INTERNATIONAL JOURNAL OF SCIENTIFIC PROGRESS AND RESEARCH (IJSPR) ISSN: 2349 - 4689
Volume - 03, Number - 02, 2014

Study of Different Digital Watermarking Schemes and Its Applications

Manoranjan Kr Sinha, Dr. Rajesh Kumar Rai, Prof. G. Kumar
Dept.of E.C.E., NIRT-Bhopal, India

Abstract* - Digital watermarking techniques have been developed to protect the copyright of digital media. In image watermarking, the hidden information is embedded into cover media to prove ownership. Copyright abuse is the motivating factor in developing new encryption technologies. The focus of this paper aims to provide a detailed review and background about the watermarking definition, concept and the main contributions in this field. We can classify the techniques according various categories such as host signal, perceptivity, robustness, watermark type, necessary data for extraction, processing domain, and applications.

Keywords: digital watermarking, Robust, Attacks, PSNR, DCT, DWT.

I. INTRODUCTION

The earliest forms of information hiding can actually be considered to be highly crude forms of private-key cryptography. Greek messengers had messages tattooed into their shave head, concealing the message when their hair finally grew back. Over time these primitive cryptographic techniques improved, increasing both speed, capacity and security of the transmitted message.

Nowadays, the rapid development of technologies has led to the significant increase of digital information, particularly multimedia such as image, audio and video content. Such technological advances have led to the ease in which it is possible to illegally share, distribute, and copy Intellectual Property (IP). An obvious requirement, therefore, is the development of solutions for copyright protection and ownership identification for digital content. Digital watermarking is the process of embedding relevant ownership information (such as a logo, fingerprint and serial number), into a media in order to protect the ownership of different media formats. This technique can be applied to different media types such as video, audio and image content. For the purpose of copyright protection and ownership identification, robust watermarking schemes are mainly used as they can tolerate a host of signal processing attacks that can be both unintentional and intentional.

During the last years, the world is rapidly becoming digital in many aspects. Among the most interesting of these aspects is multimedia. Many new technologies have come into our lives along with multimedia and one of the most recent is watermarking. Digital technology has offered users easy ways to create, process, and distribute digital assets. However, these facilities this may become disadvantages at the same time since it is also much easier to illegally copy and manipulate them. In 2000, the Motion Picture Association of America (MPAA) has calculated lost revenues for American motion picture companies from worldwide piracy to be of the amount $2.5 billion a year. Copyright protection is a very important subject but not the only one in which watermarking appears as one of the very promising solutions. In this communication, we are attempting to go back to the early beginning of this exciting new research field, make an overview of its history, discuss the applications and stakes involved, classify the proposed methods, present the problems and benchmarking tools and finally, try to peak into the future. Steganography or Stego as it is often referred to in the IT community, literally means, "covered writing" which is derived from the Greek language. Steganography is defined by Markus Kahn as follows, "Steganography is the art and science of communicating in a way which hides the existence of the communication. In contrast to Cryptography, where the enemy is allowed to detect, intercept and modify messages without being able to violate certain security premises guaranteed by a cryptosystem, the goal of Steganography is to hide messages inside other harmless messages in a way that does not allow any enemy to even detect that there is a second message present".

In a digital world, Steganography and Cryptography are both intended to protect information from unwanted parties. Both Steganography and Cryptography are excellent means by which to accomplish this but neither technology alone is perfect and both can be broken. It is for this reason that most experts would suggest using both to add multiple layers of security. While encryption technologies can be used to prevent unauthorized access to digital content, it is clear that encryption has its limitations in protecting intellectual property rights: once a content is decrypted, there's nothing to prevent an authorized user from illegally replicating digital content. Some other technology was obviously needed to help establish and prove ownership rights, track content usage, ensure authorized access, facilitate content authentication and prevent illegal replication. This need attracted attention from the research community and industry leading to a creation of a new information hiding form, called Digital Watermarking. Basic idea is to create a metadata containing information about a digital content to be protected, and hide it within that content. The information to hide, the metadata, can have different formats. For example, it may be formatted as a character string or a binary image pattern. The metadata is first mapped into its bit stream representation, and then into a watermark, a pattern of the same type and dimension as the cover work, the digital content to be protected. The watermark is then embedded into the cover work. The embedded watermark should be imperceptible, and it should be robust enough to survive not only most common signal distortions, but also distortions caused by malicious attacks.

Requirements and design of watermarking techniques are impacted by the different types of content in two major ways: imperceptibility and robustness requirements. The first challenge is designing a watermark embedding algorithm which provides an imperceptible mark, that is, one which does not noticeably degrade the original host signal. By taking advantage of psychovisual and psychoauditory properties, we can design effective watermarking schemes which remain transparent under particular conditions. Ideally, the marking algorithm should be adapted by using perceptual models appropriate for the different media types. The perceptual models used for representations of continuous tone images are not appropriate for text or graphics. The other factor for designing watermarking schemes for multimedia is the type of degradations that the watermark is expected to survive and system requirements for media specific applications. For instance, it may be desirable for a still image watermarking technique to be able to survive JPEG compression and photocopying while for some video watermarking applications, it may be important to do watermark embedding and detection in real time on a compressed bit stream. In the next section we describe watermarking for different media types including an overview of some sample algorithms proposed in the literature. This is followed by a description of a general framework for watermark embedding and watermark detection and decoding, outlining some of the differences for different applications. We then review some work on modeling the general watermarking problem and drawing parallels to communication and information theory to help understand the fundamental properties and limitations of a watermarking system. This work is very useful for future algorithm design and helping to define open areas of research. Lastly, we review and summarize future directions in this new and exciting area.

WATERMARK

A watermark is a recognizable image or pattern in paper that appears as various shades of lightness/darkness when viewed by transmitted light (or when viewed by reflected light, at a dark background), caused by thickness or density variations in the paper. Encoding an identifying code into digitized music, video, image or other file is known as a digital watermark. Digital watermarking technique is thus implementing the concept of watermarking in digital media.

DIGITAL WATERMARKING

The term "digital watermark" was first coined in 1992 by Andrew Tirkel and Charles Osborne [2]. Actually, the term used by Tirkel and Osborne was originally used in Japan--from the Japanese--"denshi sukashi" --literally, an "electronic watermark"[3]. Each watermarking application has its own specific requirements. Some of the general requirements are outlined here:

Perceptual transparency: the watermarking algorithm must embed the watermark such that this does not affect the quality of the host data. A watermark-embedding procedure is truly imperceptible if humans cannot distinguish the original data from the data with the inserted watermark. 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.

Watermarking load: The amount of information that can be stored in a watermark depends on the application. The information should be embedded such that the pixel value of image does not leave the base value of the pixel.

Robustness: There should be no way in which the watermark can be removed or altered without sufficient degradation of the perceptual quality of the host data. If a watermark is used for another application, it is desirable that the watermark always remains in the host data, even if the quality of the host data is degraded, intentionally or unintentionally.

Security: A watermarking technique is secure if knowing the exact algorithms for embedding and extracting the watermark does not help an unauthorized party to detect the presence of the watermark.

The figure shows a general watermarking approach. Fig1. shows the watermark transmission. In this phase, the watermark W is generated as a pseudo-random sequence to ensure statistical invisibility. Signal information, such as DCT coefficients are extracted from the original image I and embedded into the information to form the watermarked image J. In the watermark detection phase as shows in fig.2, a suspected image S is taken as input for obtaining its signal information. A suspected watermark W_S is extracted based on knowledge of the original image I and the watermark W. A similarity measure M is calculated based on the values of W_S and W, which is then compared with a threshold value. If the value of M is larger than the threshold value, then the watermark is detected.

Blind detection scheme. Non-blind detection needs the original host signal, which is very inconvenient to use the original data, because of the huge video data. Blind detection does not need the original host image.

High real-time: Three-dimensional video signal has more the amount of data than the image does. So calculation quality is larger and embedding /detection needs more times. The procession of embedding, using video compression standard for these specific structures such as motion vector coding.

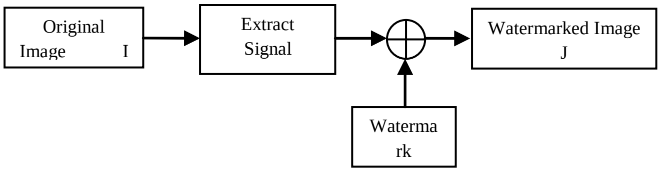

Figure 1 Watermark Transmission

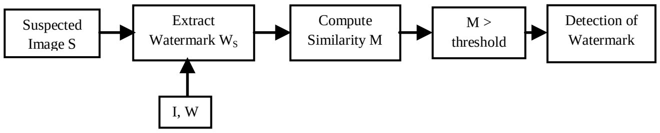

Figure 2 Watermark Detection

Random detection: The watermark is detected in any position of the video rather than the position according to the video playback order to detect the watermark.

II. DIGITAL IMAGE WATERMARKING SCHEMES

Digital watermarking is the process of embedding information into a digital signal which may be used to verify its authenticity or the identity of its owners, in the same manner as paper bearing a watermark for visible identification. In digital watermarking, the signal may be audio, pictures, or video. If the signal is copied, then the information also is carried in the copy (Yeung, Yeo, & Holliman, 1998). The concept of digital watermarking is associated with steganography. Steganography is defined as covered writing. It has a long history of being associated with methods of secret communication. Steganography does not immediately arise the suspicion of something secret or valuable.

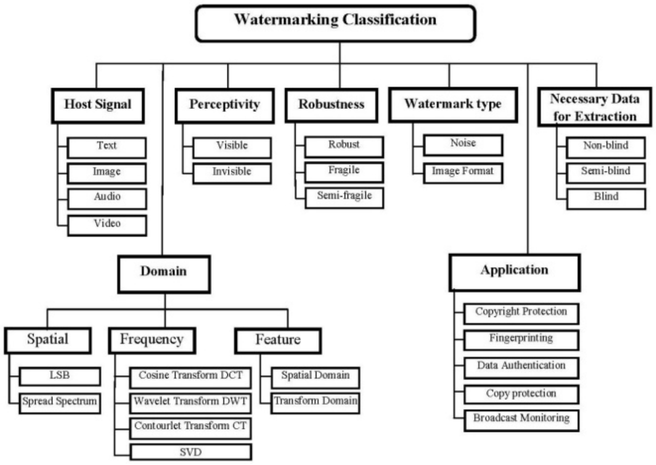

Figure 3: Classification of watermarking techniques

Instead, it hides an important message in an unimportant one. Therefore, digital watermarking is a way to hide a secret or personal message to protect a product's copyright or to demonstrate data integrity (Voyatzis & Pitas, 1999). In visible digital watermarking, the information is visible in the picture or video. Typically, the information is text or a logo, which identifies the owner of the media. The image on the right has a visible watermark. When a television broadcaster adds its logo to the corner of transmitted video, this also is a visible watermark.

The most important properties of any digital watermarking techniques are robustness, security, imperceptibility, complexity, and verification. Robustness is defined as if the watermark can be detected after media (normal) operations such as filtering, lossy compression, color correction, or geometric modifications. Security means the embedded watermark cannot be removed beyond reliable detection by targeted attacks. Imperceptibility means the watermark is not seen by the human visual system. Complexity is described as the effort and time required for watermark embedding and retrieval. Lastly, verification is a procedure whereby there is a private key or public key function (Dittmann, Mukherjee, & Steinebach, 2000). Each of these properties must be taken into consideration when applying a certain digital watermarking technique. The following sections describe a few of the most common digital watermarking techniques.

2.1. Spatial and Frequency Domain

Spatial and frequency domain watermarking are applied to graphic images and text. Spatial domain watermarking slightly modifies the pixels of one or two randomly selected subsets of an image. Modifications might include flipping the low-order bit of each pixel. However, this technique is not reliable when subjected to normal media operations such as filtering or lossy compression (Berghel, 1998). Frequency domain watermarking technique is also called transform domain. Values of certain frequencies are altered from their original. Typically, these frequency alterations are done in the lower frequency levels, since alternations at the higher frequencies are lost during compression. The watermark is applied to the whole image so as not to be removed during a cropping operation. However, there is a tradeoff with the frequency domain technique. Verification can be difficult since this watermark is applied indiscriminately across the whole image (Berghel, 1998).

Table 1: Comparison between watermarking schemes

Characteristics	**Spatial Domain**	**Transform Domain**
Computation Cost	Low	High
Robustness	Fragile	Robust
Perceptual quality	High Control	Low Control
Capacity	High(depends on image size)	Low
Application	Authentication	Copyright

2.2 Attacks

Digital watermarking does not have the same capability or level of security as data encryption. It does not prevent the viewing or listening of content, nor does it prevent accessing that content. Therefore, digital watermarking is not immune to hacker attacks (Yeung et al., 1998). The following are some intentional attacks on watermarks (Cox, Miller, & Bloom, 2000).

- Removal attacks This type of watermark attack does not attempt to find out the encryption techniques used or how the watermark has been embedded. Included in this category noising, histogram equalization, blur and sharpen attacks.

- Geometry attacks this type of attack intends to distort the watermark signal. It is however still theoretically possible for the detector to recover the original watermark if the detail of the geometry attack can be established and a countermeasure applied. The process of correcting this type of attack is often referred to as synchronization. However, the complexity of the required synchronization process might be too prohibitively expensive and slow. Included in this category of watermark attacks are image rotation, scaling, translation and skewing.

- The aim of cryptographic attacks is to crack the security methods in watermarking schemes and thus find a way to remove the embedded watermark information or to embed misleading watermarks. One of the techniques in this category is the brute-force search method.

- Another technique is called the Oracle attack, which is used to create a non-watermarked signal when a watermark detector device is available.

- Protocol attacks it add the attacker’s own watermark signals onto the data in question. This results in ambiguities on the true owners question. Protocol attacks target the entire concept of using watermarking techniques as a solution to copyright protection. Another protocol attack is the copy attack: instead of destroying the watermark, the copy attack estimates a watermark from watermarked data and copies.

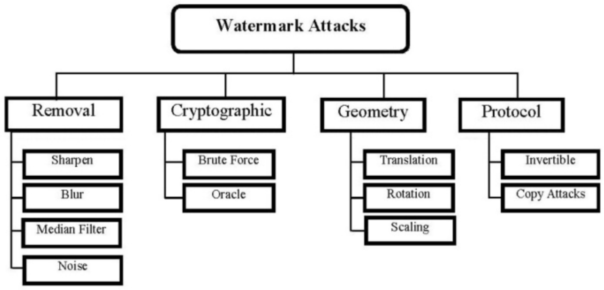

Figure 4: Classification of watermark attacks

2.3. Choice of Watermark-Object

The first question we need to ask with any watermarking or stenographic system, is what form will the embedded message take? The most straightforward approach would be to embed text strings into an image, allowing an image to directly carry information such as author, title, date…and so forth. The drawback however to this approach is that ASCII text in a way can be considered to be a form of LZW compression, which each letter being represented with a certain pattern of bits. By compressing the watermark-object before insertion, robustness suffers.

Due to the nature of ASCII codes, a single bit error due to an attack can entirely change the meaning of that character, and thus the message. It would be quite easy for even a simple task such as JPEG compression to reduce a copyright string to a random collection of characters. Rather then characters, why not embed the information in an already highly redundant form, such as a raster image? Not only do images lend themselves to image watermarking applications, but the properties of the HVS can easily be exploited in recognition of a degraded watermark.

There are different watermarks are used, based on the theoretical and experimental information capacity of the watermarking algorithm.

2.4. Purpose of Digital Watermarking

Watermarks added to digital content serve a variety of purposes. The following list details six purposes of digital watermarking (Memon & Wong, 1998).

- Ownership Assertion – to establish ownership of the content (i.e. image)

- Fingerprinting – to avoid unauthorized duplication and distribution of publicly available multimedia content

- Authentication and integrity verification – the authenticator is inseparably bound to the content whereby the author has a unique key associated with the content and can verify integrity of that content by extracting the watermark

- Content labeling – bits embedded into the data that gives further information about the content such as a graphic image with time and place information

- Usage control – added to limit the number of copies created whereas the watermarks are modified by the hardware and at some point would not create any more copies (i.e. DVD)

- Content protection – content stamped with a visible watermark that is very difficult to remove so that it can be publicly and freely distributed.Unfortunately, there is not an universal watermarking technique to satisfy all of these purposes (Memon & Wong, 1998). The content in the environment that it will be used determines the digital watermarking technique.

III. LITERATURE REVIEW

The idea of watermarking can be dated back to the late Middle Ages. The earliest use has been to record the manufacture’s trademark on the product so that authenticity could be easily established. The term "digital watermark" was first coined in 1992 by Andrew Tirkel and Charles Osborne [2]. Actually, the term used by Tirkel and Osborne was originally used in Japan--from the Japanese--"denshi sukashi" --literally, an "electronic watermark"[2]. A.Z.Tirkel et al. [1995] discuss the feasibility of coding a robust, undetectable, digital watermark on a standard 512*512 intensity image with an 8 bit gray scale image [3].

The watermark is capable of carrying such information as authentication or authorisation codes, or a legend essential for image interpretation. J.J.K. O Ruanaidh et al. [1995] discuss the watermarking digital images for copyright protection. They have demonstatrated a solution to one of the key problems in image watermarking, namely how to hide robust invisible labels inside grey scale or colour digital images [4]. Jian Zhao [1996] describes a digital watermarking service which allows the publisher and information provider to mark and identify their copyrighted materials through the World Wide Web (WWW) [5]. J.J.K. O Ruanaidh et al. [1997] describes an invisible mark embedded in a digital image which may be used for Copyright protection. The embedded marks are designed to be unaffected by any combination of rotation, scale and translation transformations. The original image is not required for extracting the embedded mark [6].

Jian Zhao et al. [1998] describe digital watermark for copyright protection, digital watermark for hidden annotation, digital watermark for proving authenticity, steganographic communication, functions and technical requirements [7]. M. Barni et al. [1998] derived a new watermarking algorithm for digital images is presented the method, which operates in the frequency domain, embeds a pseudo-random sequence of real numbers in a selected set of DCT coefficients. After embedding, the watermark is adapted to the image by exploiting the masking characteristics of the human visual system, thus ensuring the watermark invisibility [8].

Nasir Memon et al. [1998] describe protecting digital media content and Watermark insertion integrates the input image and a watermark to form the output watermarked image. Watermark extraction uncovers the watermark in watermarked images, a technique usually applicable in verification watermarks [9]. Saraju Prasad Mohanty[1999] describe the four algorithms appear under the following headings in his thesis: An Adaptive Visible Watermarking for Image Data in DCT Domain. An Invisible Image Watermarking Technique in Spatial Domain.

A Spread Spectrum Watermarking Technique for Digital Images. The thesis concludes with a discussion of the advantages and disadvantages of the techniques proposed and the future directions of research [10].

Juan R. Hernandez et al. [1999] addresses the problem of the performance analysis of image watermarking systems that do not require the availability of the original image during ownership verification. They focus on a statistical approach to obtain models that can serve as a basis for the application of the decision theory to the design of efficient detector structures. Special attention is paid to the possible nonexistence of a statistical description of the original image [11]. Ingemar J. Cox et al. [2000] describe a number of applications of digital watermarking and they examine the common properties of robustness, tamper resistance, fidelity, computational cost and false positive rate. They observe that these properties vary greatly depending on the application. Consequently, they conclude that evaluation of a watermarking algorithm is difficult without first indicating the context in which it is to be applied [12]. Ching-Yung Lin et al. [2000], in this thesis, they first propose robust digital signature methods that have proved to be useful for such types of content authentication. Also, they have developed a novel semi-fragile watermarking technique to embed the proposed robust digital signatures. They have implemented a unique Self-Authentication-and-Recovery Images (SARI) system, which can accept quantization-based lossy compression to a determined degree without any false alarms and can sensitively detect and locate malicious manipulations [13]. Chun-Shien Lu et al. [2001] they propose a novel multipurpose watermarking scheme, in which robust and fragile watermarks are simultaneously embedded, for copyright protection and content authentication. By quantizing a host image's wavelet coefficients as masking threshold units (MTUs), two complementary watermarks are embedded using cocktail watermarking and they can be blindly extracted without access to the host image. For the purpose of image protection, the new scheme guarantees that, no matter what kind of attack is encountered, at least one watermark can survive well. On the other hand, for the purpose of image authentication, our approach can locate the part of the image that has been tampered with and tolerate some incidental processes that have been executed [14].

Minya Chen et al. [2001], in this paper, they present an overview and summary of recent developments on this important topic, and discuss important issues such as robustness and data hiding capacity of the different techniques [15]. P.Tay et al. [2002], in this paper they propose a novel image watermarking scheme. This technique uses a 2-D discrete wavelet transform to decompose an image into various frequency channels. A scaled image is used as watermark and inserted into a mid-frequency wavelet channel. The watermark embedded image is produced by taking the inverse 2D discrete wavelet transform of the altered wavelet decomposition. The image size, the non-zero scaling factor, the channel in which the watermark is inserted, and the wavelet transform filters can be used as security keys for the extraction of the inserted watermark. The propose watermark extraction technique is independent of the original image [16]. Bilge Gunsel et al. [2002], in this paper they introduce two spatial methods in order to embed watermark data into fingerprint images, without corrupting their features. The first method inserts watermark data after feature extraction, thus preventing watermarking of regions used for fingerprint classification. The method utilizes an image adaptive strength adjustment technique which results in watermarks with low visibility. The second method introduces a feature adaptive watermarking technique for fingerprints, thus applicable before feature extraction. For both of the methods, decoding does not require original fingerprint image. Unlike most of the published spatial watermarking methods, the proposed methods provide high decoding accuracy for fingerprint images. High data hiding and decoding performance for color images is also observed [17].

Vassilis E. Fotopoulos et al. [2003], derives copyright protection is a very important subject but not the only one in which watermarking appears as one of the very promising solutions. In this communication, they have attempted to go back to the early beginning of this exciting new research field, make an overview of its history, discuss the applications and stakes involved, classify the proposed methods, present the problems and benchmarking tools and finally, try to peak into the future [18]. Saraju P. Mohanty et al. [2003], in this paper, they develop hardware system that can insert both robust and fragile invisible watermarks in images. The hardware module can be easily incorporated into a JPEG encoder to develop a secure JPEG encoder. A prototype chip is implemented using 0.35µ CMOS technology. According to them, this is the first watermarking chip implementing both invisible-robust and invisible-fragile watermarking capabilities [19]. Chang-Chou Lin et al. [2004], they work a novel approach to secret image sharing based on a ok; nP-threshold scheme with the additional capabilities of steganography and authentication is proposed [20].

Vidyasagar M. Potdar et al. [2005] present a detailed survey of existing and newly proposed steganographic and watermarking techniques [21]. G. Coatrieux et al. [2006] focus on the complementary role of watermarking with respect to medical information security and management [22]. Benoit Macq et al. [2007] discuss the issues related to image watermarking benchmarking and scenarios based on digital rights management requirements [23]. A new robust digital image watermarking algorithm based on Joint DWT-DCT Transformation is proposed by Saeed K. Amirgholipour et al. [2008] [24]. Two modified image adaptive watermarking techniques based on multi-scale morphological segmentation are presented by B. S. Anami et al. [2011] [25]. M. Kaur et al. [2012] aim to present a survey on different types of digital watermarks and methods to do image watermarking [26].

The main reason for development of digital watermarking research is the endeavor for coming up with innovations to protect intellectual properties of the digital world. This is because the recent technological advancement in generation, storage, and communication of digital content has created/generated problems like copying the digital contents without any constraints, forgery, and editing without any prohibitive professional efforts. The absence of protecting techniques makes it doubtful to use the digital communication system in medical, business, and military applications. Watermarking is one of the most common solutions to make the data transferring secure from the illegal interference.

IV. IMAGE QUALITY METRICS

To measure the amount of visual quality degradation between original and watermarked images different types of image quality metrics are used.

4.1 Peak Signal-to-Noise Ratio (PSNR)

It is the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of its representation. PSNR is usually expressed in terms of dB for wide range signals The PSNR is most commonly used as a measure of quality of reconstruction of lossy compression. The cover image in this case is the original data, and the information logo is the error introduced by watermarking. When comparing deformed image with the original one an approximation to human perception of reconstruction quality is made, therefore in some cases one reconstruction may appear to be closer to the original than another, even though it has a lower PSNR. So a higher PSNR would normally indicate that the reconstruction is of higher quality.

It is most easily defined via the mean square error (MSE) which is for two m x n monochrome images I and K where one of the images is considered a noisy approximation of the other and is defined as:

$$MSE = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j) - K(i,j)]^2$$

The PSNR is defined as:

$$PSNR = 10.log_{10}\left(\frac{MAX_I^2}{MSE}\right)$$

$$PSNR = 20.log_{10}\left(\frac{MAX_I}{\sqrt{MSE}}\right)$$

Here, MAX_I is the maximum possible pixel value of the image. When the pixels are represented using 8 bits per sample, this is 255.

4.2 Structural Similarity Index Measure (SSIM)

It is a method for measuring the similarity between two images. The SSIM index is a full reference metric, in other words, the measuring of image quality based on an initial distortion-free image as reference. SSIM is designed to improve on traditional methods like PSNR and MSE which have proved to be inconsistent with human eye perception. The resultant SSIM index is a decimal value between -1 and 1, and value 1 is only reachable in the case of two identical sets of data. The SSIM metric is calculated on various windows of an image. The measure between two windows x and y of common size N×N is:

$$SSIM(x,y) = \frac{\left(2\mu_x\mu_y + c_1\right)\left(2\sigma_{xy} + c_2\right)}{\left(\mu_x^2 + \mu_y^2 + c_1\right)\left(\sigma_x^2 + \sigma_y^2 + c_2\right)}$$

Where μ_x the average of x; μ_y the average of y; σ_x^2 the variance of x; σ_y^2 the variance of y;

σ_{xy} the covariance of x and y;

$C_1=(k_1L)^2$, $c_2=(k_2L)^2$ two variables to stabilize the division with weak denominator;

L the dynamic range of the pixel-values (typically this is $2^{\#\text{bits per pixel}} - 1$);

$k_1=0.01$ and $k_2=0.03$ by default.

V. APPLICATIONS OF DIGITAL WATERMARKING

One application of watermarking is in copyright protection systems, which are intended to prevent or deter unauthorized copying of digital media. In this use, a copy device retrieves the watermark from the signal before making a copy; the device makes a decision whether to copy or not, depending on the contents of the watermark. Another application is in source tracing. A watermark is embedded into a digital signal at each point of distribution. If a copy of the work is found later, then the watermark may be retrieved from the copy and the source of the distribution is known. This technique reportedly has been used to detect the source of illegally copied movies. Annotation of digital photographs with descriptive information is another application of invisible watermarking.

Digital watermarking may be used for a wide range of applications, such as:

5.1. Copyright Protection:

When a new work is produced, copyright information can be inserted as a watermark. In case of dispute of ownership, this watermark can provide evidence.

5.2. Broadcast Monitoring:

This application is used to monitor unauthorized broadcast station. It can verify whether the content is really broadcasted or not.

5.3. Tamper Detection:

Fragile watermarks are used for tamper detection. If the watermark is destroyed or degraded, it indicates presence of tampering and hence digital content cannot be trusted.

5.4. Authentication and Integrity Verification:

Content authentication is able to detect any change in digital content. This can be achieved through the use of fragile or semi-fragile watermark which has low robustness to modification in an image.

5.5. Fingerprinting:

Fingerprints are unique to the owner of digital content and used to tell when an illegal copy appeared.

5.6. Content Description:

This watermark can contain some detailed information of the host image such as labelling and captioning. For this kind of application, capacity of watermark should be relatively large and there is no strict requirement of robustness.

5.7. Covert Communication:

It includes exchange of messages secretly embedded within images. In this case, the main requirement is that hidden data should not raise any suspicion that a secret message is being communicated.

VI. CONCLUSION

In this paper we presented digital watermarking overview, application, attacks and techniques. We classified the previous researches from various point of views such as: host signal, perceptivity, robustness, watermark type, necessary data for extraction, processing domain, and applications. In this review paper, an attempt has been made to study the Digital Image Watermarking Techniques and its applications in digital image processing. Some of the applications of Image Watermarking are described. The review was conducted to study the different suitable areas of Digital Image Watermarking and its applications in digital image processing.

REFERENCES

[1] Chen Li, Cheng Yang, Wei Li, Wavelet Bases and Decomposition Series in the Digital Image Watermarking. Advances in Intelligent and Soft Computing, Advances in Multimedia, Software Engineering and Computing Vol.2 , s.l. : Springer, 2012, Vol. 129/2012.

[2] A.Z.Tirkel, G.A. Rankin, R.M. Van Schyndel, W.J.Ho, N.R.A.Mee, C.F.Osborne. "Electronic Water Mark". DICTA 93, Macquarie University. p.666-673

[3] A.Z.Tirkel, R.G.van Schyndel, C.F.Osborne, A TWO-DIMENSIONAL DIGITAL WATERMARK, DICTA 95, Macquarie University.

[4] Jian Zhao, A WWW SERVICE TO EMBED AND PROVE DIGITAL COPYRIGHT WATERMARKS, In: Proc. of the European Conference on Multimedia Applications, Services and techniques, Louvain-La-Neuve, Belgium, May 1996.

[5] J.J.K. O Ruanaidh,W.J. Dowling, F.M. Boland,Watermarking Digital Images for Copyright Protection, IEEE, 1995.

[6] Joseph J.K. O Runaidh and Thierry Pun, Rotation.Scale and Translation Invarient Digital Image Watermarking,Submitted to Signal Processing,21 August 1997.

[7] Jian Zhao, Eckhard Koch, and Chenghui Luo, In Business Today and Tomorrow, COMMUNICATIONS OF THE ACM July 1998/Vol. 41, No. 7.

[8] Mauro Barni, Franco Bartolini, Vito Cappellini, and Alessandro Piva, A DCT-domain system for robust image watermarking,. Signal Processing 66 (1998) p.357-372.

[9] Nasir Memon and Ping Wah Wong, Protecting Digital MediaContent,COMMUNICATIONS OF THE ACM July 1998/Vol. 41, No. 7.

[10] Saraju Prasad Mohanty, A Project Report Submitted in Partial Fulfillment of the Requirement for the degree of Master of Engineering In System Science and Automation, Department of Electrical Engineering INDIAN INSTITUE OF SCIENCE, JANUARY, 1999.

[11] JUAN R. HERNANDEZ, AND FERNANDO PEREZ-GONZA LEZ, Statistical Analysis of Watermarking Schemes for Copyright Protection of Images, PROCEEDINGS OF THE IEEE, VOL. 87, NO. 7, JULY 1999.

[12] Ingemar J. Cox, Matt L. Miller and Jeffrey A. Bloom, Watermarking applications and their properties, the proceedings of the International Conference on Information Technology: Coding and Computing, ITCC 2000, March 27-29, 2000, Las Vegas, Nevada.

[13] Ching-Yung Lin, Watermarking and Digital Signature Techniques for Multimedia Authentication and Copyright Protection, Submitted in partial fulfillment of the requirements for the degree of Doctor of Philosophy in the Graduate School of Arts and Sciences Columbia University, 2000.

[14] Chun-Shien Lu and Hong-Yuan Mark Liao, MultipurposeWatermarking for Image Authentication and Protection, IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 10, NO. 10, p.1579-1592, OCTOBER 2001.

[15] Minya Chen, Edward K. Wong, Nasir Memon and Scott Adams, Recent Developments in Document Image Watermarking and Data Hiding, Department of Computer and Information Science Polytechnic University 5 Metrotech Center,Brooklyn, NY 11201, 2001.

[16] P.Tay and J.P. Havlicek, Image Watermarking Using Wavelets,Copyright@IEEE,2002.

[17] Bilge Gunsel, Umut Uludag, A. Murat Tekalp, Robust watermarking of "fingerprint images, 00313203/02/$22.00 2002 Pattern Recognition Society. Published by Elsevier Science Ltd. All rights reserved. PII: S0031-3203(01)00250-3,2002.

[18] Vassilis E. Fotopoulos and Athanassios N. Skodras, Digital Image Watermarking: An Overview, European Association for Signal, Speech, and Image Processing, ISSN 1687-1421, Volume 14, Number 4, December 2003.

[19] Saraju P. Mohanty, N. Ranganathan and Ravi K. Namballa, VLSI IMPLEMENTATION OF INVISIBLE DIGITAL WATERMARKING ALGORITHMS TOWARDS THE DEVELOPMENT OF A SECURE JPEG ENCODER,2003.

[20] Chang-Chou Lin, Wen-Hsiang Tsai, Secret image sharing with steganography and authentication, The Journal of Systems and Software 73 (2004) 405–414.

[21] Vidyasagar M. Potdar, Song Han, Elizabeth Chang, A Survey of Digital Image Watermarking Techniques, 3rd International Conference on Industrial Informatics(INDIN 2005) ©2005 IEEE.

[22] G. Coatrieux, L. Lecornu, Ch. Roux, B. Sankur, A Review of Image Watermarking Applications in Healthcare,2006.

[23] BENOIT MACQ, JANA DITTMANN, AND EDWARD J. DELP, Benchmarking of Image Watermarking Algorithms for Digital Rights Management, PROCEEDINGS OF THE IEEE, VOL. 92, NO. 6, JUNE 2007 971.

[24] Saeed K. Amirgholipour ,Ahmad R. Naghsh-Nilchi, Robust Digital Image Watermarking Based on Joint DWT-DCT, International Journal of Digital Content Technology and its Applications,Volume 3, Number 2, June 2009.

[25] Basavaraj. S. Anami, J.D.Pujari, Rajesh. Yakkundimath, Multi-Scale Morphological Image Segmentation Based Modified Watermarking Techniques,International Journal of Graphics & Image Processing, Vol1 issue 1 August 2011.