ISSN: 2321-7782 (Online)
Volume 2, Issue 12, December 2014
International Journal of Advance Research in Computer Science and Management Studies
Research Article / Survey Paper / Case Study
Available online at: www.ijarcsms.com

Data Authentication using Digital Watermarking

Sunanda Datta[1]
Department of Computer Science
St. Xavier's College(Autonomous)
Kolkata, India

Dr. Asoke Nath[2]
Department of Computer Science
St. Xavier's College(Autonomous)
Kolkata, India

Abstract: ***With the widespread use of networks, intellectual properties can be obtained and reproduced easily. The ease of reproduction, distribution, and manipulation of digital documents creates problems for authorized parties that wish to prevent illegal use of such document. To this end, digital watermarking has been proposed as a last line of defence. A digital watermark is an imperceptible, robust, secure message embedded directly into a document. The watermark is imperceptible both perceptually and statistically. Current watermarking schemes may be viewed as spread-spectrum communications systems, which transmit a message redundantly using a low-amplitude, pseudonoise carrier signal. This paper incorporate the detail study of watermarking definition, concept and the main contributions in this field such as categories of watermarking process that tell which watermarking method should be used. This paper incorporate the detail study of watermarking definition, concept and the main contributions in this field such as categories of watermarking process that tells which watermarking method should be used. It starts with overview, classification, features, framework, techniques, application, challenges, limitations and performance metric of watermarking and a comparative analysis of some watermarking techniques. In the present work the authors have made main focus on image only.***

Keywords: digital documents; digital watermarking; secure message; carrier signal; pseudo-noise

I. INTRODUCTION

The term 'digital watermarking' first appeared in 1993, when Tirkel presented two watermarking techniques to hide the watermark data in the images. The success of the Internet, cost-effective and popular digital recording and storage devices, and the promise of higher bandwidth and quality of service for both wired and wireless networks have made it possible to create, replicate, transmit, and distribute digital content in an effortless way. The growth of e-commerce applications in the World Wide Web also requires the need to increase the security of data communications over the internet. To provide security to these applications and the protection and enforcement of intellectual property rights for digital media, data encryption and information hiding techniques were introduced & developed. Digital watermarking is a technology that provides and ensures security, data authentication and copyright protection to the digital media. Digital Watermarking is the process of embedding data called a watermark (also known as Digital Signature or Tag or Label) into the digital media (such as text, image, audio and video) such that watermark can be detected or extracted later to make an assertion about the object. A digital watermarking system embeds information *directly into a document*. For example, information about copyrights, ownership, timestamps, and the legitimate receiver could be embedded. Digital watermarking cannot by itself prevent copying, modification, and re-distribution of documents. However, if encryption and copy protection fail, watermarking allows the document to be traced back to its rightful owner and to the point of unauthorized use. Digital watermarking requires elements from many disciplines, including signal processing, telecommunications, cryptography, psychophysics, and law. Watermarking is used for Proof of Ownership (copyrights and IP protection), Copying Prevention, Broadcast Monitoring, Authentication and Data Hiding.

Fig.1 Example of watermark on Indian currency

II. WHAT IS DIGITAL WATERMARKING ?

Simple Digital watermarking is a technology in which a watermark (secret information) is hidden in the digital media using an appropriate algorithm for the authentication and identification of original owner of the product. The outcome of this is the watermarked image.

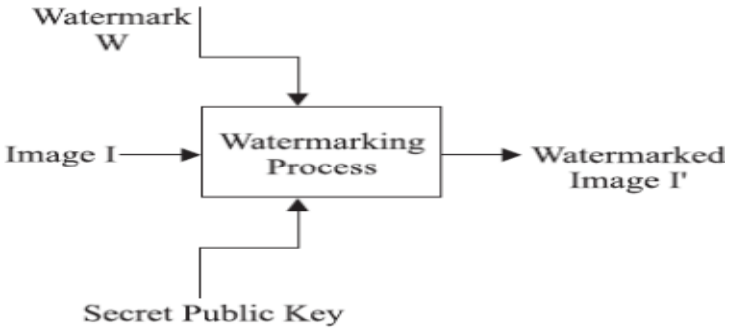

Fig.2 Simple Digital Watermarking

A complete digital watermarking system is composed of two basic modules: watermark embedding module and watermark detection and extraction module.

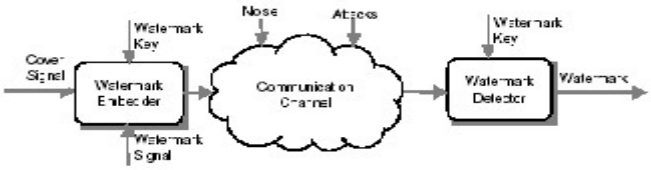

Fig.3 General Watermarking System

Watermark embedding module is responsible for adding the watermark signal to the original data. The watermark can be any form of data, such as numeric, text, image, and so on. Key can be used to strengthen security to prevent unauthorized parties restore and modify the watermark. The watermark embedding module is shown in the following figure:

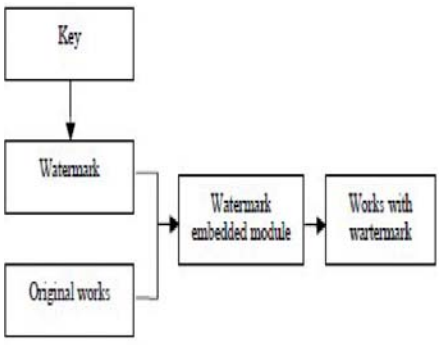

Fig.4 Watermark Embedding Module

Watermark detection and extraction module is used to determine whether the data contains specified watermark or the watermark can be extracted. The module input may be image, key, watermark or original image, the output is a watermark or some kind of credibility value. It indicates the possibility of the data having a given watermark. The watermark embedding module is shown in the following figure:

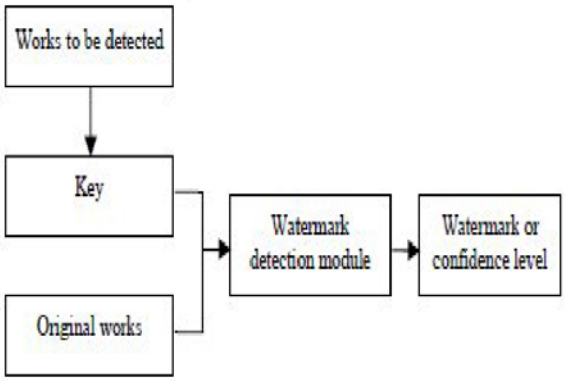

Fig.5 Watermark Detection and Extraction Module

a) Properties

An effective watermark should have several properties which are listed below, whose importance will vary depending upon the application.

1. Robustness

The watermark should be reliably detectable after alterations to the marked document. Robustness means that it must be difficult (ideally impossible) to defeat a watermark without degrading the marked document severely—so severely that the document is no longer useful or has no (commercial) value.

2. Imperceptibility or a low degree of obtrusiveness

To preserve the quality of the marked document, the watermark should not noticeably distort the original document. Ideally, the original and marked documents should be perceptually identical.

3. Security

Unauthorized parties should not be able to read or alter the watermark. Ideally, the watermark should not even be detectable by unauthorized parties.

4. Fast embedding and/or retrieval

The speed of a watermark embedding algorithm is important for applications where documents are marked "on-the-fly" (i.e., when they are distributed). The large bandwidth necessary for video also requires fast embedding methods. However, since ownership disputes will likely take weeks or months to resolve, a watermark recovery algorithm may emphasize reliable detection over speed.

5. No reference to original document

For some applications, it is necessary to recover the watermark without requiring the original, unmarked document (which would otherwise be stored in a secure archive).

6. Multiple watermarks

It may also be desirable to embed multiple watermarks in a document. For example, an image might be marked with a unique watermark each time it is downloaded.

7. Unambiguity

A watermark must convey unambiguous information about the rightful owner of a copyright, point of distribution, etc.This requirement is a cryptographic and protocol issue and not covered in this paper.

Of these properties, robustness, imperceptibility, and security are usually the most important. When speaking of robustness, we often talk about *attacks* on a watermark. An attack is an operation on the marked document that, intentionally or not, may degrade the watermark and make the watermark harder to detect. For text documents, an attack might consist of photocopying. For images and video, compression(e.g., JPEG or MPEG), filtering, cropping, resizing, and other signal processing manipulations (even printing and rescanning) must not destroy the watermark.

b) Comparison With Different Data Hiding Techniques

1. Watermarking and Steganography

The information hidden by a watermarking system is always associated to the digital object to be protected or to its owner while steganographic systems just hide any information. "Robustness" criteria are also different,since steganography is mainly concerned with detection of the hidden message while watermarking concerns potential removal of a pirate Steganographic communications are usually point-to- point (between sender and receiver) while watermarking techniques are usually one-to-many.

2. Watermarking and Cryptography

In cryptography two keys are used for encryption and detection while in watermarking information is added in data for security. In cryptography keys are needed for detection but watermarking does not need any key.

3. Watermarking and Fingerprinting

In watermarking modifications of contents are done by adding identification data while in fingerprinting contents are not affected. Watermarking allow the precise identification of each piece of content and fingerprinting work for legacy content Watermarking is stand alone and in finger printing connection to database is required.

c) Classification

Digital watermarking techniques are classified into various types. This classification is based on several criteria. All the classifications are described in following table:

Table. I Types of watermarking basis of different Criteria

S.no	Criteria	Classification
1.	Watermark Type	1. Noise: pseudo noise, Gaussian random and chaotic sequences 2. Image: Any logo, Stamp Image etc.
2.	Robustness	1. Fragile: Easily Manipulated 2. Semi-Fragile: Resist from some type of Attacks 3. Robust: not affected from attack

3.	Domain	1. Spatial: LSB, Spread Spectrum 2. Frequency: DWT, DCT, DFT, SVD
4.	Perceptivity	1. Visible Watermarking: Channel logo 2. Invisible Watermarking: like Steganography
5.	Host Data	1. Image Watermarking 2. Text Watermarking 3. Audio Watermarking 4. Video Watermarking
6.	Data Extraction	1. Blind 2. Semi-Blind 3. Non- Blind

III. WATERMARKING TECHNIQUES

Watermarking is the method used to hide the secret information into the digital media using some strong and appropriate algorithm. Algorithm plays a vital role in watermarking because if the used watermarking technique is efficient and strong then the watermark being embedded using that technique cannot be easily detected. The attacker can only destroy or detect the secret information if he know the algorithm otherwise it is critical to know the watermark. There are various algorithms present in today's scenario that are used to hide the information. Those algorithms come into two domains, Spatial and Frequency domain.

a) *Spatial domain:*

Spatial domain digital watermarking algorithms directly load the raw data into the original image. Spatial watermarking can also be applied using color separation. In this way, the watermark appears in only one of the color bands. This renders the watermark visibly subtle such that it is difficult to detect under regular viewing. Spatial domain is used in manipulating or changing an image representing an object in space to enhance the image for a given application. Techniques are based on direct manipulation of pixels in an image . Some of its algorithms are as discussed below:

1. Texture mapping coding Technique:

This method is useful in only those images which have some texture part in it. This method hides the watermark in the texture part of the image. This algorithm is only suitable for those areas with large number of arbitrary texture images (disadvantage), and cannot be done automatically. This method hides data within the continuous random texture patterns of a picture.

2. Patchwork Algorithm:

Patchwork is a data hiding technique developed by Bender et alii and published on IBM Systems Journal, 1996[11]. It is based on a pseudorandom, statistical model. Patchwork imperceptibly inserts a watermark with a particular statistic using a Gaussian distribution. A pseudo randomly selection of two patches is carried out where the first one is A and the second is B. Patch A image data is brightened where as that of patch B is darkened (for purposes of this illustration this is magnified). The following are the steps involved in the Patchwork algorithm:

» Generate a pseudo-random bit stream to select pairs of pixels from the cover data.

» For each pair, let d be the difference between the two pixels.

» Encode a bit of information into the pair. Let d < 0 represent 0 and d > 0represent that the given pixels are not ordered correctly, swap them.

» In the event that d is greater than a predefined threshold or if is equal to 0, ignore the pair and proceed to the next pair.

» Patchwork being statistical methods uses redundant pattern encoding to insert message within an image.

3. Correlation-Based Technique:

In this technique, a pseudorandom noise (PN) pattern say W(x, y) is added to cover image I(x, y). Iw(x, y) = I(x, y) + k*W(x, y) Where K represent the gain factor, Iw represent watermarked image at position x, y and I represent cover image. Here, if we increase the gain factor then although it increases the robustness of watermark but the quality of the watermarked image will decrease.

Proposed method:

Least Significant Bit: Old popular technique embeds the watermark in the LSB of pixels. This method is easy to implement and does not generate serious distortion to the image. The embedding of the watermark is performed choosing a subset of image pixels and substituting the least significant bit of each of the chosen pixels with watermark bits. The watermark may be spread throughout the image or may be spread in the selected locations of the image. The principle of embedding is fairly simple and effective. If we use a grayscale bitmap image, which is 8- bit, we would need to read in the file and then add data to the least significant bits of each pixel, in every 8-bit pixel. In a grayscale image each pixel is represented by 1 byte consist of 8 bits. It can represent 256 gray colors between the black which is 0 to the white which is 255. The principle of encoding uses the Least Significant Bit of each of these bytes, i.e. the bit on the far right side. If data is encoded to only the last two significant bits (which are the first and second LSB) of each color component it is most likely not going to be detectable; the human retina becomes the limiting factor in viewing pictures.

For the sake of this example only the least significant bit of each pixel will be used for embedding information. If the pixel value is 138 which is the value 10000110 in binary and the watermark bit is 1, the value of the pixel will be 10000111 in binary which is 139 in decimal. In this example we change the underline pixel.

WATERMARK EMBEDDED AND EXTRACTION

All images are 256*256 Pixels by 8 bit per pixel gray scale image. Select an image CI to be used as base image or cover image in which watermark will be inserted. Select an image to be used as watermark Reading images WI which will be added to base image.

n = no. of least significant bits to be utilized to hide most significant bits of watermark under the base image

Watermark Embedding

For each pixel in base, watermark, watermarked_image

Do

Base_image:set n least significant bits to zero

Watermark: shift right by 8-n bits

Watermarked-image: add values from base and watermark

End do

End

Watermark Extraction

In watermarked image for each pixel in watermarked image and extracted image

Do

Watermarked image: Shift left by 8-n bits

Extracted image: Set to the shifted value of watermarked image

Enddo

End

This technique is used to add an invisible and visible watermark in the image by varying the number of bits to be replaced in base image.

b) Frequency domain:

Spatial embedding inserts message into image pixels. The oldest and the most common used method in this category is the insertion of the watermark into the least significant bits (LSB) of pixel data [2][5][6]. The embedding process of the LSB technique can be illustrated as follows:Consider that the system is required to hide a watermark number 178 in a 2x2 gray-scale (8-bit) image. Let's assume that the image pixels are 234, 222, 190 and 34. In an 8-bit binary format the number 178 is represented as 10110010.Since there are 4 pixels that can be used to store this data we can easily decide to embed pairs of bits of the watermark to the last 2 insignificant bits of the pixels. The process therefore modifies the original bits from 11101010, 11011110, 10111110 and 00100010 to 11101010, 11011111, 10111100 and 00100010 respectively. In decimal representation the watermarked image has pixel values of 234, 223, 188 and 34. Since the modification of pixel values occurs in the LSB of the data, the effect to the cover image is often visually in different. This effect however becomes more apparent as more bits are used to hide the watermark. One of the major limitations in spatial domain is the capacity of an image to hold the watermark. In the case of LSB technique, this capacity can be increased by using more bits for the watermark embedding at a cost of higher detection rate. Improving this limitation seems to be one of the major drives in spatial domain research. So we use Frequency domain. Here **t**he aim is to embed the watermarks in the spectral coefficients of the image. The most commonly used transforms are the Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT), Discrete Wavelet Transform (DWT).The reason for watermarking in the frequency domain is that the characteristics of the human visual system (HVS) are better captured by the spectral coefficients. Some of its main algorithms are discussed below:

Proposed method:

Discrete cosine transforms (DCT): DCT represents data in terms of frequency space rather than an amplitude space. This is useful because that corresponds more to the way humans perceive light, so that the part that are not perceived can be identified and thrown away. DCT based watermarking techniques are robust compared to spatial domain techniques. Such algorithms are robust against simple image processing operations like low pass filtering, brightness and contrast adjustment, blurring etc. However, they are difficult to implement and are computationally more expensive. At the same time they are weak against geometric attacks like rotation, scaling, cropping etc. The transform domain watermarking techniques use a DCT to transform successive 8 X 8 pixel blocks of the image into 64 DCT coefficients each. The DCT coefficients F(u, v) of an 8 X 8 block of image pixels f(x, y) are given by

$$F[u,v] = 1/N^2 \sum_{m=0}^{N-1} \sum_{n=0}^{N-1} f[m,n] \cos[(2m+1)u\pi/2N] \cos[(2n+1)v\pi/2N]$$

Where f(x) = $1/\sqrt{2}$ where x equals to zero and f(x) is 1 otherwise

Embedding Process

1. Read the cover image and watermark.
2. Define block size = 8 and mid band for DCT.3.Generate PN sequence for Zero of length equal to number of mid band coefficients.
3. Divide the cover image into blocks of 8 X 8.
4. For each block,
    a. Find DCT.
    b. If (watermark bit = 0)
       Add one bit of the PN sequence for Zero to each mid band coefficient.
    c. Convert the block back to spatial domain.

Extraction Process

1. Read the cover image watermark.
2. Define block size = 8 and mid band for DCT.
3. Generate PN sequence for zero of length equal to number of mid band coefficients.
4. Divide the cover image into blocks of 8 X 8.
5. For each block,
    a. Find DCT.
    b. Extract the middle band coefficients.
    c. Find correlation between middle band coefficients and the PN sequence for zero.
    d. If correlation > threshold
       Set recovered watermark bit = 0.
       Else
       Set recovered watermark bit = 1.
    e. Reshape the recovered watermark according to the size of original watermark.

Other two methods in the frequency domain are:

a) *Discrete wavelet transforms (DWT):*

Wavelet Transform is a modern technique frequently used in digital image processing, compression, watermarking etc. The transforms are based on small waves, called wavelet, of varying frequency and limited duration. The wavelet transform decomposes the image into three spatial directions, i.e. horizontal, vertical and diagonal. Hence wavelets reflect the anisotropic properties of HVS more precisely. Magnitude of DWT coefficients is larger in the lowest bands (LL) at each level of decomposition and is smaller for other bands (HH, LH, and HL). The Discrete Wavelet Transform (DWT) is currently used in a wide variety of signal processing applications, such as in audio and video compression, removal of noise in audio, and the simulation of wireless antenna distribution. Wavelets have their energy concentrated in time and are well suited for the analysis of transient, time-varying signals. Since most of the real life signals encountered are time varying in nature, the Wavelet Transform suits many applications very well . One of the main challenges of the watermarking problem is to achieve a better tradeoff between robustness and perceptivity. Robustness can be achieved by increasing the strength of the embedded watermark, but the visible distortion would be increased as well. However, DWT is much preferred because it provides both a simultaneous spatial localization and a frequency spread of the watermark within the host image. The basic idea of discrete wavelet transform in image processing is to multi-differentiated decomposition of the image into sub-image of different spatial domain and independent frequencies.

Advantages of DWT over DCT: Wavelet transform understands the HVS more closely than the DCT. Wavelet coded image is a multi-resolution description of image. Hence an image can be shown at different levels of resolution and can be sequentially processed from low resolution to high resolution.

Disadvantages of DWT over DCT: Computational complexity of DWT is more compared to DCT. As Feig (1990) pointed out it only takes 54 multiplications to compute DCT for a block of 8x8, unlike wavelet calculation depends upon the length of the filter used, which is at least 1 multiplication per coefficient .

b) Discrete Fourier transform (DFT):

Transforms a continuous function into its frequency components. It has robustness against geometric attacks like rotation, scaling, cropping, translation etc. DFT shows translation invariance. Spatial shifts in the image affects the phase representation of the image but not the magnitude representation.Circular shifts in the spatial domain don't affect the magnitude of the Fourier transform.

Advantages of DFT over DWT and DCT: DFT is rotation, scaling and translation (RST) invariant. Hence it can be used to recover from geometric distortions, whereas the spatial domain, DCT and the DWT are not RST invariant and hence it is difficult to overcome from geometric distortions.

Table. II Comparisons of Different Watermarking Techniques

Algorithm	Advantages	Disadvantages
LSB	1. Easy to implement and understand 2. Low degradation of image quality 3. High perceptual transparency.	1. It lacks basic robustness 2. Vulnerable to noise 3. Vulnerable to cropping, scaling.
Correlation	1. Gain factor can be increased resulting in increased robustness	1. Image quality gets decreased due to very high increase in gain factor.
Patchwork	1. High level of robustness against most type of attacks	1. It can hide only a very small amount of information.
Texture mapping coding	1. This method hides data within the continuous random texture patterns of a picture.	1. This algorithm is only suitable for those areas with large number of arbitrary texture images.
DCT	1. The watermark is embedded into the coefficients of the middle frequency, so the visibility of image will not get affected and the watermark will not be removed by any kind of attack.	1. Block wise DCT destroys the invariance properties of the system. 2. Certain higher frequency components tend to be suppressed during the quantization step.
DWT	1. Allows good localization both in time and spatial frequency domain 2. Higher compression ratio which is relevant to human perception.	1. Cost of computing may be higher. 2. Longer compression time. 3. Noise/blur near edges of images or video frames.
DFT	1. DFT is rotation, scaling and translation (RST) invariant. Hence it can be used to recover from geometric distortions	1. Complex implementation 2. Cost of computing may be higher.

IV. APPLICATION OF WATERMARKING

In recent years the phenomenal growth of the internet has highlighted the need for the mechanism to protect ownership of digital media. Digital Watermarking is a technique that provides a solution to the longstanding problems faced with copyrighting digital data. Watermarking technologies is applied in every digital media where security and owner identification is needed. A few most common applications are listed hereby.

a) *Owner Identification*

The application of watermarking is developed is to identify the owner of any media. Some paper watermark is easily removed by some small exercise of attackers. So the digital watermark was introduced. In that the watermark is the internal part of digital media so that it cannot be easily detected and removed.

b) Copy Protection

Illegal copying is also prevent by watermarking with copy protect bit. This protection requires copying devices to be integrated with the watermark detecting circuitry.

c) *Broadcast Monitoring*

Broadcasting of TV channels and radio news is also monitoring by watermarking. It is generally done with the Paid media like sports broadcast or news broadcast.

d) Medical applications

Medical media and documents are also digitally verified, having the information of patient and the visiting doctors. These watermarks can be both visible and invisible. This watermarking helps doctors and medical applications to verify that the reports are not edited by illegal means.

e) Data Authentication

Authentication is the process of identify that the received content or data should be exact as it was sent. There should be no tampering done with it. So for that purpose sender embedded the digital watermark with the host data and it would be extracted at the receivers end and verified. Example are CRC (cyclic redundancy check) or parity check.

f) Tamper proofing

Digital watermarks which are fragile in nature, can be used for tamper proofing. Digital content can be embedded with fragile watermarks that get destroyed whenever any sort of modification is made to the content. Such watermarks can be used to authenticate the content.

g) Fingerprinting

Fingerprints are the characteristics of an object that tend to distinguish it from other small objects. As in the applications of copyright protection, the watermark for finger printing is used to trace authorized users who violate the license agreement and distribute the copyrighted material illegally. Thus, the information embedded in the content is usually about the customer such as customer's identification number.

h) Media forensics

Forensic watermark applications enhance a content owner's ability to detect and respond to misuse of its assets. Forensic watermarking is used not only to gather evidence for criminal proceedings, but also to enforce contractual usage agreements between a content owner and the people or companies with which it shares its content.

i) Locating content online

The volume of content being uploaded to the web continues to grow as we rely more and more on the Internet for information sharing, customer engagement, research and communication. It has also become a primary sales tool and selling environment, providing an opportunity to showcase our products or services and attract buyers from around the world.

V. WATERMARKING ATTACKS

There are various possible malicious intentional or unintentional attacks that a watermarked object is likely to subject to. The availability of wide range of image processing soft wares made it possible to perform attacks on the robustness of the watermarking systems. The aim of these attacks is to prevent the watermark from performing its intended purpose. A brief introduction to various types of watermarking attacks is as under:

a) Removal Attack

Removal attacks intend to remove the watermark data from the watermarked object. Such attacks exploit the fact that the watermark is usually an additive noise signal present in the host signal.

b) Interference attack

Interference attacks are those which add additional noise to the watermarked object. Lossy compression, quantization, collusion, denoising, remodulation, averaging, and noise storm are some examples of this category of attacks.

c) Geometric attack

All manipulations that affect the geometry of the image such as flipping, rotation, cropping, etc. should be detectable. A cropping attack from the right-hand side and the bottom of the image is an example of this attack.

d) Low pass filtering attack

A low pass filtering is done over the watermarked image and it results in a difference map composed of noise.

e) Security Attack

In particular, if the watermarking algorithm is known, an attacker can further try to perform modifications to render the watermark invalid or to estimate and modify the watermark. In this case, we talk about an attack on security. The watermarking algorithm is considered secure if the embedded information cannot be destroyed, detected or forged.

f) Protocol Attack

The protocol attacks do neither aim at destroying the embedded information nor at disabling the detection of the embedded information (deactivation of the watermark). Rather than that, they take advantage of semantic deficits of the watermark‘s implementation. Consequently, a robust watermark must not be invertible or to be copied. A copy attack, for example, would aim at copying a watermark from one media into another without knowledge of the secret key.

g) Cryptographic attacks

Cryptographic attacks deal with the cracking of the security. For example, finding the secret watermarking key using exhaustive brute force method is a cryptographic attack. Another example of this type of attack is the oracle attack . In the oracle attack, a non-watermarked object is created when a public watermark detector device is available. These attacks are similar to the attacks used in cryptography.

h) Active Attacks

Here, the hacker tries deliberately to remove the watermark or simply make it undetectable. This is a big issue in copyright protection, fingerprinting or copy control for example.

i) Passive Attacks

In this case, the attacker is not trying to remove the watermark but simply attempting to determine if a given mark is present or not.

j) Collusion Attacks

In collusive attacks, the goal of the hacker is the same as for the active attacks but the method is slightly different. In order to remove the watermark, the hacker uses several copies of the same data, containing each different watermark, to construct a new copy without any watermark. This is a problem in fingerprinting applications *(e.g.* in the film industry) but is not the widely spread because the attacker must have access to multiple copies of the same data and that the number needed can be pretty important.

k) Image Degradation

These type of attacks damage robust watermarks by removing parts of the image. The parts that are replaced may carry watermark information. Examples of these operations are partial cropping, row removal and column removal. Insertion of Gaussian noise also comes under this category, in which the image is degraded by adding noise controlled by its mean and its variance.

l) Image Enhancement

These attacks are convolution operations that desynchronize the watermark information in an image. These attacks include histogram equalization, sharpening, smoothing, median filtering and contrast enhancement.

m) Image Compression

In order to reduce the storage space and cut the cost of bandwidth required for transmitting images, images are generally compressed with JPEG and JPEG2000 compression techniques. These lossy compression methods are more harmful as compared to lossless compression methods. Lossless compression methods can recover the watermark information with inverse operation. However lossy compression techniques produce irreversible changes to the images. Therefore probability of recovering watermarked information is always very low.

n) Image Transformations

These types of attacks are also called synchronization attacks or geometrical attacks. The famous software Stir Mark uses small local geometrical distortions to invalidate watermark detection. Geometrical attacks include rotation, scaling and translation also called RST attacks. Some researchers focus on RST robustness while designing the robust watermarking systems, because it is fundamental problem. Besides RST transforms, image transformations also include other transforms such as aspect ratio change, shearing, reaction and projection .

VI. RESULT AND DISCUSSION

Performance Evaluation Metric

Performance evaluation is very important part in the any algorithmic design in watermarking. The main task of this is to evaluate the quality matrices of algorithm or method to find out, how much he is effective?

Some of the quality matrices an image watermarking method or algorithm.

The *MSE (mean square error)* is defined as average squared difference between a reference image and a distorted image. It is calculated by the formula given below

$$MSE = \frac{1}{mn}\sum_{0}^{m-1}\sum_{0}^{n-1}\|f(i,j) - g(i,j)\|^2$$

m and n are height and width respectively of the image. The f (i, j) is the pixel value of the cover image and g (i, j) is the pixel value of the embed image.

SNR (Signal to Noise ratio) measures the sensitivity of the imaging. It measures the signal strength relative to the background noise. It is calculated by the formula given below

$$SNR_{dB} = 10\log_{10}\left(\frac{P_{signal}}{P_{noise}}\right)$$

The PSNR (peak signal to noise ratio) is used to determine the degradation in the embedded image with respect to the host image. It is calculated by the formula given below

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

R is the peak signal value of the cover image which is equal to 255 for 8 bit images.

The *BER (bit error ratio)* is the ratio that describes how many bits received in error over the number of the total bits received. It is calculated by comparing bit values of embedded and cover image.

BER = P/ (H*W)

H and W are height and width of the watermarked image. P is the count number initialized to zero and it incremented by one if there is any bit difference between cover and embeeded image.

Result of LSB

The result shown below are of the large watermark embedded into a original image using LSB embedding algorithm, which uses the logo as watermark and spreads it out to full image size. Results from LSB substitution closely match with the expected one. The watermarked image shows slight but unnoticeable degradation, while the watermark(logo) was recovered perfectly.

Fig.6 Cover Image CI (Flower)

Fig.7 Watermark Image WI (logo)

1st bit substitution

2nd bit substitution

3rd bit substitution

4th bit substitution

Fig.8 (Invisible Watermarked Image)

5th bit substitution 6th bit substitution 7th bit substitution 8th bit substitution

Fig.9 (Visible Watermarked Image)

The above figure shows various images, WI, upon which the algorithm was implemented and their corresponding watermarked copy WM. Values for mean square error (MSE) and peak signal to noise ratio (PSNR) are measured.The following table shows the values of MSE and PSNR:

Table. III PSNR & MSE for Different Bit Substitution

Method	**PSNR**	**MSE**
LSB or 1st Bit Substitution	54.87	0.21
2nd Bit Substitution	45.54	1.83
3rd Bit Substitution	38.25	9.80
4th Bit Substitution	31.68	44.50
5th Bit Substitution	25.42	188.28
6th Bit Substitution	19.28	772.72
7th Bit Substitution	13.21	3129.01
MSB or 8th Bit Substitution	14.3467	2.3900e+003

Result of DCT

A set of four 8-bit grayscale digital images, shown in the following figure, were selected. The embedded watermark is shown in the next figure, is a binary logo of size 32× 32 pixels

Fig. 10 Image database (size of 512×512 pixels)

Fig.11 Embedded Watermark(size of 32×32 pixels)

Results show that there are no visual degradation on images that watermarked by DCT based techniques as their PSNR for 'Lena' is 66.13db.

PSNR 66.1336db

MSE 0.0158386

Fig.12 Watermarked Image

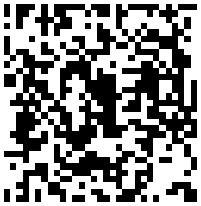

Fig.13 Extracted Watermark

Literature survey shows that each watermark method has its own strengths and weaknesses. The quality of watermarked images is measured in terms of PSNR (Peak Signal to Noise Ratio) and MSE (Mean Square Error). In ideal case the value of PSNR & MSE should be infinite and zero respectively . But it is not possible for watermarked image. So, large PSNR and small MSE is desirable.

VII. Conclusion and Future Scope

In this paper the authors have presented various aspects for digital watermarking like overview, framework, techniques, and applications. Apart from it a brief and comparative analysis of watermarking techniques is presented with their advantages and disadvantages which can help the new researchers in related areas. I also tried to classify the digital watermarking in all the known aspects like robustness, host signal, perceptivity, purpose, watermark type, domain, detection process and use of keys. Watermarking embeds ownership information directly into the document, and it is proposed as a "last line of defense" against unauthorized distribution of digital media. Desirable properties of watermarks include imperceptibility, robustness, and security. Each type of document presents unique problems for embedding and recovery. The success of these methods encourages the development of more sophisticated watermarking algorithms as part of a larger system for protecting valuable digital documents. According to different applications, there are different requirements of the watermarking system. However, it is hard to satisfy all the requirements at the same time. So, benchmark is used to evaluate and compare the performance of different watermarking systems.

Acknowledgement

The authors are grateful to Prof. Shalabh Agarwal for giving opportunity to do research work in the field of Digital Watermarking. One of the authors AN is very much grateful to Fr. Dr. John Felix Raj, principal of St. Xavier's College(Autonomous), Kolkata for giving constant inspiration to do research work in Computer Science and Engineering.

References

1. Lalit Kumar Saini, Vishal Shrivastava,"A Survey of Digital Watermarking Techniques and its Applications", International Journal of Computer Science Trends and Technology (IJCST) – Volume 2 Issue 3, May-Jun 2014
2. Jonathan K. Su, Frank Hartung, Bernd Girod," Digital Watermarking of Text, Image, and Video Documents"
3. K.Sridhar, Dr. Syed Abdul Sattar , Dr. M Chandra Mohan," Comparison of Digital Watermarking with Other Techniques of Data Hiding", International Journal of Computer Science and Information Technologies (IJCSIT), Vol. 5 (1) , 2014, 350-353
4. Namita Chandrakar, Jaspal Bagga,"Performance Comparison of Digital Image Watermarking Techniques: A Survey", International Journal of Computer Applications Technology and Research Volume 2– Issue 2, 126 - 130, 2013
5. Prabhishek Singh, R S Chadha,"A Survey of Digital Watermarking Techniques, Applications and Attacks",International Journal of Engineering and Innovative Technology (IJEIT) Volume 2, Issue 9, March 2013
6. L. Robert, T.Shanmugapriya,"A Study on Digital Watermarking Techniques", International Journal of Recent Trends in Engineering, Vol. 1, No. 2, May 2009
7. "Literature Survey on Digital Image Watermarking" Er-Hsien Fu ,EE381K-Multidimensional Signal Processing,8/19/98
8. Puneet Kr Sharma and Rajni ," ANALYSIS OF IMAGE WATERMARKING USING LEAST SIGNIFICANT BIT ALGORITHM", International Journal of Information Sciences and Techniques (IJIST) Vol.2, No.4, July 2012
9. Bhupendra Ram," Digital Image Watermarking Technique Using Discrete Wavelet Transform And Discrete Cosine Transform", International Journal of Advancements in Research & Technology, Volume 2, Issue4, April-2013 ISSN 2278-7763

10. Ensaf Hussein, Mohamed A. Belal , "A Comparative Study of Digital Watermarking Techniques in Frequency Domain", International Journal of Computer Applications (0975 – 8887) Volume 52– No.20, August 2012

11. Deepshikha Chopra, Preeti Gupta, Gaur Sanjay B.C., Anil Gupta,"Lsb Based Digital Image Watermarking For Gray Scale Image", IOSR Journal of Computer Engineering (IOSRJCE) ISSN: 2278-0661, ISBN: 2278-8727 Volume 6, Issue 1 (Sep-Oct. 2012), PP 36-41 www.iosrjournals.org

AUTHOR(S) PROFILE

Sunanda Datta, currently pursuing MSc degree in Computer Science from St.Xavier's Collage,(Autonomous).

Dr. Asoke Nath is Associate Professor in the Department of Computer Science, St. Xavier's College (Autonomous), Kolkata, India. Presently he is involved in research work in the areas like Cryptography and Network security, Steganography, Visual Cryptography, Green Computing, MOOCs, e-learning Methodologis, Artificial Neural Networks. He has published more than 116 papers in International Journals and conference proceedings.

