www.ijecs.in

International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 3 Issue 7 July, 2014 Page No. 7204-7313

Digital Image Watermarking Technique

Aditya Bhagat, Shikha Singh
M.Tec (DC)
Dr. C.V. Raman University
Bilaspur, India
rajeaadi@gmail.com
Asst Professor
Dr. C V Raman University
Bilaspur India
shikha.mishra687@gmail.com

***Abstract*—The "Digital Image Watermarking" is the process of embedding information into a digital media without compromising the media's value in a way that it is difficult to remove. This is basically used to hide the information from attackers.**

The rapid expansion of the Internet in the past years has rapidly increased the availability of digital data such as images, audio and videos to the public. As it is witnessed in the past few years, the problem of protecting multimedia information becomes more and more important and a lot of copyright owners are concerned about protecting any illegal duplication of their data or work. Some serious work needs to be done in order to maintain the availability of multimedia information but, in the meantime, the industry must come up with ways to protect intellectual property of creators, distributors or simple owners of such data [1].

This is an interesting challenge and this is probably why so much attention has been drawn toward the development of digital images protection schemes. Of the many approaches possible to protect visual data, digital watermarking is probably the one that has received most interest. With the growing popularity of digital media through the World Wide Web, intellectual property needs copyright protection, prevention of illegal copying and verification of content integrity. So keeping all these aspects and need of such system the proposed work is to provide more robustness, clarity and authentication to digital data. The system is based on digital image watermarking centering the attention to image authentication and clarity to give support to digital rights management in real world and internet or world web.

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. Digital watermarking today is used in various applications. Copyright protection for online shops by customer identification watermarking, also called transaction watermarking, may be the most prominent example for this, offering an alternative to more restrictive digital rights management approaches. But in order to enable efficient transaction watermarking, a new challenge for applied algorithms arises: Besides the common requirements of transparency and robustness a very fast embedding strategy is necessary as otherwise users would face unacceptable delays before they can download their marked content. This can be addressed either by designing algorithms of very low complexity or by choosing suitable support mechanisms to speed up watermark embedding. The first approach is still an open challenge as watermarking algorithms of low complexity today fail to provide high robustness and transparency. Therefore an introduction to strategy is provided to support fast and less complex watermark embedding in which algorithm is slightly altered to enhance the clarity. For this some of the existing and popular image watermarking techniques are compared on the basis of their performance and least complex as well as suitable technique is chosen for the alteration.

1. PROPOSED WORK

The new data hiding techniques need to be developed that satisfy the requirements of imperceptibility, robustness, capacity, or data hiding rate and security of the hidden data etc. The attention here is centered to give the benchmark algorithm watermark more clarity, robustness and authentication as well as making it less complex for the computation. The objective of this project is to compare available Digital Image Watermarking Techniques and thus finding the benchmark technique available till date. After finding the benchmark technique its algorithm is slightly modified to get more robustness and clarity in the recovered message, which results in better authentication in the completely watermarking process. The modification uses correlation factors and different sequences for '0' and '1' for

Digital Image. Now, Cosine transform plays the role of an efficient tool because of multi resolution capability that highlights the local and global property of the signal. Data embedding in image characteristics regions expected to show resiliency against different types of the unintentional and or deliberate attacks. Bit Plane modulation in wavelet domain is to be developed to provide resiliency against volumetric distortion sources. The aim of this thesis is to explore the issues in domain data hiding and make possible improvements.

The immense advantages offered by the Digital domain over that of the Analog has prompted us to switch over to the former domain. The world is primarily analog. However, the quality obtained in analog signal processing and transmission is often far from the desired. Thus, a digital system both for signal processing and for transmission has gained importance over the past few years. Digitization of real life analog signals requires sampling and quantization. This leads to the loss of some information in the form of quantization error. However, by suitably adjusting the number of quantization levels this error may be limited to render undetectable by the human senses, which have a finite resolution capability. On the other hand, transmissions over digital channels provide high noise immunity, and efficient utilization of channel capacity through multiplexing [2].

2. FACTORS TO BE CONSIDERED

A watermark can show several noteworthy features. These include that the watermark is difficult to make out, tolerates common distortions, transfers several bits of information, is competent of synchronizing with other watermarks, and requires a bit of computation for insertion or detection. An excellent watermarking system for images should fulfill the following requirements:

- Clarity:
  While transmitting, hacker is not able to detect that the hidden image is present only if watermarked image has more clarity just like it is the single image. Moreover, receiver gets less distortion while detecting the image if more clarity is there.

- Security:
  The watermarking scheme must be protected even while the embedding algorithm is enabled as public. Security is basically obtained by employing cryptographic techniques.

- Transparency:
  The embedded watermark is ought to grade the image quality to a higher level. Message should be clear in HVS.

- Appropriate complexity:
  The computation and memory requirements should be less compared with the compression/decompression processes, particularly for real time applications.

- Robustness:
  The embedded watermark should endure general image processing operations like cropping, rotation, filtering and compression.

There are a number of measurable characteristics that a watermark should exhibit. These include that it should be difficult to notice, robust to common distortions of the signal, resistant to malicious attempts to remove the watermark, support a sufficient data rate commensurate with these application, allow multiple watermarks to be added and that the decoder be scalable [3].

3. MOTIVATION

Digital systems and channels are highly cost effective. This has generated a natural gradient in favor of the digital domain. The revolution in information technology may be mainly attributed to the advancements in digital signal processing and data transmissions over digital channels. Watermarking has the potential to provide simple and easily implemental solution to rightful ownership. Most of the standard cryptographic techniques are beyond the use because of their complexity and their weakness in providing copyright protection. In this work an algorithm is developed altering the benchmark algorithm in transform domain for gray level image as watermark to give it more clarity and robustness. The work can be extended to video, speech and audio.

4. CONTRIBUTION

In this proposed work, a project is developed in order to make digital rights management system less complex and enhancing clarity in digital image watermark system.
Here is a short description of my work:

- Analysis of different data hiding techniques and their contribution in today’s digital world, analysis of digital image watermarking techniques.

- Study and comparison among different digital image watermarking techniques on basis of their performance parameters and thus choosing benchmark technique among them.

- Programming according to requirement and modifying algorithm.

- Alteration is benchmark algorithm to get more clarity and studying the result found, altering it again if more clarity is required.

- Last step is to imply the alteration in programming and again comparing the results.

5. DATA HIDING

Data Hiding is a process to hide a data from attackers. Data Hiding should be done through a various methods.

5.1. HISTORY OF DATA HIDING

Data Hiding has been used in various forms for 2500 years. It has found use in variously in military, diplomatic, personal and intellectual property applications. Briefly stated, data hiding is the term applied to any number of processes that will hide a message within an object, where the hidden message will not be apparent to an observer. This chapter will explore data hiding from its earliest instances and watermarking as its present potential application. The idea of communicating secretly is as old as communication itself. The earliest allusion to secret writing in the west appears in

Homer's Iliad. Steganographic method made their record debut few centuries later in several tales by Herodotus, the father of history. An important technique was the use of sympathetic inks. Later chemically affected sympathetic inks were used. This was used in World War 1 and 2. The term steganography came into use in 1500's after the appearance of Trithemius' book on Steganographia, semagram, and open code. Semagram is secret message not in written form.

Watermarking has evolved from Steganography. Watermarking is as old as paper manufacturing. Today most developed countries watermark their paper, currencies and postage stamps to make forgery more difficult. The digitization of the world has expanded the watermarking concept to include immaterial digital impressions for use in authentication ownership claims and protecting proprietary interests. Watermarking gives guarantee of authenticity, quality ownership and source confirmation. In the past 10 years, data-hiding technique has been very popular in area of research and watermarking is being the most technique in this area for scholars.

5.2. PREVIOUS RESEARCH WORK ON WATERMARKING

Successive generations of researchers have addressed watermarking techniques and its different aspects.

D. Kahaner, C. Moler and S. Nash, in 1989 proposed numerical methods and software for watermarking techniques which basically gives the computational measures for watermarking methods[4].

Chang Tsun Li et. al. in 1993, describes fragile watermarking scheme for image authentication. In which an efficient fragile watermarking scheme intended for image authentication and integrity verification is proposed. To watermark the underlying image, the gray scale of each pixel is adjusted by an imperceptible quantity according to the consistency between a key dependent binary watermark bit and the parity of a bit stream converted from the gray scales of a secret neighborhood of the pixel. To counter "collage" and "look-up table inferring" attacks, the scanning/watermarking order of the pixels follows a zig-zag path and the secret neighborhood of a pixel is formed by picking previously watermarked pixels before the current pixel on the scanning path[5].

Cox, J. Kilian, T. Leighton, and T. Shamoon in 1997 had proposed technique for secure spread spectrum watermarking for multimedia in which CDMA spread spectrum watermarking is discussed in brief with security issues[6].

Memon, N. and Wong, P., in 1998 gave paper about Protecting Digital Media Content which defines the necessity of protection and security in digital media and also suggested methods for protection of media [7].

Chiou Ting et. al in 1999 shows the survival of watermark after lossy attacks. In experiment, an image authentication technique by embedding digital "watermarks" into images was proposed. Watermarking is a technique for labeling digital pictures by hiding secret information into the images. Sophisticated watermark embedding is a potential method to discourage unauthorized copying or attest the origin of the images. Embed the watermarks with visually recognizable patterns into the images by selectively modifying the middle-frequency parts of the image. Several variations of the proposed method were addressed. The experimental results shown that the proposed technique successfully survives image processing operations, image cropping, and the Joint Photographic Experts Group (JPEG) lossy compression [8].

G. Voyatzis and I. Pitas,in 1999 proposed The use of watermarks in the protection of digital multimedia products which details that digital media can be secured with the help of watermark and the implementation method [9].

G. C. Langelaar, I. Setywan and R. L. Lagendijk, in 2000 gave method for Watermarking digital image and video data, which specifies the size constraints and the different strategies for still and video image [10].

J. Hernandez, M. Amado and F. Perez-Gonzalez,in 2000 proposed DCT domain watermarking techniques for still images in which Detector performance is analyzed and a new structure is proposed for the same [11].

Katzenbeisser S. and Petitcolas F.A.P., in 2000 proposed Information Hiding Techniques for Steganography and Digital Watermarking where the common factors about two methods are discussed and shown that advancement in first results in the second method [12].

Ohbuchi R. et. al in 2002, discussed robust watermarking for digital vector maps. Digital maps are used, for example, in car navigation systems and Web-based map services. As digital data, digital maps are easy to update, duplicate, and distribute. At the same time, illegal duplication and distribution or forgery of the maps is also easy. This research proposes a digital watermarking algorithm for vector digital maps as a method to counter such abuses of the maps. A watermark bit is embedded by displacing an average of coordinates of a set of vertices that lies in a rectangular area created on a map by adaptively subdividing the map. The watermark is resistant against additive random noise, similarity transformation, and vertex insertion/removal, and, to some extent, cropping [13].

R. Liu and T. Tan, in 2002 gave a SVD-Based watermarking scheme for protecting rightful ownership which gives the definition of Digital Rights Management and proposes the scheme for protection [14].

R. Mehul and R. Priti, in 2003 proposed Discrete Wavelet Transform based multiple watermarking schemes which show the DWT algorithm can be implemented in different ways to the watermark [15].

E. Ganic and A. M. Eskicioglu, in 2004 proposed Secure DWT-SVD Domain Image Watermarking in which data is embedded in all frequencies removing the need of only main frequency components and also making the system less complex [16].

Ko Ming et. al in 2004 proposed a novel public watermarking system based on advanced encryption system. Until then many digital watermarking techniques have been proposed to resolve the issues of copyright protection. However, almost proposed watermarking methods keep the watermarking algorithm private to ensure the embedded watermark secret. If the watermarking technique needs to be widespread applied to realistic multimedia environment, the algorithm used by watermarking techniques should be public. In this work, a novel watermarking scheme, which can be public, is presented. The proposed watermarking technique is developed based on the following criterions: first the watermarking algorithm is open; and second the embedded watermark can be extracted and embedded by the people who own the secret key. The watermarking scheme employs the advance encryption standard (AES) and the Reed-Solomon code, to make the watermarking algorithm public. Simulation shows that the proposed algorithm can be very robust to resolve the ownership of the digital image [17].

Fan Jhang et.al. in 2004, did research on watermarking capacity. The work shows image-watermarking capacity is an evaluation of how much information can be hidden in a digital image. Watermarking capacity research studies how to transmit more watermark information. In watermarking schemes, the image is considered as a communication channel to transmit messages. Watermark power should be constrained according to the content of the image. Analyses the shortcomings of some previous watermarking capacity methods and present a watermarking capacity method using the noise visibility function, and discuss the watermarking capacity of blind watermarking and non-blind watermarking [18].

Celik M.U. et.al. in 2006 presented a novel framework for lossless (invertible) authentication watermarking, which enables zero-distortion reconstruction of the un-watermarked images upon verification. As opposed to earlier lossless authentication methods that required reconstruction of the original image prior to validation, the new framework allows validation of the watermarked images before recovery of the original image. This reduces computational requirements in situations when either the verification step fails or the zero-distortion reconstruction is not needed. For verified images, integrity of the reconstructed image is ensured by the uniqueness of the reconstruction procedure. The framework also enables public-key authentication without granting access to the perfect original and allows for efficient tamper localization. Effectiveness of the framework is demonstrated by implementing the framework using hierarchical image authentication along with lossless generalized-least significant bit data embedding [19].

Lahouari Ghouti, Ahmed Bouridane, Mohammad K. Ibrahim, and Said Boussakta, in 2006 proposed concept of Digital Image Watermarking using balanced multiwavelets which includes the wavelets decomposition method for watermarking of images [20].

Xiang-Yang Wang and Hong Zhao, in 2006 proposed A Novel Synchronization Invariant Audio Watermarking Scheme Based on DWT and DCT in which audio watermarking is done with DCT as well as DWT method to improve the performance of watermark [21].

Steinebach M.i et.al. in 2007 proposed efficient transaction watermarking, a new challenge for applied algorithms arises: Besides the common requirements of transparency and robustness a very fast embedding strategy is necessary as otherwise users would face unacceptable delays before they can download their marked content. This can be addressed either by designing algorithms of very low complexity or by choosing suitable support mechanisms to speed up watermark embedding. The first approach is still an open challenge as watermarking algorithms of low complexity today fail to provide high robustness and transparency. We therefore provide an introduction to three strategies to support fast watermark embedding: Container watermarking based on pre-calculations which today is already used in industrial applications, client-server watermarking where the content is marked after the transfer to the customer and grid watermarking using the computational power of grid networks [22].

Jiang Bin et.al. in 2008 proposed multi-channel DWT domain image watermarking which is robust to geometric attacks, Firstly, this DWT domain watermarking generates a watermarking template referring to one channel DWT coefficients of the image. Secondly, this watermarking template is embedded into other DWT channel of this image. Because both watermarking template and watermarking image undergo same geometric attack, self-synchronization between the embedded watermarking and watermarking image can be obtained automatically during detecting watermarking. Therefore, a high robust performance of resist geometric attack is gained. Finally, several experimental results are given to show that the proposed watermarking algorithm achieves a high robustness even if an image undergoes some serious geometric distortion attacks [23].

Lintav Lv et.al. in 2010 proposed a semi-fragile watermarking algorithm resisting to RST (Rotation, Scaling, Translation). The algorithm can be used to verify the authenticity and integrity of image content. Firstly, the algorithm generates watermarking information by using the edge of the scaled image, and embeds watermarking information based on human visual system. Before detecting watermarking, the parameters of geometric distortions are estimated and restored by using the original moment information. Finally, users compare the extracted watermarking information with the reconstructed watermarking information of the watermarked image to achieve authentication. The experiment results show that the watermarking algorithm has the immunity to common operation (Compression, Noise, Filtering, RST, and so on). The watermarking algorithm can also achieve accurate authentication and tampering localization to malicious processing (Cropping, Replacing)[24].

Shinfeng D. Lin, Shih-Chieh Shie, J.Y. Guoa,in 2010 proposed method for improving the robustness of DCT-based image watermarking against JPEG compression where compression is taken as attack and is dealt with right strategy [25].

6. PROBLEMS IN DIGITAL IMAGE WATERMARKING

6.1. PROBLEM STATEMENT

In an attempt to satisfy the conclusion made in literature review chapter and in today’s digital media world, here it is required to understand first, what is the problem that is faced by digital media world, which may be considered as follows:

- What is the threat in digital media world.
- Why is there constant need of newer methods of data hiding.
- How the authentication and copyright protection is achieved.
- Which method of watermarking is optimum for image protection i.e. benchmark algorithm for watermarking.
- How the watermark can be given more clarity, robustness and authentication while keeping the algorithm less complex.

The above is the summary of the information obtained from the literature review and the present techniques to describe problem of robustness, authentication, clarity and complexity in digital watermarking.

6.2. PROBLEM IN DIGITAL MEDIA WORLD

The ease of accessibility of digital media and the simplicity of the digital systems has rendered the contents over the digital media highly insecure. Digital entities can be easily duplicated, manipulated, or even tampered with. Thus the question of copyright associated with a digital entity faces a severe threat from hackers. The Internet is considered as a perfect auction and distributionchannel for digital data; however their remains a hindrance, whiledealing with copyright compliance and content management.Nowadays, digital images can be employed in any area ofinterest– with or without permission. When the images are put towrong use or leaked, it can spoil brand image, marketing works,eventually this extends and produce a major impact in sales. It isvital to safeguard the copyright of digital content against piracyand malicious manipulation, due to the quick development andextensive use of network distributions of digital media content[26].

With the availability of internet around the globe, security ofdigital images has resulted in a greater significance. The launchof image processing tools has brought in a higher liability forillegal copying, alterations, and dispersion of digital images.Watermarking systems have been presented as a feasible andeffectual solution to these problems. Digital watermarking isemployed with an intention of disallowing illegal replication orutilization of digital images. In recent times, there has beena rapid advancement of digital imagery and digital watermarktechnology. The categories of protection systems comprise theutilization of encryption and authentication techniques also[27].

6.3. PROBLEM IN IMAGE WATERMARKING

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 listed below:

- 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
- 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 third party [28].

Here it is needed to run different application and constraints are to be taken into consideration. In this thesis mainly clarity and robustness are considered as primary concern.

6.4. WATERMARKING CONSTRAINTS

The success of the watermarking scheme largely depends upon the choice of the watermark structure and insertion strategy. The two main constraints involved in the problem of watermarking are those of maintaining the robustness of the watermark information while keeping visual perception of the original image intact. If the insignificant portions of the original image are used for hiding the watermark structure then the visual perceptions of the original image may remain unaffected but the robustness of the technique decreases. On the other hand, if the hiding is done in the significant portions of the original image then the robustness of the technique increases at the cost of visual perceptions. Thus, the cost of function of the problem of watermarking is a weighed sum of these factors:

Cost Function, $S = F_R * R + F_V * V$

Where,

F_R = Weighted factor for Robustness,

F_V = Weighted factor for Visual Perceptions,
R = Robustness,
V = Visual Perceptions.

The challenge in any watermarking technique is to maximize this cost function [29].

Properties of Watermarks:

There are a number of measurable characteristics that a watermark should exhibit. These include that it should be difficult to notice, robust to common distortions of the signal, resistant to malicious attempts to remove the watermark, support a sufficient data rate commensurate with these application, allow multiple watermarks to be added and that the decoder be scalable [30].

- Imperceptibility:

The watermark should not be noticeable to the viewer, nor should then watermark degrade the quality of the original image. However, if a signal is truly imperceptible, then perceptually based lossy compression algorithms probably, still leave room for an imperceptible signal to be inserted. This may not be true for the next generation compression algorithms. Thus, to survive the next generation of lossy compression algorithms, it will probably be necessary for a watermark to be noticeable to a trained observer.

- Robustness:

The watermark must be difficult to remove. If only partial knowledge is available (e.g. the exact location of the watermark in an image is unknown) then attempts to remove or destroy a watermark, should result in severe degradation in fidelity before the watermark is lost.

- Common Signal Processing:

The watermark should still be retrievable even if common signal processing operations are applied to the data. These include digital to analog and analog to digital conversion, re-sampling and re-quantization and common signal enhancements to image contrast and color, or audio bass and treble.

- Common Geometric Distortion (Image and video):

Watermarks in image and video data should also be immune from geometric image operations such as rotation, translation, cropping and scaling.

- Subterfuge Attacks:

In addition, the watermarks should be robust to collusion by multiple individuals each possessing a watermarked copy of the data, i.e., the watermark should be robust to combining copies of the same data set to destroy the watermarks. Further, if a digital watermark is to be used in litigation, it must be impossible for colluders to combine their images to generate a different valid watermark with the intention of framing a third party.

- Universal:

The same digital watermarking algorithm should apply to all the three media under considerations. This is potentially helpful in the watermarking of multimedia products. In addition, this feature is conductive to the implementation of audio and image/video watermarking algorithms on common hardware.

7. DIGITAL IMAGE WATERMARKING

This section of the report details different techniques by which image is watermarked**.**

7.1. CRYPTOGRAPHY,STEGANOGRAPHY AND WATERMARKING

First starting with a few definitions,Cryptography can be defined as the processing of information into an unintelligible (encrypted) form for the purposes of secure transmission. With a “key”, the receiver can decode the encrypted message (decrypting) to retrieve the original message. Steganography improves on this by hiding the fact that a communication even occurred. The message *m* is embedded into a harmless message *c*, which is defined as the cover-object. The message *m* is then embedded into *c*, generally with use of a key *k* that is defined as the stego-key. The resulting message is then embedded into the cover-object *c*, which results in stego-object. Ideally the stego-object is indistinguishable from the original message c, appearing as if no other information has been encoded. This can all be seen below in Figure 7.1.

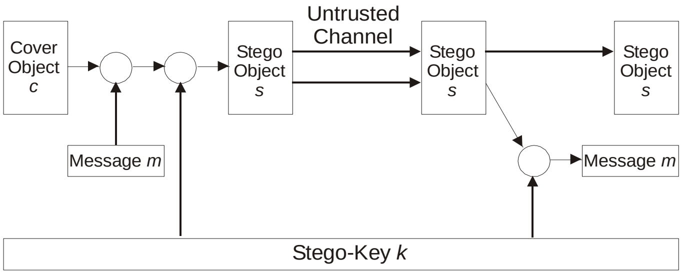

Figure 7.1 Illustration of a Steganographic System

The cover object is only used for the stego-object generation and is then discarded. The hope of the system is that the stego-object will be close enough in appearance and statistics to the original such that the presence of information will go undetected. As mentioned previously, for the purposes of this report we will assume the stego-object to be a digital image, keeping in mind that concepts may be extended to other cover objects as well. Watermarking is very similar to steganography in a number of respects. Both seek to embed information inside a cover message with little to no degradation of the cover-object. Watermarking however adds the additional requirement of robustness. An ideal steganographic system would embed a large amount of information, perfectly securely with no visible degradation to the cover object. An ideal watermarking system however would embed an amount of information that could not be removed or altered without making the cover object entirely unusable. As a side effect of these different requirements, a watermarking system will often trade capacity and perhaps even some security for additional robustness[31].

A generalized watermarking system is devised in Figure 7.2. In the Watermark Insertion Block, copyright information is hidden inside the original piece of work in an encrypted form.

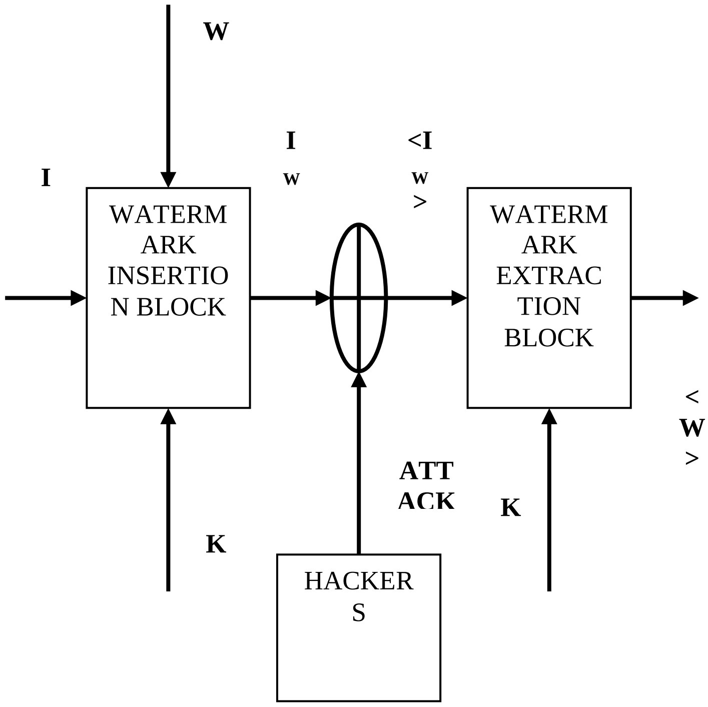

Figure 7.2 Generalized Modelfor a Watermarking System

The original image, I is processed inside this watermark insertion system. The other input to this block is the copyright information or the watermark, W to be embedded inside I using the secret key, K. Thus, the final image available in the market is a composite image, I_w containing the encrypted logo inside the original image. This composite image available in the market has every possibility of being attacked by the hackers in a bid to destroy the watermark embedded inside it, to generate the hacked version, <I_W> of the composite image. Once the hackers become successful in destroying the watermark the original piece of work becomes susceptible to all kinds of fraud. The primary aim of the Watermarking Extraction Block is to successfully extract an estimate of the copyright information, <W> from the hacked version <I_W>**.** The better the watermarking system the more <W> resembles W[33].

7.2. 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 make an assertion about the object. The object may be an image, 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).
- 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[32].

7.3. ENCODING PROCESS

Let us denote an image by a signature by $S = S_1, S_2$ and the watermarked image by 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, mathematically,

$$E(I,S) = \bar{I} \qquad (1)$$

It should be noted that the signature S might be dependent on image I. In such cases, the encoding process described by equation 1 still holds. Following figure 7.3 illustrates the encoding process.

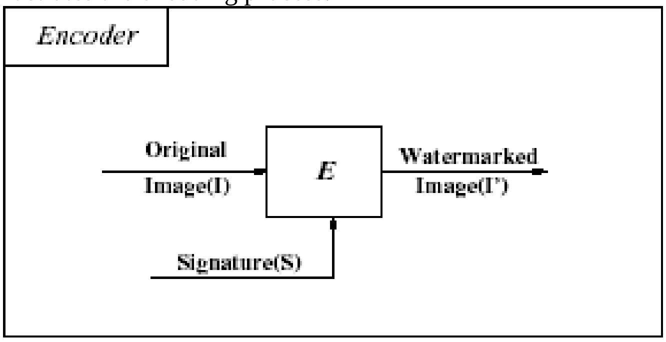

Figure 7.3 Encoder

7.4. 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 because 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

$$D(J,I) = S' \qquad (2)$$

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.

$$C_d = \begin{cases} 1, c \le \delta \\ 0, otherwise \end{cases}$$

$$C_\delta(S', S) = \begin{cases} 1, c \le \delta \\ 0, otherwise \end{cases} \qquad (3)$$

Where C the correlator is $I = C_{\delta}(S^{'}, S)$ is the correlation of two signatures and 0 is certain threshold. Without loss of generality, watermarking scheme can be treated as a three-tupple (E, D, C_{δ}) [34].

Following figures demonstrate the decoder and the comparator.

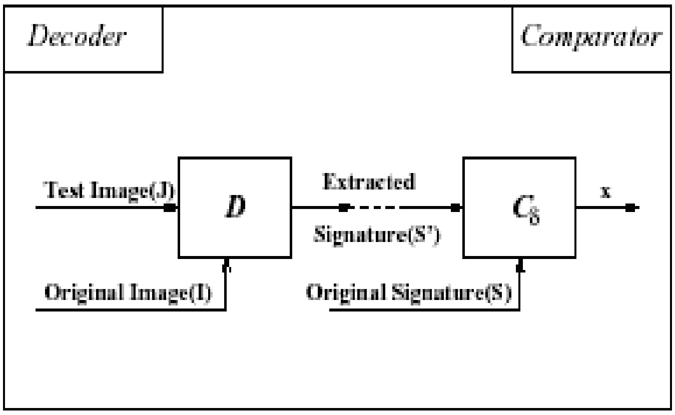

Figure 7.4 Decoder

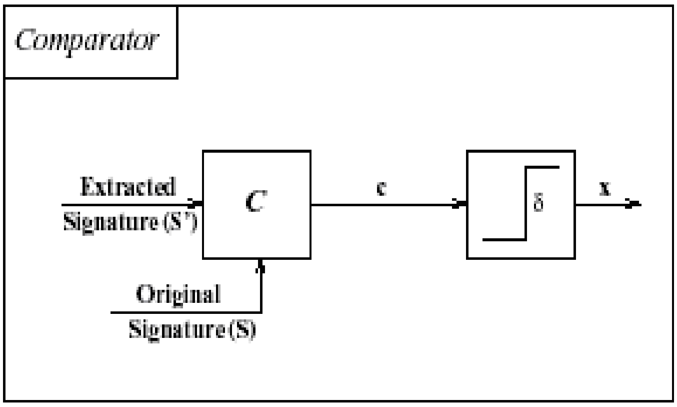

Figure 7.4.1 Comparator

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 could prove ownership whereas watermark detection can only verify ownership[34].

7.5. TYPES OF WATERMARKING

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 divided into 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 embedding in such a way that an alternation 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 [35].In this type of watermark an invisible watermark is used as a backup for the visible watermark as clear from figure 7.5

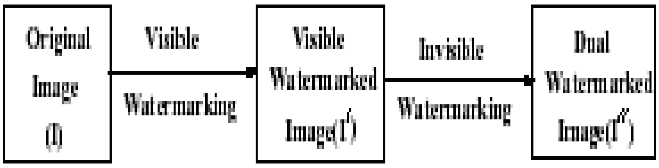

Figure 7.5 Schematic representation of dual watermarking

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 is called invertible watermarking scheme. From application point of view digital watermark could be as below:

- Source based or
- Destination based.

Source-based watermarks 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[36].

Digital watermarking is a technology, which allows a secret message to be hidden in a computer file, without the detection of the user. The watermark is not apparent to the user, and does not affect in any way, the use of the original file. Watermark information is predominantly used to identify the creator of a digital file, i.e. picture, a song, or text[37].

The DRM (Digital Rights Management) software ensures that the user has paid for the file by comparing the watermark to the existing purchased licenses on the system. Other non-rights related uses for watermarking technology include embedding auxiliary information which is related to a particular image or album, album information, or a small web page, etc. A video application of this technology would consist of embedding subtitles or closed captioning information as a watermark.

8. CONCLUSION

An image authentication technique by embedding digital "watermarks" into images is proposed. Watermarking is a technique for labeling digital pictures by hiding secret information into the images. Sophisticated watermark embedding is a potential method to discourage unauthorized copying or attest the origin of the images. In these work different techniques of watermarking is compared based on timing and psnr value. Based on above comparison an optimum algorithm is chosen and it is modified to enhance the clarity of watermark. In this approach, Cox algorithm is used for watermarking and clarity is enhanced by modifying the algorithm slightly not making it complex. This work also enhances the imperceptibility and robustness of the watermark. The work can be very significantly implanted in today's digital media world for authentication purpose by selectively modifying the middle-frequency parts of the image. Several variations of the proposed method are addressed. The experimental results show that the proposed technique successfully survives clarity, authentication and imperceptibility issue and being based on cox algorithm it is not much complex also gives optimum psnr.

This method presents a novel framework for lossless (invertible) authentication watermarking, which enables less distortion reconstruction of the un-watermarked images upon verification. As opposed to earlier lossless authentication methods that required reconstruction of the original image prior to validation, the new framework allows validation of the watermarked images before recovery of the original image. This reduces computational requirements in situations when either the verification step fails or the zero-distortion reconstruction is not needed. For verified images, integrity of the reconstructed image is ensured by the uniqueness of the reconstruction procedure. The framework also enables public(-key) authentication without granting access to the perfect original and allows for efficient tamper localization. Effectiveness of the framework is demonstrated by implementing the framework using hierarchical image authentication along with lossless generalized significant bit data embedding.

9. SCOPE OF FURTHER WORK

The experiment deals with the modification in Cox algorithm in DCT domain and in future the same modification can be applied to any of the other watermarking technique like CDMA watermarking, core watermarking, LSB watermarking, or DWT watermarking so that proper clarity can be achieved in watermarked and recovered images.

This experiment can be extended further by using more numbers of PN sequences and the result can be compared. Using more PN sequences will give the image more authenticity but on the other hand, it can increase the complexity and time of watermarking. For highly secured data transmission that experiment would work perfectly with the transmitter and receiver having private key encryption.

The standard 2-band wavelet transforms result in a logarithmic frequency resolution, thereby suitable for analysis of signals with a justified bandwidth. The resiliency, data embedding rate, computational cost, etc all these have to be examined against volumetric distortions in order to get a benchmark algorithm. Therefore, further work is directed towards the testing of resiliency of data embedding process in wavelet domain.

10. REFERENCES

[1]A. M. Eskicioglu and E. J. Delp, "An overview of multimedia content protection in consumer electronics devices," Signal Processing: Image Communication, vol. 6, no. 7, pp. 618–699, 2001.

[2] Steinebach, M. Hauer, E. Wolf, P. Fraunhofer SIT, Darmstadt "EfficientWatermarking Strategies" on Automated Production of Cross Media Content for Multi-Channel Distribution, AXMEDIS'07, Third International Conference on 28-30 Nov. on pages 65 – 71, 2007.

[3] M. Kutter, S. Voloshynovskiy, and A. Herrigel, "The watermark copy attack," Proceedings of the SPIE Security and Watermarking of Multimedia Contents II, vol. 3971, Jan., pp. 371–380. SPIE-IS&T/ Vol. 5306, 2000.

[4] D. Kahaner, C. Moler and S. Nash, Numerical Methods and Software at New Jersey: Prentice-Hall, Inc, 1989.

[5] Chang-Tsun Li "Oblivious fragile watermarking scheme for image authentication" Acoustics, Speech, and Signal Processing, 1993. In ICASSP-93, IEEE International Conference on 27-30 April on pages IV – VI, 1993.

[6] I. Cox, J. Kilian, T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia," IEEE Transactions on Image Processing, vol. 6, no. 12, pp. 1673–1687, 1997.

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

[8] Chiou-Ting Hsu Ja-Ling Wu , "Hidden digital watermarks in images", Image Processing, IEEE Transactions , issue 1, January on pages 58-68, 1999.

[9] G. Voyatzis and I. Pitas, "The use of watermarks in the protection of digital multimedia products," IEEE Proceedings, Vol. 87, No. 7, pp 1197-1207, July 1999.

[10] G. C. Langelaar, I. Setywan, and R. L. Lagendijk, "Watermarking digital image and video data," IEEE Signal Process. Mag., vol. 17, no. 5, pp. 20-46, Sep. 2000.

[11] J. Hernandez, M. Amado and F. Perez-Gonzalez, "DCT domain watermarking techniques for still images: Detector performance analysis and a new structure", IEEE Trans. Im. Process, Vol: 9, 2000.

[12] Katzenbeisser S. and Petitcolas F. A. P., "Information Hiding Techniques for Steganography and Digital Watermarking", Artech House, UK, 2000.

[13] Ohbuchi, R.; Ueda, H."Robust watermarking of vector digital aps","Multimedia and Expo, In ICME'02. In Proceedings 2002 IEEE International Conference ",on pages 577-580, 2002.

[14] R. Liu and T. Tan, “A SVD-Based Watermarking Scheme for Protecting Rightful Ownership”, IEEE Transactions on Multimedia, 4(1), pp121-128, March 2002.

[15] R. Mehul and R. Priti, “Discrete Wavelet Transform Based MultipleWatermarking Scheme,” Proceedings of IEEE Region 10 Technical Conference on Convergent Technologies for the Asia-Pacific, Bangalore, India, October 14-17, 2003.

[16] E. Ganic and A. M. Eskicioglu, “Secure DWT-SVD Domain Image Watermarking: Embedding Data in All Frequencies,” ACM Multimedia and Security Workshop 2004, Magdeburg,Germany, September 20-21, 2004.

[17] Ko-Ming Chan Long-Wen Chang “Advanced Information Networking and Applications, AINA 18th International Conference “, pages 48-52 vol 1,2004.

[18] Fan Zhang Hongbin Zhang “Communications, Circuits and Systems, ICCCAS 2004. 2004 International Conference” , 27-29 June , pages 796-799 Vol2,2004.

[19] Celik, M.U.; Sharma, G. ” Image Processing, IEEE Transactions “April 2006 ,Issue 4 pages 1042-1049,2006.

[20] Lahouari Ghouti, Ahmed Bouridane, Mohammad K. Ibrahim, and Said Boussakta, "Digital Image Watermarking Using Balanced Multiwavelets", IEEE Transactions On Signal Processing, Vol. 54, No. 4, 2006.

[21] Xiang-Yang Wang and Hong Zhao, "A Novel Synchronization Invariant Audio Watermarking Scheme Based on DWT and DCT", IEEE Transactions On Signal Processing, Vol. 54, No. 12, December 2006.

[22] Steinebach, M. Hauer,” Automated Production of Cross Media Content for Multi-Channel Distribution, 2007. AXMEDIS'07. Third International Conference “, 28-30 Nov, pages 65-71,2007.

[23] Jiang-Bin Zheng Sha Feng, “Machine Learning and Cybernetics, International Conference “ on 12-15 July ,vol2 pages 1046-1051,2008.

[24] Lintao Lv Liang Hao Hui Lv,”Networks Security Wireless Communications and Trusted Computing (NSWCTC), Second International Conference“ on 24-25 April, vol2 on pages 361-364, 2010.

[25] Shinfeng D. Lin, Shih-Chieh Shie, J.Y. Guoa, "Improving the robustness of DCT-based image watermarking against JPEG compression", Computer Standards & Interfaces, Vol: 32, No: 1-2, pp: 54-60, 2010.

[26] E. T. Lin, A. M. Eskicioglu, R. L. Lagendijk, and E. J. Delp, “Advances in digital video content protection” , Proceedings of the IEEE, 2004.

[27] J. Lichtenauer, I. Setyawan, T. Kalker, and R. Lagendijk, “Exhaustive geometrical search and the false positive watermark detection probability,” Proceedings of the SPIE Security and Watermarking of Multimedia Contents V, vol. 5020, Santa Clara, CA, pp. 203–214, Jan. 21–24, 2003.

[28] R. B. Wolfgang, C. I. Podilchuk, and E. J. Delp, “Perceptual watermarking for images and video,” Proceedings of the IEEE, vol. 87, no. 7, pp. 1108–1126, July 1999.

[29] H. C. Kim, H. Ogunleye, O. Guitart, and E. J. Delp, “The watermark evaluation testbed (WET),” Proceedings of the SPIE Security, Steganography, and watermarking of Multimedia Contents VI, vol. 5306, San Jose, CA, January 19–22, 2004.

[30] Rongsheng Xie Keshou Wu Jiangbo Du Chunguang Li Xiamen Univ., Xiamen “Survey of public key Digital Watermarking System” on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing”, 2007. SNPD Eighth ACIS International Conference issue on pages 439-443, date July 30 2007-Aug. 1 2007.

[31] M. Barni, C. I. Podilchuk, F. Bartolini, and E. J. Delp, “Watermark embedding: Hiding a signal within a cover image,” IEEE Communications Magazine, vol. 39, no. 8, pp. 102–108, Aug. 2001.

[32] J. Dugelay, S. Roche, “A Survey of Current Watermarking Techniques”
in Information Techniques for Steganography and Digital Watermarking,
S.C. Katzenbeisser et al., Eds. Northwood, MA Artec House,
pp 121-145,Dec. 1999.

[33] N.F. Johnson, S.C. Katezenbeisser, “A Survey of Steganographic Techniques” in Information Techniques for Steganography and Digital Watermarking, S.C. Katzenbeisser et al., Eds. Northwood, MA: Artec House, pp 43-75,Dec. 1999.

[34] R. B. Wolfang, C. I. Podilchuck, and E. J. Delp, “Perceptual watermarks for digital images and video,” Proceedings of the IEEE, vol. 87, no. 7, pp. 1108–1126, July 1999.

[35] G. Langelaar, I. Setyawan, R.L. Lagendijk, “Watermarking Digital Image and Video Data”, in IEEE Signal Processing Magazine, Vol 17, pp 20-43, September 2000.

[36] I. Cox, J. Kilian, T. Leighton, and T. Shamoon, “Secure spread spectrum watermarking for multimedia,” IEEE Transactions on Image Processing, vol. 6, no. 12, pp. 1673–1687, 1997.

[37] S. Pereira and T. Pun, “Robust template matching for affine resistant image watermarks,” IEEE Transactions on Image Processing, vol. 9, no. 6, pp. 1123–1129, June 2000.

[38] C. I. Podilchuk and E. J. Delp, “Digital watermarking: Algorithms and applications,” IEEE Signal Processing Magazine, vol. 18, no. 4, pp. 33–46, July 2001.

[39] R.C. Gonzalez, R.E. Woods, “Digital Image Processing”, Upper Saddle River, New Jersey, Prentice Hall, pp 23-28 Inc., 2002.