3

Robust Multiple Image Watermarking Based on Spread Transform

Jaishree Jain and Vijendra Rai
Mahamaya Technical University
Noida
India

1. Introduction

In this chapter, some multiple watermarking techniques and their limitations are discussed which include both spatial and transform domain methods. Since many algorithms are applied to graphical images, the concept of graphical image perceptibility and measures of PSNR and Bit Error Ratio (BER) are also discussed.

Watermarks are used to keep track of paper provenance and thus format and quality identification in the art of handmade papermaking nearly 700 years ago. In 1993 the term Watermark is used first time. In 1993-1994 the first papers on digital watermarking was published whereas in 1995 the first special session on image watermarking at NSIP95, Neos Marmaras, Greece was held. In 1995 one of the first images watermarking algorithms Patchwork algorithm was proposed. Watermarking has developed basically from two different streams, Cryptography meaning, secret writing and Steganography, which in the Greek language means, cover writing.

This is the digital information revolution era. It has connectivity over the Internet and connectivity through the wireless network. Innovative devices such as digital camera and camcorder, high quality scanners and printers have reached consumers worldwide to create, manipulate and enjoy the multimedia data. The development of high speed computer networks and that of internet, in particular, has explored means of new business, scientific, entertainment and social opportunities in the form of electronic publishing and advertising, real-time information delivery, product ordering, transaction processing, digital repositories and libraries, personal communication etc.

Digital content are spreading rapidly in the world via the internet. It is possible to produce a number of the same one with the original data without any limitation. Copying is simple with no loss of fidelity. A copy of a digital media is identical to the original. This has many instances, led to the use of digital content with malicious intent. The current rapid development of new IT technologies for multimedia services has resulted in a strong demand for reliable and secure copyright protection techniques for multimedia data. One way to protect multimedia data against illegal recording and retransmission is to embed a signal, called digital signature or copyright label or watermark that authenticates the owner of the data. With the ease of editing and perfect reproduction in digital domain, the

protection of ownership and the prevention of unauthorized tampering of multimedia data (audio, image, video, and document) have become important concerns. Digital watermarking schemes to embed secondary data in digital media, have made considerable progress in recent years and attracted attention from both academia and industry. Techniques have been proposed for a variety of applications, including ownership protection, authentication and access control. Imperceptibility, robustness against moderate processing such as compression, and the ability to hide many bits are the basic but rather conflicting requirements for many data hiding applications.

Digital watermarking is a technique to embed invisible or inaudible data within multimedia contents. Watermarked contents contain a particular data for copyrights. A hidden data is called a watermark, and the format can be an image or any type media. In case of ownership confliction in the process of distribution, digital watermark technique makes it possible to search and extract the ground for ownership. Many researches on watermarking have been come out in the advanced countries including USA and EU so far, because of its importance of this area in the future.

To avoid the unauthorized distribution of images or other multimedia property, various solutions have been proposed. Most of them make unobservable modifications to images that can be detected afterwards. Such image changes are called watermarks. Watermarking is defined as adding (embedding) a payload signal to the host signal. The payload can be detected or extracted later to make an assertion about the object i.e. the original data that may be an image or audio or video.

Multiple watermarking is an embranchment of digital watermarking which has many desirable characteristics that common singular watermarking does not have, such as robustness to union attacks. For example, employ multiple watermarks to convey multiple sets of information, intended to satisfy differing or similar goals, Used to increase robustness with many different methods, the embedded information is not easily lost, it is possible to support different access levels. To accomplish several goals, one might wish to embed several watermarks into the same image. For example, the owner might desire to use one watermark to convey ownership information, a second watermark to verify content integrity, a third watermark to convey a caption.

The aim of watermarking is to include subliminal information (i.e., imperceptible) in a multimedia document to ensure a security service or simply a labeling application. But existing multiple watermarking has inherent problem such as low validity and high complexity.

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

- The watermark (payload)
- The encoder (marking 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.

1.1 Watermark insertion and extraction

Watermark insertion involves watermark generation and encoding process.

1.1.1 Watermark generation

The watermark can be a logo picture, sometimes a binary picture, sometimes a ternary picture; it can be a bit stream or also an encrypted bit stream etc. The encryption may be in the form of a hash function or encryption using a secret key. The watermark generation process varies with the owner.

1.1.2 Encoding process

Inputs to the embedding scheme are the watermark, the cover data and an optional public or secret key. The output is watermarked data. The key is used to enforce security.

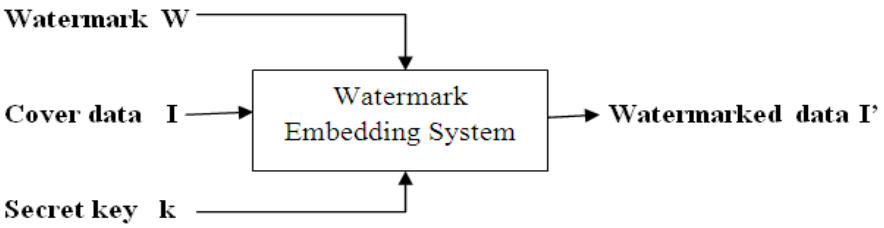


Fig. 1. Embedding Process

1.1.3 Watermark extraction

Extraction is achieved in two steps. First the watermark or payload is extracted in the decoding process and then the authenticity is established in the comparing process.

1. **Decoding process**: Inputs to the decoding scheme are the watermarked data, the secret or public key and depending on the method, the original data and/or the original watermark. The output is the recovered watermarked W.

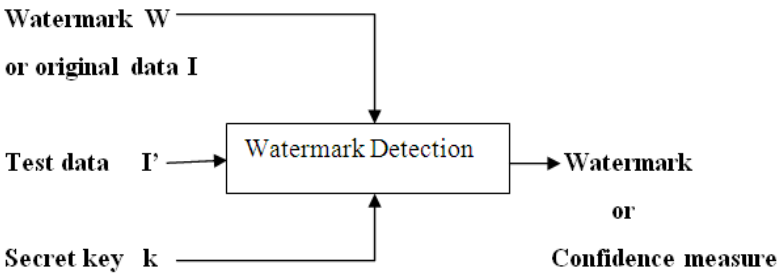


Fig. 2. Extraction Process

2. **Comparison Process:** The extracted watermark is compared with the original watermark by a comparator function and a binary output decision is generated. The comparator is basically a correlated. Depending on the comparator output it can be determined if the data is authentic or not. If the comparator output is greater than equal to a threshold then the data is authentic else it is not authentic. Figure illustrates the comparing function. In this process the extracted watermark and the original watermark are passed through a comparator. The comparator output C is the compared with a threshold and a binary output decision generated. It is 1 if there is a match i.e. C ≥ δ and 0 otherwise. A watermark is 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 [5].

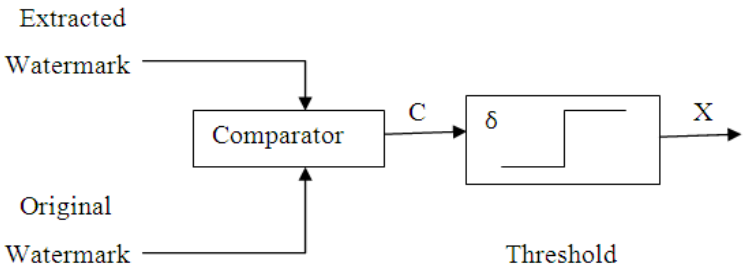


Fig. 3. Comparison Process

1.2 Practical challenges of watermarking

Watermark by itself is not sufficient to prevent abuses unless a proper protection protocol is established. The exact properties that a watermarking algorithm must satisfy cannot be defined exactly without considering the particular application scenario; the algorithm has to be used in. A brief analysis of requirements of data hiding algorithms from a protocol perspective permits to decide whether a given algorithm is suitable for a certain application or not. Each watermarking application has its own specific requirements. Most often than not these requirements have conflicting effects on each other. A good watermarking algorithm obtains optimal tradeoff between these requirements; is not weakened/ destroyed by attacks, both malicious and non-malicious; at the same time unambiguously identifies the owner. These properties can be broadly classified as primary and secondary requirements. The primary requirements include data hiding capacity, imperceptibility and robustness as shown in figure4. However these three characteristics conflict with each other. Increasing fidelity of the watermarked images (i.e. increasing imperceptibility of the mark) would lower the strength of the watermark. Embedding large amount of information reduces the fidelity of the watermark. The secondary requirements include performance i.e. the speed of embedding and of detection of the watermark. These attributes though less commonly

discussed are very important for many real world applications. Each of the primary attributes has been discussed in detail below.

1.2.1 Capacity of watermarking techniques

Capacity is a fundamental property of any watermarking algorithm, which very often determines whether a technique can be profitably used in a given context or not. However no requirement can be set without considering the application the technique has to serve in. Possible requirements range from some hundreds of bits in security oriented applications, where robustness is a major concern, through several thousands of bits in applications like captioning or labeling, where the possibility of embedding a large number of bits is a primary need. For copy protection purposes, a payload of one bit is usually sufficient. Capacity requirements always struggle against two other important requirements, watermark imperceptibility and watermark robustness. A higher capacity is always obtained at the expense of either robustness or imperceptibility or both. It is therefore mandatory that a good trade-off be found depending on the application at hand.

1.2.2 Imperceptibility

The watermark should be imperceptible so as not to affect the viewing experience of the image or the quality of the image signal. In most applications the watermarking algorithm must embed the watermark such that this does not affect the quality of the underlying host data. A watermark embedding procedure is truly imperceptible if humans cannot distinguish the original data from the data with the inserted watermark. However even the smallest modification in the host data may become apparent when the original data is compared directly with the watermarked data. Since users of watermarked data normally do not have access to the original data, they cannot perform this comparison. Therefore, it may be sufficient that the modifications in the watermarked data go unnoticed as long as the data are not compared with the original data.

1.2.3 Robustness

Watermark robustness accounts for the capability of the hidden data to survive host signal manipulations, including both non-malicious manipulations, which do not explicitly aim at removing the watermark or at making it unreadable, and malicious manipulations, which precisely aim at damaging the hidden information. The exact level of robustness the hidden data must possess cannot be specified without considering a particular application. Robustness against signal distortion is better achieved if the watermark is placed in perceptually significant parts of the signal. This is particularly evident in the case of lossy compression algorithms, which operate by discarding perceptually insignificant data. Watermarks hidden within perceptually insignificant data are likely not to survive compression. Achieving watermark robustness, and, to a major extent, watermark security is one of the main challenges watermarking researches are facing with.

1.3 Watermarking attacks

Any procedure that can decrease the performance of the watermarking scheme may be termed as an attack. Voloshynovskiy et.al [1] categorizes attacks into four classes' viz.

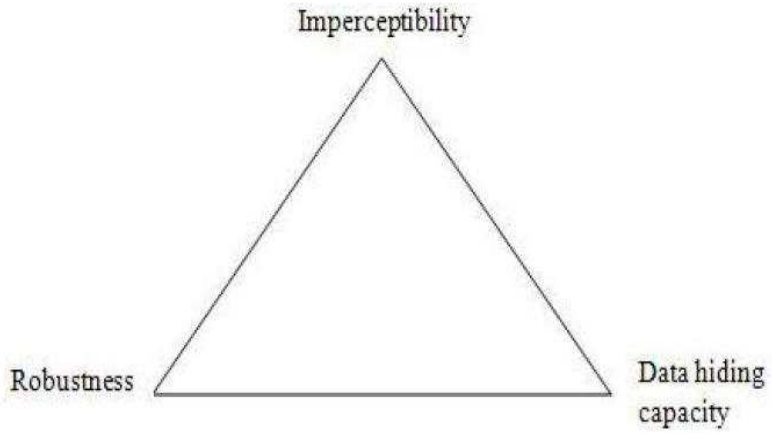


Fig. 4. Primary Requirements of Watermarking Algorithms

removal, geometric, cryptographic and protocol. Removal attack removes the watermark without having any prior knowledge about the watermark, while geometric attacks deal with de-synchronization of the receiver so that watermark detection is distorted. Cryptographic schemes are those that tend to crack the watermarking scheme and protocol attacks exploit invertible watermarks to cause ownership ambiguity. These attacks can be broadly classified as non-malicious (unintentional) such as compression of a legally obtained, watermarked image or video file and malicious (intentional) such as an attempt by a multimedia pirate to destroy the embedded information and prevent tracing of illegal copies of watermarked digital video. Watermarking systems utilized in copy protection or data authentication schemes are especially susceptible to malicious attacks. Non-malicious attacks usually come from common signal processing operations done by legitimate users of the watermarked materials.

1.3.1 Malicious attack

An attack is said to be malicious if its main goal is to remove or make the watermark unrecoverable. Malicious attacks can be further classified into two different classes.

Blind: A malicious attack is said to be blind if it tries to remove or make the watermark unrecoverable without exploiting knowledge of the particular algorithm that was used for watermarking the asset. For example, copy attack that estimates the watermark signal with aim of adding it to another asset.

Informed: A malicious attack is said to be informed if it attempts to remove or make the watermark unrecoverable by exploiting knowledge of the particular algorithm that was used for watermarking the asset. Such an attack first extracts some secret information about the algorithm from publicly available data and then based on this information nullifies the effectiveness of the watermarking system. Examples of malicious attacks: Printing and Rescanning.

1.3.2 Non-malicious attack

An attack is said to be non malicious if it results from the normal operations that watermarked data or any data for that matter has to undergo, like storage, transmission or fruition. The nature and strength of these attacks are strongly dependent on the application for which the watermarking system is devised. For example lossy- compression, geometric and temporal manipulations digital to analogue conversion, extraction of asset fragments (cropping), processing aimed at enhancing asset (e.g. noise reduction), etc. Examples of Non-Malicious Attacks: 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 and videos and include such operations as rotation, translation, scaling and cropping.

2. Different types of watermarks and watermarking techniques

2.1 Visible watermark

Visible watermarks are the watermarks, existence of which is visible to the user. For example, to indicate ownership of originals, the content owner desires a visible mark that makes clear the source of the materials.

i. Spatial domain visible watermarking

Using patch work algorithm was proposed by N. Memon and P. Wong in 1998 [2].The author has selected n number of patches randomly and make certain statistics to make use of these patches as watermark. This method is more resistant to attempts of data removal by a third party but the scheme is extremely sensitive to geometric transformation. If the patch size is very small with sharp edges then it results in removal of watermark in lossy compressions, also optimal choice of patch shape is dependent upon the expected image modification. Due to the limitations of the spatial domain techniques the visible watermarking is also developed in the transform domain.

ii. Transform domain visible watermarking

A DCT domain visible watermarking technique for images [3] was developed by S. P. Mohanty, et al. The technique modifies DCT coefficients of the cover image and exploits the texture sensitivity of the human visual system. The perceptual quality of the image is better preserved in this technique as compared to the previous one but this technique is not robust for images having very few objects and large uniform areas.

2.2 Invisible watermark

The invisible watermark's existence should be determined only through a watermark extraction or detection algorithm. The invisible watermark falls into three categories:

1. Fragile watermarking

Invisible image watermarks that will change, or disappear, if a watermarked image is altered are called as fragile watermarking. These watermarks are called fragile invisible watermarks because it is desired that they be altered or destroyed by most common image processing techniques. For example, invisible watermarking for a trustworthy camera.

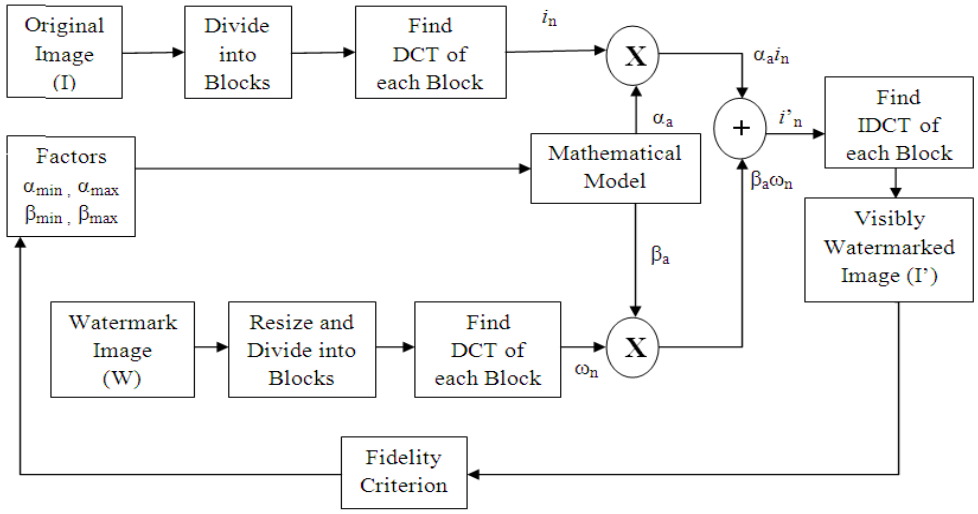


Fig. 5. Watermark Insertion Process [4]

A Fragile Watermarking Scheme for Image Authentication with Tamper Localization Using Integer Wavelet Transform was proposed by M. Venkatesan, et al. in [4] in spatial domain. Watermark is randomly scattered in the LSB of the cover image. The technique is capable of detecting and localizing the malicious changes in the cover image and it has the ability to discriminate watermark and content tampering. The only limitation of the technique is that the relationship between the reliability of tamper detection and the localization accuracy has not investigated.

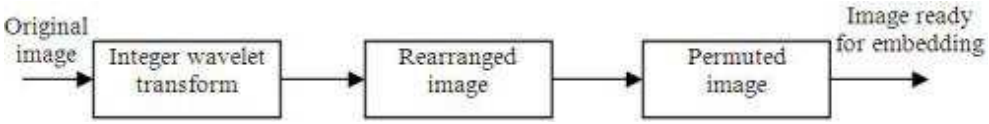


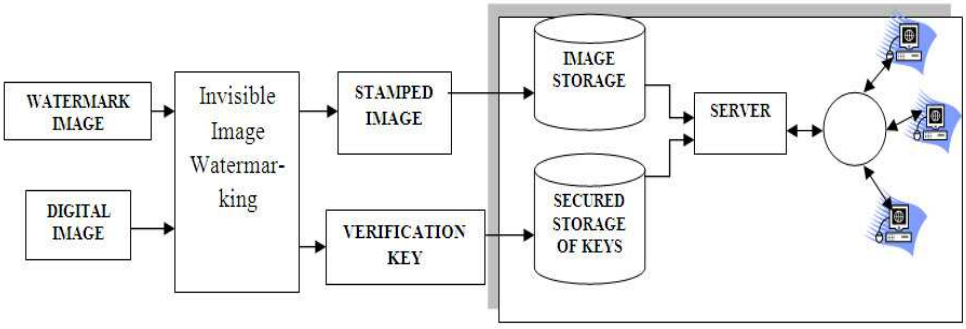
Fig. 6. Preprocessing [4]

2. Semi-fragile watermarking

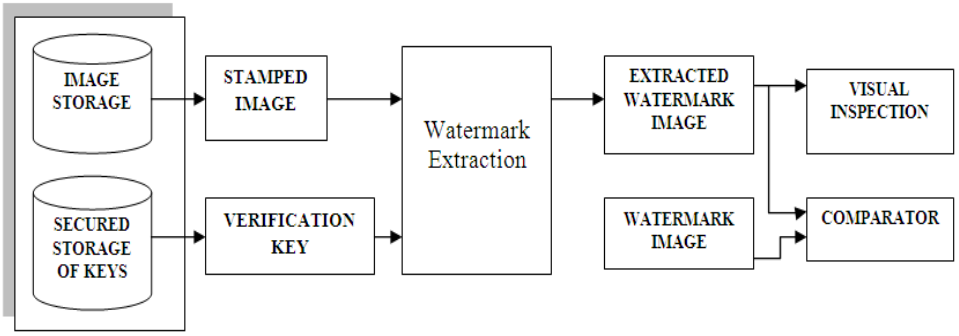
These are the watermarking systems where content needs to be strictly protected, but the exact representation during exchange and storage need not be guaranteed. Semi fragile watermarking methods validate image content, but not its representation, and are thus made robust against allowable alterations, while being sensitive to non permitted modifications. For example, Semi fragile tamper detection methods are designed to monitor changes in the content and tamper detection is based on the visual assessment of perceived differences by an operator.

An invisible watermarking technique for image verification was proposed by Yeung, M.M and Mintzer F. [5] in spatial domain. The technique is developed using least significant Bit method and the verification key is generated using Look up Table (LUT). The method can localize the regions of image alterations and hence effectively use for tamper detection. The

watermarking process does not introduce visual artifacts and retain the quality of the image and provide protection against retention of watermark after unauthorized alterations. As LUT is generated randomly, the pixel values may have to be adjusted by larger amounts to get desired unary value.



(a)



(b)

Fig. 7. The block Diagram of the Image Verification System with Proposed Invisible Watermarking Technique [5]

Semi Fragile Watermarking Based on Wavelet Transform was proposed by Yuichi Nakai [6]. The technique is based on wavelet transform and embeds watermark to wavelet coefficients for evaluating the degree of tampering for each pixel. It embeds MSB of watermarks in low frequency components and LSB in high frequency component. The proposed scheme can evaluate the degree of tampering for each pixel but the number of watermarks that can be embedded without degradation of image quality is less.

3. Robust watermarking

Watermarks that persist even if someone tries to remove them are called as robust watermarking. Since they are desired to survive intentional attacks (e.g. active attack,

passive attack etc.), these are called as robust image watermarks. For example, Evidence of ownership.

Van Schyndel, et al. has developed robust watermarking in his paper ''A Digital Watermark'' [7] in spatial domain. The original 8 bit grey scale image data is compressed to 7 bits by adaptive histogram manipulation. The watermark is generated using an m sequence generator. The watermark was embedded to the LSB of the original image and

Cross-correlation based detection was proposed. The method utilizes linear addition of watermark data and is more difficult to decode, offering inherent security. The technique is compatible with JPEG processing. The watermark is not robust to additive noise.

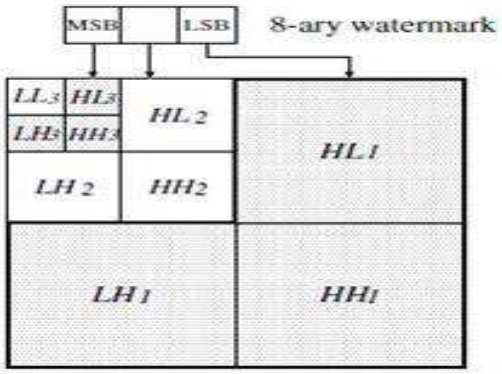


Fig. 8. Embedding 8-ary Watermarks in Several Wavelet Coefficient Level [7]

I.A. Nasir has divided the host image into four different regions each consisting of 128 ×128 blocks in order to hide a watermark [8]. The watermark is a binary image encrypted and embedded into different regions of the blue component of the image by altering intensity values of the selected regions. The watermarks can be extracted by comparing the intensities of the selected region of the original image with the corresponding region of the watermarked image. The proposed watermarking scheme is robust for a wide range of attacks including JPEG compression, rotation, scaling, filtering, etc. The number of watermarks that can be embedded effectively is not statistically proved.

3. Multiple watermarking basics

Multiple watermarking is an embranchment of digital watermarking, which has many desirable characteristics that common singular watermarking does not have. For example, employ multiple watermarks to convey multiple sets of information, intended to satisfy differing or similar goals, used to increase robustness with many different methods, the embedded information is not easily lost, it is possible to support different access levels. To accomplish several goals, one might wish to embed several watermarks into the same image. For example, the owner might desire to use one watermark to convey ownership information, a second watermark to verify content integrity, a third watermark to convey a caption [9].In general, to apply multiple disparate watermarks, ownership watermarks should be very robust, captioning watermarks should be robust, and Verification

watermarks should be quite fragile. In general, to apply multiple disparate watermarks, the most robust (ownership) watermark should be embedded first, the most fragile (verification) watermark should be embedded last, and moderately robust (captioning) watermarks should be inserted in between.

Embedding multiple watermarks will then be successful if the robust watermarks are sufficiently robust to withstand all subsequent watermark insertions. After the insertion of multiple watermarks, the watermarked image will possess texture resulting from each watermark. Embedding multiple watermarks also requires that each watermark add less texture than would be permissible.

3.1 Types of multiple watermark

The multiple watermarking is broadly classified into three categories [10] as follows:

i. Composite watermarking

All watermarks are combined into a single watermark which is subsequently embedded in one single embedding step. The composite watermarks are separable if the watermarking patterns are orthogonal (or uncorrelated) in some sense relevant to the watermark detection. Example: Averaged watermarking

ii. Segmented watermarking

The host data is partitioned into disjoint segments a priory and each watermark is embedded into its specific share. If all keys are present the detector can find a watermark in every segment, otherwise it cannot. Example: Interleaved watermarking.

iii. Successive watermarking

It is the most straightforward method to embed the watermarks one after the other.

This method is useful in the applications where retrieval of one watermark should depend on the retrieval of other watermark. For example, it allows us to determine the order in which the watermarks are embedded. The object becomes more degraded with every new watermark inserted into it, both in terms of PSNR and perceived quality. Example: Re-watermarking.

In general, to apply multiple disparate watermarks, the most robust (ownership) watermark should be embedded first, the most fragile (verification) watermark should be embedded last, and moderately robust (captioning) watermarks should be inserted in between. Embedding multiple watermarks will be successful if the robust watermarks are sufficiently robust to withstand all subsequent watermark insertions. After the insertion of multiple watermarks, the watermarked image will possess texture resulting from each watermark. Embedding multiple watermarks also requires that each watermark add less texture than would be permissible.

3.2 Multiple watermarking techniques

The different watermarking techniques are broadly classified between two domains, namely spatial and transform domain.

3.2.1 Spatial domain

The spatial techniques insert the watermark in the underused least significant bits of the image. This allows a watermark to be inserted in an image without affecting the value of the image. Example: Least Significant Bit, Statistical, block based method. The most common implementation of spatial domain watermarking is Least Significant Bit (LSB) replacement method. It involves replacing the n least significant bits of each pixel of a container image with the data of a hidden image. Since the human visual system is not very attuned to small variations in color, the method adjusts the small differences between adjacent pixels leaving the result virtually unnoticeable.

3.2.2 Transformed domain techniques

In the transform domain approach, some sort of transforms is applied to the original image first. The transform applied may be (DCT), (DFT), (DWT), etc. The watermark is embedded by modifying the transform domain coefficients. Example: DFT, DCT, DWT, Spread Spectrum.

Traditional watermarking schemes consisted of visible watermarking. Applications now demand that the watermark being embedded be highly robust to attacks. Techniques of hiding information in images include the use of discrete cosine transform (DCT), discrete

Fourier transforms (DFT) and wavelet transform.

i. Discrete cosine transform

This is the most commonly used transform for watermarking purpose. The DCT allows an image to be broken up into different frequency bands making it much easier to embed watermarking information into the middle frequency bands of an image. In our technique we use middle-band DCT coefficients to encode the message. It avoids the most visual important parts of the image without over exposing themselves to removal through compression and noise-attacks.

I J. Cox have considered watermarking as communications with side information [11].

The DCT allows an image to be broken up into different frequency bands, making it much easier to embed watermarking information into the middle frequency bands of an image.

Algorithm achieves good robustness against compression and other signal processing attacks due to the selection of perceptually significant transform domain coefficients. Robustness and the quality of the watermark could be improved if the properties of the host image could similarly be exploited.

M. Barni has embedded pseudo-random sequence of real numbers having normal distribution with zero mean and unity variance in selected set of DCT coefficients [12]. The watermark is robust to several signal processing techniques, including JPEG compression, low pass and median filtering, dithering etc. But watermark does not resist geometric translations. Mitchell et al. has computed a frequency mask for each block [13].The resulting perceptual mask is scaled and multiplied by the DCT of a pseudo-noise sequence which is different for each block. This watermark is then added to the corresponding DCT block. The watermark is robust to several distortions including white and colored noise, cropping, etc. For JPEG coding at 10% the quality of original image degrades.

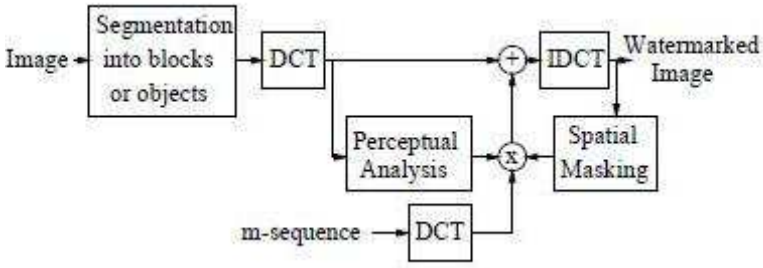


Fig. 9. Diagram of New Watermarking Technique [14]

ii. Discrete wavelet transform

This technique is also called as multiresolution technique. The important aspect of this technique is that watermark is introduced in imperceptibly significant regions of the data in order to remain robust. It decomposes the image into frequency bands using resolution of wavelets. X.Xia in 1997 proposed the concept of Multiresolution Watermark for Digital Images using wavelet transformation [14]. An image can be decomposed into a pyramid structure with various bands information: such as low-low frequency bands, low-high, high-low or high-high frequency bands. Adding watermarks on the large coefficients (HH, LH, HL and LL) is difficult for the human eyes to perceive. If distortion of a watermarked image is not serious, only a few bands worth of information are needed to detect the signature and therefore computational load can be served. This method is robust to all kinds of distortions such as compression, additive noise, etc. If distortion of a watermarked image is more, more bands of DWT are needed to detect watermark and computational load increases.

X. Liang and Wu Huizhong have proposed the multiple perceptual watermarks using multiple-based number conversion in wavelet domain [15]. Multiple watermarks coding and decoding system for image copyright protection is presented. Just Noticeable Difference (JND) threshold in wavelet domain is used to determine the locations for embedding. A multiple-based number system (every digit in number has base bi 0) is proposed to convert the watermark information into values to be embedded in the wavelet coefficient. The method has good robustness to JPEG compression, median filtering, Gaussian noise suppression, cropping and morphing type of distortions. Watermark strength is more as JND is used. The method fails to stir mark attack.

The limitations of wavelet transform have been overcome in dual tree complex wavelet transform. Lan Hong xing et al. in the paper ''A Digital Watermarking Algorithm Based on Dual-tree Complex Wavelet Transform'' [16], has proposed a multipurpose watermarking algorithm based on dual tree complex-wavelet transform. The authors notify the copyright owner with visible watermark and to protect the copyright with an invisible watermark. Dual- tree DWT has relatively high capacity to make the visible watermark hard to remove and invisible watermark robust. The only difficulty is in redesign of watermark with perfect reconstruction properties. It can only bring less visual effects for reconstruction of image in +/-45 sub bands.

iii. Spread spectrum

Spread spectrum watermarking is one of the most popular methods of watermarking. In this technique, the watermark bits are randomly scattered in the cover object. This not only ensures that the watermark is robust to attacks but also simplifies the detection algorithm using correlation analysis. Cryptographers believe that spread spectrum (SS) method of watermarking can incorporate a high degree of robustness because the pseudo-random sequences being used in SS watermarking are very difficult to generate without the prior knowledge of the initial state of the random number generator. This secures decoding or removal of the watermark and also provides resistance to cropping. The major drawback of the SS watermarking scheme is that it requires a high gain value Δ, which sometimes tends to alter the cover data file considerably such that it is noticeable. To overcome this problem, the improved spread spectrum (ISS) technique is used. In this technique a feature vector extraction mechanism has been established which enhances the performance by modulating the energy of the inserted watermark to compensate for the signal interference. The ISS technique using the dither quantization is used to enhance the performance of the embedding procedure and improve the overall performance of the watermarking scheme.

Spread transform dither modulation method is a transform domain method. The transform methods are more complex, but more robust than the spatial methods. The watermark is inserted into the cover image in a spread-spectrum fashion in the spectral domain, thereby making it robust against signal processing operations. In this case, the feature vector extraction process can be seen as an extension of the spread transform technique (a more general method of spreading watermark information over a host signal than spread spectrum) that is frequently employed on multimedia. To this feature vector a quantization based watermarking algorithm is used. Quantization index modulation (QIM) methods are a class of watermarking methods that achieve provably good rate-distortion-robustness performance.

a. Quantization index modulation

The process of mapping a large possible infinite set of values to a much smaller set is called quantization. Since quantization reduces the number of distinct symbols that have to be coded, it is central to many lossy compression schemes. A quantizer consists of two mappings: an encoder mapping and a decoder mapping. The encoder divides the range of source values into a number of intervals. Each interval is represented by a codeword. The encoder represents all the source values that fall into a particular interval by the codeword assigned to that interval. As there could be many possibly infinitely many distinct samples that can fall in any given interval, the encoder mapping is irreversible. For every codeword generated by the encoder, the decoder generates a reconstruction value.

Quantizers, or a sequence of quantizers, can be used to as appropriate-identity functions to embed the watermark information. The number of possible values of m determines the number of required quantizers, m acts as an index that selects the quantizer that is used to represent m. For the case m = 2 we have a binary quantizer. The following figure illustrates the QIM information embedding process. To embed one bit m, m € 0, 1 and image pixel is mapped to the nearest reconstruction point representing the information of m. The minimum distance d min between the sets of reconstruction points of different quantizers in the ensemble determines the robustness of the embedding,

$$d_{\min} = \min_{(i,j):i\neq j} \min_{(x_i,x_j)} \left\| s(x_i;i) - s(x_j;j) \right\|$$

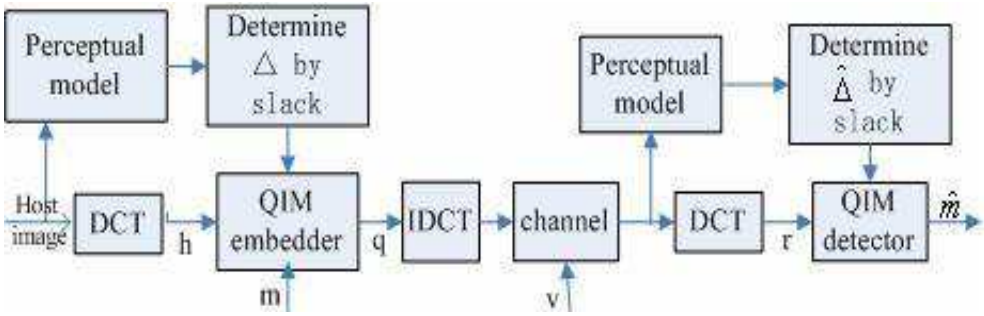


Fig. 10. QIM Scheme

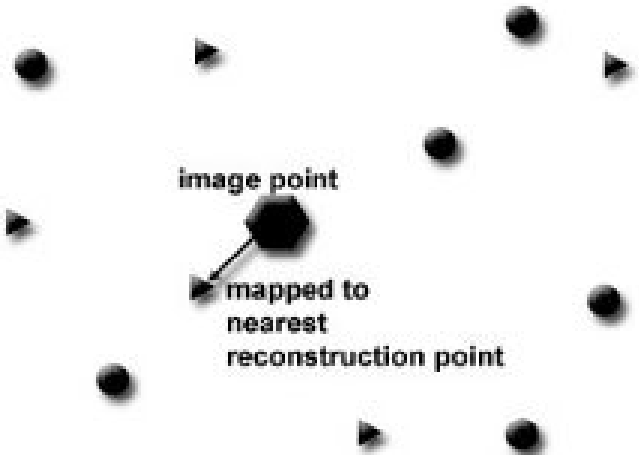


Fig. 11. Quantization Index Modulation

Intuitively, the minimum distance measures the amount of noise that can be tolerated by the system.

b. Dither modulation

A low-complexity realization of QIM called dither modulation which is better than both linear methods of spread spectrum and nonlinear methods of low-bit modulation against square-error distortion constrained intentional attacks. Dither modulation (DM) is the simplest form of quantization index modulation and is the most thoroughly analyzed by its ease of practical implementation. Dither modulation systems embed watermark by modulating the amount of the shift, which is called the dither vector, by the embedded signal. The host signal is quantized with the resulting dithered quantizer to form the composite signal. Dithered quantization (or Dither Modulation) is an operation in which a

dither vector d of length L is added to the input x prior to quantization. The output of the subtractive quantization operation is denoted by

$$s_i = Q(x_i + d_i) - d_i;\ 0 \le i < L$$

Or, using the notation introduced above,

$$s(x; m) = Q(x + d(m)) - d(m)$$

For our discussion, we only consider uniform, scalar quantizer with a step size M. The binary dither ensemble can be generated pseudo-randomly by choosing di with a uniform distribution over [–Δ/2; +Δ/2] and assigning di as follows:

$$d_i(2) = \begin{Bmatrix} d_i(1) + \frac{\Delta}{2},\ if\ d_i(1) < 0 \\ d_i(1) - \frac{\Delta}{2},\ if\ d_i(1) \ge 0 \end{Bmatrix}$$

Where, 0 ≤ i < L. For the single embedding case (Figure12 (a)), let the QIM embed ding logic be converting an element to the nearest even/odd multiple of the quantization interval, Δ, to embed 0/1, respectively.

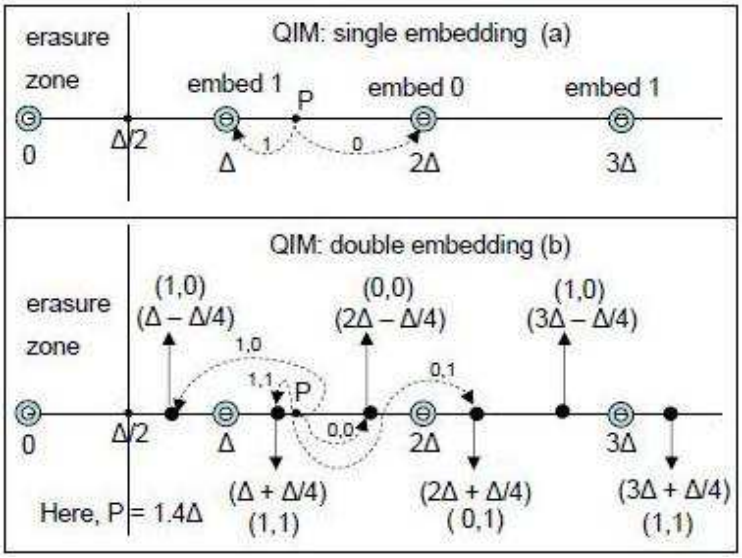


Fig. 12. QIM based Information hiding for single and double embedding

For hiding, we use quantized discrete cosine transform (DCT) coefficients. For perceptual transparency, we do not modify coefficients that are too close to zero; hence, all coefficients in the range [-0.5, 0.5] are mapped to zero and are regarded as erasures.

The two quantizers used for double embedding (Figure 12(b)) have quantization intervals of Δ and Δ/2, respectively. In the example (Figure 12(b)), Δ = 1 and the DCT coefficient (P) equals 1.4. Let the first bit to be embedded be 1 (using the coarser quantizer) and the second

bit be 0 (using the finer quantizer).To embed 1, the coefficient (1.4) is changed to the nearest odd multiple of Δ (1). For the second bit, the coefficient is decreased/ increased by Δ/4 to embed 0/1 respectively. To embed 0, the coefficient is changed from 1 to 0.75.

Although it is now well-accepted that binning methods (QIM) are better suited for high-capacity hiding, SS techniques continue to receive a lot of attention because of their perceived advantage for achieving robustness. QIM-based schemes provide robustness against several attacks while embedding large number of bits. The subtractive dither quantization error (SDQE) does not depend on the quantizer input when the dither signal d has a uniform distribution within the range of one quantization bin (d_i € [-Δ/2, Δ/2]), leading to an expected squared error $e^2 = \Delta^2/12$.

c. Spread transform

Spread transform (also called projection) makes the embedding distortion concentrating on one coefficient spread to multiple coefficients. This leads to some advantages, such as the satisfaction of peak distortion limitations. This section presents a multiple watermarking method based on spread transform, in which cover vectors extracted from the cover works are projected to multiple orthogonal projection vectors. Then different watermark signals are embedded in different orientations of these orthogonal projection vectors. The embedding and extracting methods are introduced, and its performances are analyzed.

i. Watermark embedding process

The above discussion suggests the following general procedure for embedding multiple watermarks into the same image.

1. Read the input image to be watermarked.
2. Extract the cover vectors from the cover image by first dividing the image into blocks of 8×8 pixels and compute DCT for each block.
3. Choose L projection vectors to hide L different watermark signals such that number of projection vectors remains orthogonal to each other.
4. Embed different watermarks into corresponding projected data using dither modulation.

The mark is a Watermark sequence of binary values, w_i € 0, 1.

Coefficient selection

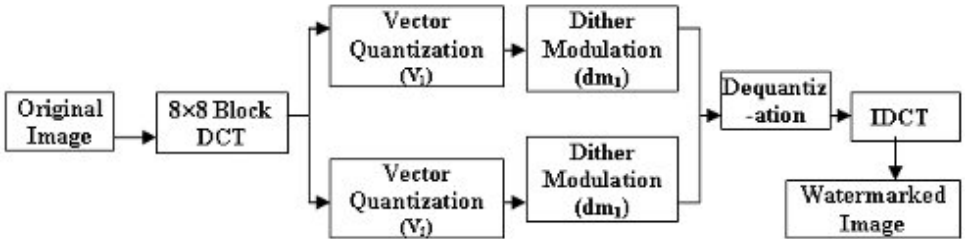


Fig. 13. Watermark Embedding

The proposed algorithm pseudo randomly selects 88 DCT coefficient blocks which are orthogonal to each other. These blocks are considered as a vector and the condition of orthogonality is $V_1 . V_2^T = 0$.

For embedding firstly, each block is quantized using to the JPEG quantization matrix and a quantization factor Q. Quantization is defined as division of each DCT coefficient by its corresponding quantizer step size, followed by rounding to the nearest integer. In this step the less important DCT coefficients are wiped out. This (lossy) transformation is done by dividing each of the coefficients in the 8x8 DCT matrices by a weight taken from a quantization table. If all the weights are equal, the transformation does nothing but if they increase sharply from origin, higher spatial frequencies are dropped quickly. Most existing compressors start from a sample table developed by the ISO JPEG committee. Subjective experiments involving the human visual system have resulted in the JPEG standard quantization matrix. With a quality level of 50, the matrix renders both high compression and excellent decompressed image quality. If however, another level of quality and compression is desired, scalar multiplies of the JPEG Standard quantization matrix (QM) may be used

16	11	10	16	24	40	51	61
12	12	14	19	26	58	60	55
14	13	16	24	40	57	69	56
14	17	22	29	57	87	80	62
18	22	37	56	68	109	103	77
24	35	55	64	81	104	113	92
49	64	78	87	103	121	120	101
72	92	95	98	112	100	103	99

Table 1. JPEG standard quantization matrix for quality factor (QF) =50

For a quality level greater than 50 (less compression and higher image quality), the standard QM is multiplied by (100-quality level)/50. For a quality less than 50 (more compression, lower image quality), the standard QM is multiplied by 50/quality level. The scaled QM is then rounded and clipped to have positive integer values ranging from 1 to 255. For example, the following QM yields quality levels of 10 and 90.

Then, let f_b denote an 8×8 DCT coefficient block and $f_b(m_1; n_1)$,

80	60	50	80	120	200	255	255
55	60	70	95	130	255	255	255
70	65	80	120	200	255	255	255
70	85	110	145	255	255	255	255
90	110	185	255	255	255	255	255
180	175	255	255	255	255	255	255
245	2555	255	255	255	255	255	255
255	255	255	255	255	255	255	255

Table 2. JPEG standard quantization matrix for quality factor 10

3	2	2	3	5	8	10	12
2	2	3	4	5	12	12	11
3	3	3	5	8	11	14	11
3	3	4	6	10	17	16	12
4	4	7	11	14	22	21	15
5	7	11	13	16	12	23	18
10	13	16	17	21	24	24	21
14	18	19	20	22	20	20	20

Table 3. JPEG standard quantization matrix for quality factor 90

f_b (m_2; n_2) are the selected coefficients within that block. The absolute difference between the selected coefficients is given by:

$$\Delta_b = f_b(m_1; n_1) - f_b(m_2; n_2)$$

In order to embed one bit of watermark information, w_i, in the selected block b_i, the coefficient pair $f_b(m_1; n_1)$; $f_b(m_2; n_2)$ is modified such that the distance becomes where q is a parameter controlling the embedding strength.

$$\Delta_b = \begin{cases} \leq q, \ if \ w_i = 0 \\ \geq q, \ if \ w_i = 1 \end{cases}$$

In this proposed method the two watermarks are embedded using DM method with uniform, scalar quantizer of step size Δ, where Δ is the quantization step used to control the embedding distortion. This method is called double spread transform dither modulation (DSTDM). Figure 14 shows the realization of DM, where, x_0 is the original data, x_w is the watermarked data and q_Δ (·) is the basic quantizer function, that is

$$q_\Delta(x) = \text{round}(x/\Delta) \times \Delta$$

Where Δ is the quantization step used to control the embedding distortion and each coefficients quantization step can differ from each other, d[m] is the dither value corresponding to the watermark information m.

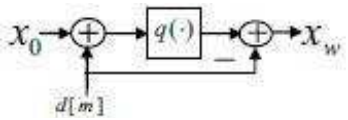


Fig. 14. Watermark Embedding Process of DM

iv. Watermark extraction method

In watermark detection process the embedded watermark signals are extracted using corresponding extraction method and compared with the original watermarked data. Extraction method depends on the embedding method used. The watermark extracting process is the reverse process of the watermark embedding process. Minimum distance decoder is used to extract the watermark which is similar to STDM algorithm. The detailed extracting method of DSTDM is following:

1. Extract the cover vectors by computing DCT in the blocks of 8 × 8 pixels of watermarked image.
2. Project the cover vectors to the same projection vectors used in the embedding process.
3. Apply DM with the same quantization step M.
4. Apply minimum distance decoding rule into the corresponding dither value received by dither modulation.

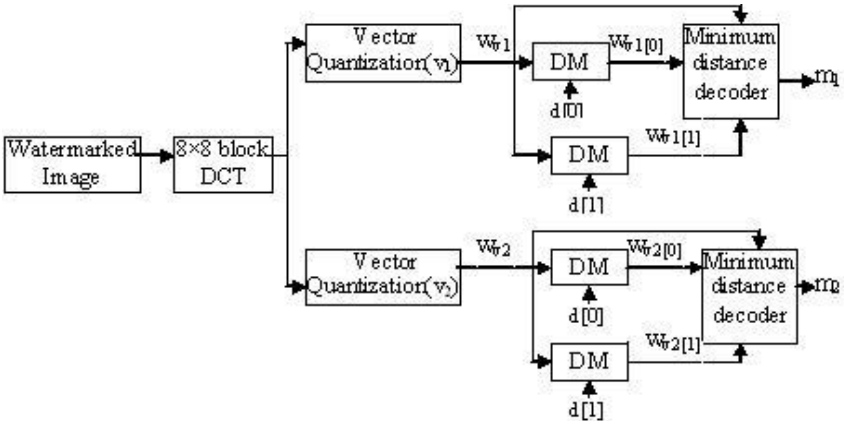


Fig. 15. Watermark extraction

The minimum distance decoding rule is

$$m_i = \arg_{h \in 0} \min \; | W_{vi}[h] - W_{vi} | \; i \in 1,2$$

Where W_{vi} [0] and W_{vi} [1] represent dither modulation result of W_{vi} using d[0] and d[1] as dither value , Vi is the projection vector and mi is the ith extracted watermark signal. During watermark extraction phase, the elements of the signal received at the decoder are quantized using each dither quantizer. The received message is reconstructed from the indices of the sequence of quantizers which contain the reconstruction points closest to the elements. The decoder extracts the embedded information mi based on dither modulation result W_{vi}. It is well known that due to insertion of watermark, there will be degradation in visual quality of the host image (cover image). The degree of deterioration depends on the size of watermark embedded as well as step size used for DM. To achieve that goal, watermark bits are detected using minimum distance decoder and the remaining self-noise due to watermark embedding is suppressed to provide better quality of image. In case of more than two watermark signals, DSTDM can be generalized to multiple spread transform dither modulation (MSTDM). In this situation, the cover vector extracted from the cover work using Rule 1 is projected to multiple (for example, M) projection vectors Vi (i2 1,2,...,M) orthogonal to each other. Then different watermark signals are embedded using DM in different directions, respectively. The extracting method of MSTDM is similar to that of DSTDM.

4. Statistical measures of image robustness

Performance of embedding technique is decided based on some numerical identities such as quality of reconstructed image and extracted information similarity. These are measured with PSNR and bit error ratio respectively.

4.1 PSNR (Peak Signal to Noise Ratio)

The PSNR computes the peak signal-to-noise ratio, in decibels, between two images. This ratio is often used as a quality measurement between the original and a compressed image. The higher the PSNR, the better is the quality of the compressed or reconstructed image. The Mean Square Error (MSE) and the Peak Signal to Noise Ratio (PSNR) are the two error metrics used to compare image compression quality. The MSE represents the cumulative squared error between the compressed and the original image, whereas PSNR represents a measure of the peak error. The lower the value of MSE, the lower is the error. To compute the PSNR, first calculates the mean-squared error using the following equation:

$$\text{MSE}= \sum_{M,N} \frac{[\text{I}_1(m,n) - \text{I}_2(m,n)]^2}{M \times N}$$

M and N are the number of rows and columns in the input images, respectively. The PSNR is given by the following equation:

$$\text{PSNR} = 10 \log_{10} \left| \frac{R^2}{MSE} \right|$$

R is the maximum fluctuation in the input image data type. For example, if the input image has a double-precision floating-point data type, then R is 1. If it has an 8-bit unsigned integer data type, R is 255, etc. Logically, a higher value of PSNR is good because it means that the ratio of Signal to Noise is higher. Here, the 'signal' is the original image and the 'noise' is the error in reconstruction. So, if you find a compression scheme having a lower MSE (and a high PSNR), you can recognize that it is a better one. Usually PSNR of more than 35 dB is considered good quality.

4.2 Bit error ratio

Compare the difference between the original binary watermark w and the extracted binary watermark w, and this equals to computing the bit error ratio (BER):

$$\text{BER} = \frac{XOR(w, w')}{L}$$

Where L is length of the binary bit stream of watermark.

5. Summary

The method presented provides effective balance between robustness, complexity, and image quality. Multiple watermark signals are embedded in different orientations of the cover vectors extracted from the cover works, so that different watermark signals will not mutually interfere. Comparing with other relative watermarking techniques, this method yields significant improvements in invisibility and robustness. The proposed method is very flexible and its mathematical background is very clear. Experimental results also show that the presented method can avoid the interference of one watermark signal with another very well, which is one of the most important and difficult problems for a multiple watermarking algorithm and its achieved validity can be 100%.

6. References

[1] Voloshynovskiy, S.et al., ''Attacks on digital watermarks: Classification, estimation based attacks and benchmarks'', IEEE Communications Magazine, vol.39(8), pp.118-126, Aug 2001.

[2] Nasir Memon and Ping Wah Wong, ''Protecting Digital Media Content'', Communications of the ACM, Volume 41, No. 7, pp. 34-43, 1998.

[3] S. P. Mohanty, J. R. Ramakrishnan, and M. S. Kankanhalli, ''A DCT domain visible watermarking technique for images'', IEEE International Conference on Multimedia and Expo, Volume 2, pp. 10291032, 2000.

[4] Hongjie He, Jiashu Zhang, Fan Chen, ''Block-wise Fragile Watermarking Scheme Based on Scramble Encryption'', IEEE International conference on Bio-Inspired Computing: Theories and Applications, PP. 216 220, 2007.

[5] M. M Yeung, F. Mintzer, "An invisible watermarking technique for image verification'', Proceedings of IEEE International Conference on Image Processing, pp. 680 683, 1997.

[6] Yuichi Nakai, ''Semi Fragile Watermarking Based on Wavelet Transform'', Proceeding of the SPIE, Security and Watermarking of Multimedia Contents, pp. 796- 803, 2001.

[7] Van Schyndel, R.G.; Tirkel, A.Z.; Osborne, C.F., ''A Digital Watermark'', Proceedings of IEEE International Conference on Image Processing, pp. 86-90, 1994.

[8] I. Nasir, Ying Weng, Jianmin Jiang, ''Novel Multiple Spatial Watermarking Technique in Color Images'', IEEE International Conference on Information Technology: New Generations, pp. 777 - 782, 2008.

[9] F. Mintzer and G. W. Braudaway, ''If one watermark is good, are more better?'' Proceedings of the International Conference on Accoustics, Speech and Signal Processing, Volume 4, pp. 20672070, 1999.

[10] N. P. Sheppard, R. Shafavi-Naini, and P. Ogunbona, ''On multiple watermarking'' Proceedings of the ACM Multimedia and Security Workshop 2001, ACM Press, pp. 36 , 2001

[11] J. Cox, M. L. Miller, and J. A. Bloom, ''DigitalWatermarking and fundamentals'', Morgan Kaufmann series, San Francisco, 2002.

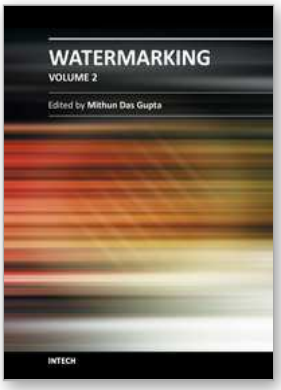
[12] M Barni, Franco Bartolini, Vito Cappellini, Alessandro Piva, ''A DCT-domain system for robust image watermarking'', Elsevier journal of Signal Processing, Volume 66, No. 3, pp. 357-372, 1998.

[13] Mitchell D. Swanson, Bin Zhu, and Ahmed H. Tewfik, ''Transparent Robust Image Watermarking'', Proceedings of IEEE International Conference On Image Processing, pp. 211-214, 1996.

[14] X. Xia, Charles G. Boncelet, Gonzalo R. Arce, ''A Multiresolution Watermark for Digital Images'' Proceedings of IEEE International Conference on Image Processing, pp.548-551, 1997.

[15] X. Liang; Wu Huizhong, ''Multiple perceptual watermarks using multiple-based number conversion in wavelet domain'', IEEE International Conference on Communication Technology, Volume 1, pp. 213 - 216, 2003.

[16] Lan Hongxing,Chen Songqiao, Li Taoshen, Hu Aina,''A Digital Watermarking Algorithm Based on Dual-tree Complex Wavelet Transform'', IEEE International Conference for Young Computer Scientists, pp. 1488-1492, 2008.



Watermarking - Volume 2

Edited by Dr. Mithun Das Gupta

ISBN 978-953-51-0619-7
Hard cover, 276 pages
Publisher InTech
Published online 16, May, 2012
Published in print edition May, 2012

This collection of books brings some of the latest developments in the field of watermarking. Researchers from varied background and expertise propose a remarkable collection of chapters to render this work an important piece of scientific research. The chapters deal with a gamut of fields where watermarking can be used to encode copyright information. The work also presents a wide array of algorithms ranging from intelligent bit replacement to more traditional methods like ICA. The current work is split into two books. Book one is more traditional in its approach dealing mostly with image watermarking applications. Book two deals with audio watermarking and describes an array of chapters on performance analysis of algorithms.

How to reference

In order to correctly reference this scholarly work, feel free to copy and paste the following:

Jaishree Jain and Vijendra Rai (2012). Robust Multiple Image Watermarking Based on Spread Transform, Watermarking - Volume 2, Dr. Mithun Das Gupta (Ed.), ISBN: 978-953-51-0619-7, InTech, Available from: http://www.intechopen.com/books/watermarking-volume-2/robust-multiple-image-watermarking-based-on-spread-transform

INTECH
open science | open minds

InTech Europe
University Campus STeP Ri
Slavka Krautzeka 83/A
51000 Rijeka, Croatia
Phone: +385 (51) 770 447
Fax: +385 (51) 686 166
www.intechopen.com

InTech China
Unit 405, Office Block, Hotel Equatorial Shanghai
No.65, Yan An Road (West), Shanghai, 200040, China
中国上海市延安西路65号上海国际贵都大饭店办公楼405单元
Phone: +86-21-62489820
Fax: +86-21-62489821