniques for Digital Images", *Proc. of the 2nd International Workshop on Information Hiding*, Portland, Oregon, USA, 15-17 Apr 1998, Lecture Notes in Computer Science, Vol.1525, Springer-Verlag, David Aucksmith (Ed.).

[100] R. G. Van Schyndel, et.al., "A Digital Watermark", *Proc. IEEE Intl. Conf. on Image Processing, ICIP-94*, Vol.2, pp.86-90.

[101] R. G. Wolfgang and E. J. Delp, "A Watermark for Digital Images", *Proc. IEEE Intl. Conf. on Image Processing, ICIP-96*, Vol.3, pp.219-222.

[102] R. B. Wolfgang and E. J. Delp, "A Watermarking Technique for Digital Imagery: Further Studies", *Proc. Intl. Conf. on Imaging Sciences, Systems and Tech.*, Los Vegas, June 30-Jul 3, 1997, http://dynamo.ecn.purdue.edy/ac/delp-pub.html

[103] N. Nikolaids and I. Pitas, "Copyright Protection of Images Using Robust Digital Signatures", *Proc. IEEE International Conf. on Accoustics, Speech and Signal Processing, ICASSP-96*, Vol. 4, pp.2168-2171.

[104] N. Nikolaidis and I. Pitas, "Robust Image Watermarking in Spatial Domain", *Signal Procesing*, Vol.66, No.3, pp 385-403.

[105] I.Pitas, ”A Method for Signature Casting on Digital Images”, *Proc. IEEE International Conf. on Image Processing, ICIP-96*, Vol.3, pp 215-218.

[106] I.Pitas and T. Kaskalis, ”Applying Signature on Digital Images”, *Proc. of IEEE Workshop on Non-linear Signal and Image Processing*, I. Pitas(Ed.), pp. 460-463

[107] G. Voyatzis and I. Pitas, ”Application of Toral Automorphism in Image Watermarking”, *Proc. IEEE International Conf. on Image Processing, ICIP-96*, Vol.2, pp.237-240.

[108] M.Kutter, et. al., ”Digital Signature of color Images using Adaptive Modulation”, *Proc.SPIE-EI97*, 1997, pp 518-526

[109] G. Voyatzis and I. Pitas, ”Chaotic Watermarks for Embedding in the Spatial Digital Image Domain”, *Proc. IEEE International Conf. on Image Processing, ICIP-98*, Vol.2, pp.432-436.

[110] M.J.J.J.B. Maes and C.W.A.M. van Overveld, ”Digital Watermarking by Geometric Warping”, *Proc. IEEE International Conf. on Image Processing, ICIP-98*, Vol.2, pp.424-426.

[111] M.S. Hwang, et al., ”A Watermarking Technique Based on One-way Hash Functions”, *IEEE Trans. on Consumer Electronics*, Vol.45, No.2, May 1999, pp.286-294.

[112] J.F.Delaiglee, et al., ”Watermarking Algorithm based on Human Visual Model”, *Signal Processing*, Vol.66, No.3, May 1998, pp.319-335.

[113] A.Z.Tirkel, et al., ”Electronic Watermarking”, *Proc. of Digital Image Computing, Technology and Applications*, Sydney, Australia, 1993, pp.666-672.

[114] R.G. van Schyndel, et. al., ”Key Independent Watermarking Detection”, *Proc. of IEEE Int. Conf. on Multimedia Computing Systems, ICMCS-99*, Cento Affari, Florence, Italy, June 1999, pp.580-585.

[115] I.Pitas, ”A Method for Watermark Casting on Digital Images”, *IEEE Trans. on Circuits and Systems for Video Technology*, Vol.8, No.6, Oct 1998.

[116] A.Z.Tirkel, et al., ”A Two-Dimensional Digital Watermark”, *Proc. of Digital Image Computing, Technology and Applications*, Brisbane, Australia, 1995, pp.378-383.

[117] R.G.van Schyndel, et al., ”Towards a Robust Digital Watermark”, *Proc. of 2nd Asian Conference on Computer Vision*, Singapore, 1995, Vol.2, pp.504-508.

[118] W. Zhu, et al., ”Multiresolution Watermarking for Images and Video”, *IEEE Tran. on Circuits & Systems for Video Technology*, Vol.9, No.4, June 1999, pp.545-550.

[119] W. Zhu, et al., ”Multiresolution Watermarking for Images and Video : A Unified Approach”, *Proc. IEEE International Conf. on Image Processing, ICIP-98*, Vol.1, pp.465-468.

[120] I.J.Chae, et al., ”Color Image Embedding Using Multidimensional Lattice Structure”,*Proc. IEEE International Conf. on Image Processing, ICIP-98*, Vol.1, pp.460-464.

[121] R.Dugad, et al., ”A New Wavelet-Based Scheme for Watermarking Images *Proc. IEEE International Conf. on Image Processing, ICIP-98*, Vol.2, pp.419-423.

[122] H.Inoue, et al., ”A Digital Watermark Based on the Wavelet Transform and its Robustness on Image Compression”, *Proc. IEEE International Conf. on Image Processing, ICIP-98*, Vol.2, pp.391-395.

[123] P.Bas, et al., ”Using the Fractal Code to Watermark Images”, *Proc. IEEE International Conf. on Image Processing, ICIP-98*, Vol.1, pp.469-473.

[124] J.Puate and F.Jordan, ”Using Fractal Compression Scheme to Embed a Digital Signature into an Image”, *Proc. of SPIE Photonics East Symposuim*, Boston, USA, Nov. 18-22 1996.

[125] H.Choi, et al., ”Robust Watermarks for Images in Subband Domain”, *Proc. of the 6th IEEE International Workshop on Intelligent Signal Processing and Communication Systems*, 5-6 Nov. 1998, Melbourne, Australia, pp.168-172.

[126] X.G.Xia, et al., ”A Multiresolution Watermarking for Digital Images”, *Proc. of IEEE International Conference on Image Processing, ICIP-97*, Vol.1, pp.548-551.

[127] D.Kundur and D.Hatzinakos, ”A Robust Digital Image Watermarking Method using Wavelet-Based Fusion”, *Proc. of IEEE International Conference on Image Processing, ICIP-97*, Vol.1, pp.544-547.

[128] G. L. Friedman, ”The Trustworthy Digital Camera: Restoring Credibility to the Photographic Image”, *IEEE Trans. Consumer Electronics*, Vol.39, No.4, Nov. 1993.

[129] M.M.Yeung and F. Mintzer, ”An Invisible Watermarking technique for Image Verification”, *Proc. IEEE International Conf. on Image Processing, ICIP-96*, Vol. 2, pp 680-683.

[130] Min Wu and Bede Liu, "Watermarking for Image Authentication" *Proc. IEEE International Conf. on Image Processing, ICIP-98*, Vol.2, pp.437-441.

[131] P.W.Wong, "A Public Key Watermark for Image Verification and Authentication", *Proc. IEEE International Conf. on Image Processing, ICIP-98*, Vol.1, pp.455-459.

[132] L.Xie and G.R.Arce, "Joint Wavelet Compression and Authentication Watermarking", *Proc. IEEE International Conf. on Image Processing, ICIP-98*, Vol.2, pp.427-431.

[133] Jiri Fridrich, "Image Watermarking for Tamper Detection", *Proc. IEEE International Conf. on Image Processing, ICIP-98*, Vol.2, pp.404-408.

[134] Jiri Fridrich, "Methods for Detecting Changes in Digital Images", Proc. of the 6th IEEE International Workshop on Intelligent Signal Processing and Communication Systems, 5-6 Nov. 1998, Melbourne, Australia, pp.173-177.

[135] D.Kundur and D.Hatzinakos, "Digital Watermarking for Telltale Tamper Proofing and Authentication", *Proceedings of the IEEE*, Vol.87, No.7, July 1999, pp.1167-1180.

[136] F.Hartung and B.Girod , "Digital Watermarking of Raw and Compressed Video", *Digital Compression Technologies and Systems for Video Communications, Vol.2952 of SPIE Proc. Series*, Oct 1996, pp.205-213.

[137] F.Hartung and B. Girod, "Copyright Protection in Video Delivery Networks by Watermarking of precompressed Video", in *Multimedia applications, Services and Technologies-ECMAST-97*, Lecture Notes in Comp Sc., S.Fadida and M.Morganti(Ed.), Tokyo, Japan, Springer 1997, Vol.1242, pp.423-436.

[138] F.Hartung and B.Girod, "Fast Public-Key Watermarking of compressed Video", *Proc. IEEE International Conf. on Image Processing, ICIP-97*, Vol.1, pp.528-531.

[139] F.Hartung and B.Girod, "Digital Watermarking of MPEG-2 coded Video in Bitstream Domain", *Proc. IEEE International Conf. on Accoustics, Speech and Signal Processing, ICASSP-97*, Vol.4, pp.2621-2624.

[140] F.Hartung and B.Girod , "Watermarking of uncompressed and compressed Video", *Signal Processing*, Vol.66, No.3, May 1998, pp.283-301.

[141] M.D.Swanson, et al., "Data Hiding for Video-in-Video", *Proc. IEEE International Conf. on Image Processing, ICIP-97*, Vol.2, pp.676-679.

[142] M.D.Swanson, et al., "Object Based Transparent Video Watermarking", *IEEE First Workshop on Multimedia Signal Processing*, June 23-25, 1997, Princeton, New Jersey, USA, pp.369-374.

[143] M. D. Swanson, et al., "Multiresolution Scene-Based Video Watemarking using Perceptual Models", *IEEE Jrnl. Selected Areas in Communications*, Vol.16, No.4, May 1998, pp.540-550.

[144] C.T.Hsu and J. L. Wu, "DCT-Based Watermarking for Video", *IEEE Trans. on Consumer Electronics*, Vol.44, No.1, Feb 1998, pp. 206-216.

[145] T. Y. Chung, et. al., "Digital Watermarking for Copyright Protections of MPEG-2 Compressed Video", *IEEE Trans. on Consumer Electronics*, Vol.44, No.3, Aug 1998, pp.895-901.

[146] J.Meng and S.F.Chang, "Embedding Visible Video Watermarking in the Compressed Domain", *Proc. IEEE International Conf. on Image Processing, ICIP-98*, Vol.1, pp.474-477.

[147] M.S.Swanson, et al., "Robust Audio Watermarking Using Perceptual Masking", *Signal Processing*, Vol.66, No.3, May 1998, pp.337-355.

[148] P.Bassia and I.Pitas, "Robust Audio Watermarking in Time Domain", *Proc. of the 9th European Signal Processing Conference, EUSIPCO-98*, 8-11 Sep 1998.

[149] D.Gruhl, "Echo Hiding", *Proc. of First Int. Workshop on Information Hiding*, Cambridge, UK, May30-June1, 1996, Lecture notes in Computer Science, Vol.1174, Ross Anderson(Ed.), pp.295-316.

[150] J.T.Brassil, et al., "Electronic Marking and Identification Techniques to Discourage Document Copying", *IEEE Journal on on Selected Areas in Communications*, Vol.13, No.8, Oct 1995, pp.1495-1504.

[151] S.H.Low and N.F.Maxemchuk, "Performance Comparision of Two Text Marking Methods", *IEEE Journal on Selected Areas in Communications*, Vol.16, No.4, May 1998, pp.561-572.

[152] J.T.Brassil, et al., "Copyright Protection for the Electronic Distribution of Text Documents", *Proc. of the IEEE*, Vol.87, No.7, July 1999, pp.1181-1196.

[153] J.Brassil and L.O'Gorman, "Watermarking Document Images with Bounding Box Expansion", *Proc. of First Int. Workshop on Information Hiding*, Cambridge, UK, May30-Jun1, 1996, Lecture Notes in Computer Science, Vol.1174, Ross Anderson(Ed.), pp.227-236.

[154] J.A.Bloom, et al., ”Copy Protection for DVD Video”, *Proceedings of the IEEE*, Vol.87, No.7, July 1999,pp.1267-1276.

[155] S.Craver, et al., ”Can Invisible Watermarks Resolve Rightful Ownership?”, IBM Research Report, RC205209, July25 1996.

[156] S. Craver, et. al., ”On the Invertibility of Invisible Watermarking Techniques”, *Proc. IEEE Intl. Conf. on Image Processing, ICIP-97*, Vol.1, pp.540-543.

[157] S. Craver, et. al., ”Resolving Rightful Ownerships with Invisible Watermarking Techniques: Limitations, Attacks and Implications”, *IEEE Jou. on Selected Areas in Communications*, Vol.16, No.4, May 1998, pp.573-586.

[158] W. Zeng and B Liu, ”On Resolving Rightful Ownership of Digital Images by Invisible Watermarks”, *Proc. IEEE Intl. Conference on Image Processing, ICIP-97*, Vol.1, pp.552-555.

[159] I. J. Cox and J. P. M. G. Linnartz, ”Some General Methods for Tampering with Watermarks”, *IEEE Jou. on Selected Areas in Communications*, Vol.16, No.4, May 1998, pp.587-593.

[160] F.Bao, et al., ”Copyright Protection Through Watermarking: Towards Tracing Illegal Users”, Proc. of the 6th IEEE International Workshop on Intelligent Signal Processing and Communication Systems, 5-6 Nov. 1998, Melbourne, Australia, pp.163-167.

[161] M.Ramkumar and A.N.Akansu, ”Image Watermarks and Counterfeit Attacks : Some Problems and Solutions”, Proc. of Content Security and Data Hiding in Digital Media, Newark, NJ, USA, May 14 1999.

[162] F.A.P.Petitcolas, et al., ”Attacks on Copyright Marking Systems”, *Proc. of the 2nd International Workshop on Information Hiding*, Portland, Oregon, USA, 15-17 Apr 1998, Lecture Notes in Computer Science, Vol.1525, Springer-Verlag, David Aucksmith (Ed.).

[163] M.Maes, ”Twin Peaks : The Histogram Attacks to Fixed Depth Images Watermarks”, *Proc. of the 2nd International Workshop on Information Hiding*, Portland, Oregon, USA, 15-17 Apr 1998, Lecture Notes in Computer Science, Vol.1525, Springer-Verlag, David Aucksmith (Ed.).

[164] L.M.Marvel, et al., ”Hiding Information in Images”, *Proc. IEEE Intl. Conference on Image Processing, ICIP-98*, Vol.2, pp.396-398.

[165] J.Zhao and E. Koch, ”Embedding Robust Labels into Images for Copyright Protection”, *Proc. of International Congress on Intellectual Property Rights for Specialized Information Knowledge and New Technologies*, Vienna, Austria, Aug.21-25 1995, pp.242-251.

[166] M. Schneider and S. F. Chang, ”A Content Based Digital Signature for Image Authentication”, *Proc. IEEE Intl. Conf. on Image Processing, ICIP-96*, Vol.3, pp.227-230.

[167] S.Bhattacharjee and M.Kutter, ”Compression Tolerant Image Authentication”, *Proc. IEEE Intl. Conf. on Image Processing, ICIP-98*, Vol.1, pp.435-439.

[168] K. Hirotsugu, ”An Image Digital Signature System with ZKIP for the Graph Isomorphism”, *Proc. IEEE International Conf. on Image Processing, ICIP-96*, Vol 3, pp 247-250.

[169] P.Davern and M.Scott, ” Fractal Based Image Steganography”, *Proc. of First Int. Workshop on Information Hiding*, Cambridge, UK, May30-Jun1, 1996, Lecture Notes in Computer Science, Vol.1174, Ross Anderson(Ed.), pp.279-294.

[170] A.Westfeld and G.Wolf, ”Steganography in a Video Conferencing System”, *Proc. of the 2nd International Workshop on Information Hiding*, Portland, Oregon, USA, 15-17 Apr 1998, Lecture notes in Computer Science, Vol.1525, Springer-Verlag, David Aucksmith (Ed.).

[171] L.M.Marvel, et al., ”Reliable Blind Information Hiding for Images”, *Proc. of the 2nd International Workshop on Information Hiding*, Portland, Oregon, USA, 15-17 Apr 1998, Lecture notes in Computer Science, Vol.1525, Springer-Verlag, David Aucksmith (Ed.).

[172] R.Anderson, et al., ”The Steganographic File System”, *Proc. of the 2nd International Workshop on Information Hiding*, Portland, Oregon, USA, 15-17 Apr 1998, Lecture notes in Computer Science, Vol.1525, Springer-Verlag, David Aucksmith (Ed.).

[173] N.F.Johnson and Sushil Jajodia, ”Steganalysis : The Investigation of Hidden Information”, *Proc. of 1998 IEEE Information Technology Conference*, Syracuse, New York, USA, 1-3 Sep 1998, pp.113-116.

[174] N.F.Johnson and Sushil Jajodia, ”Steganalysis of Images created using Current Steganography Software”, *Proc. of the 2nd International Workshop on Information Hiding*, Portland, Oregon, USA, 15-17 Apr 1998, Lecture notes in CS, Vol.1525, Springer-Verlag, David Aucksmith (Ed.).

[175] J.M.Ettinger, "Steganalysis and Games Equilibria", *Proc. of the 2nd International Workshop on Information Hiding*, Portland, Oregon, USA, 15-17 Apr 1998, Lecture notes in CS, Vol.1525, Springer-Verlag, David Aucksmith (Ed.).

[176] N.R.Wagner, "Finger Printing", *Proc. of the 1983 Symposium on Security and Privacy*, Apr.25-27 1983, Oakland, California, IEEE Computer Society, pp.18-22.

[177] D.Kesdogan, et al., "Stop-and-Go-MIXes Providing Anonymity in an Open System", *Proc. of the 2nd International Workshop on Information Hiding*, Portland, Oregon, USA, 15-17 Apr 1998, Lecture notes in Computer Science, Vol.1525, Springer-Verlag, David Aucksmith (Ed.).

[178] G.J.Simmons, "The History of Subliminal Channels", *IEEE Journal on Selected Areas in Communications*, Vol.16, No.4, May 1998, pp.452-462.

[179] G.J.Simmons, "The History of Subliminal Channels", *Proc. of First Int. Workshop on Information Hiding*, Cambridge, UK, May30-Jun1, 1996, Lecture Notes in Computer Science, Vol.1174, Ross Anderson(Ed.), pp.237-256.

[180] G.J.Simmons, "Results Concerning the Bandwidth of Subliminal Channels", *IEEE Journal on Selected Areas in Communications*, Vol.16, No.4, May 1998, pp.463-473.

[181] R.Anderson, et.al., "The Newton Channel" *Proc. of First Int. Workshop on Information Hiding*, Cambridge, UK, May30-Jun1, 1996, Lecture Notes in Computer Science, Vol.1174, Ross Anderson(Ed.), pp.151-156.

[182] C. Meadow and I.S.Maskowintz, "Covert Channels : A Content- Based view", *Proc. of First Int. Workshop on Information Hiding*, Cambridge, UK, May30-June1 1996, Lecture Notes in Computer Science, Vol.1174, Ross Anderson(Ed.), pp.73-94.

[183] M.Burmster, et.al., "A Progress Report on Subliminal-free Channels", *Proc. of First Int. Workshop on Information Hiding*, Cambridge, UK, May30-Jun1, 1996, Lecture Notes in Computer Science, Vol.1174, Ross Anderson(Ed.), pp.157-168.

[184] M.Anderson and M.Ozols, "Covert Channel Analysis for Stubs", *Proc. of First Int. Workshop on Information Hiding*, Cambridge, UK, May30-Jun1, 1996, Lecture Notes in Computer Science, Vol.1174, Ross Anderson(Ed.), pp.95-114.

[185] Y.Desmedt, "Establishing Big Brother Using Covert Channels and other Covert Techniques", *Proc. of First Int. Workshop on Information Hiding*, Cambridge, UK, May30-Jun1, 1996, Lecture Notes in Computer Science, Vol.1174, Ross Anderson(Ed.), pp.65-72.

[186] http://www.altern.org/watermark

[187] http://www.cl.cam.ac.uk/∼fapp2/watermarking

[188] http://www.research.ibm.com

[189] http://www.neci.nj.nec.com

[190] http://www.dlib.org

[191] http://www.macrovision.com

[192] http://www.intertrust.com

[193] http://www.musicode.com

[194] http://www.bluespike.com

[195] http://www.digimarc.com

[196] http://www.mediasec.com

[197] http://www.signumtech.com

[198] http://www.signafy.com

[199] http://www.krdl.org.sg

[200] http://www.digital-watermark.com

[201] http://www.jjtc.com/Steganography

[202] http://nif.www.media.mit.edu/DataHiding