Digital Watermarking and Security Techniques: A Review

[1]Baljit Kaur, [2]Sonia Sharma
[1,2]Dept. of CSE, Guru nanak Dev University, Amritsar, Punjab, India

Abstract
In today's world internet technology made our life very much easy. Security and reliability of images or information are major factors, but there are security problems. When we transmit the data over the internet the main problem is to secure the data from redundancy. Digital watermarking technique is use to provides security or protection of digital information,so that unauthorized user can't access the information. Digital watermarking is commonly used in medical applications. Digital watermarking techniques have been developed to protect the copyright of digital media. In this paper our aim is to provide the detailed review of digital watermarking its applications and recent existing techniques for security applications.

Keywords
Digital Watermarking, Classification, Security Techniques.

I. Introduction

Digital watermarking is that technology that provides protection, appropriate data and copyright protection of the digital data. Security of digital data has become a popular matter due to the fast development of the multimedia technology. Digital watermarking is the process of inserting secret digital data, signal into the digital media such as image, video, audio and text. Digital Image Watermarking technology has many applications for protection of digital data. The basic idea of digital watermarking is to embed the information i.e. watermark into a host image. Then that watermarked image will be transmitted over the internet and at the receiver side information is taking out.

II. Digital Watermarking

Digital watermarking is that technology which is used for security purpose of digital media such as video, audio and image [1]. In this technique, watermark i.e. secret information is inserted in digital media using some algorithms and the watermarked media is processed. After that, secret information is taken out(extracted) using the particular algorithm. This technique, i.e. digital watermarking is used for justification of data and protection of copyright [2].

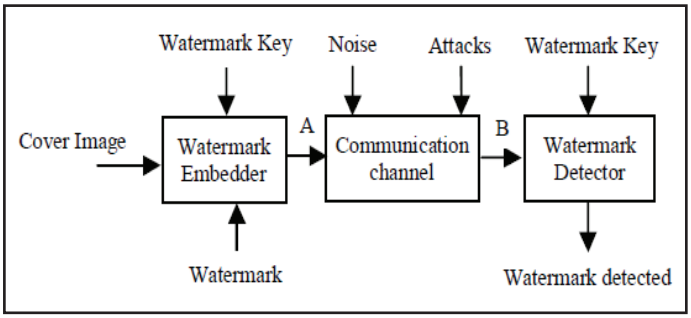

Fig. 1:

III. Properties or Requirement of Watermarking

The basic requirements of the digital watermarking can be treated as properties or qualities, there are some basic qualities of digital watermarking.

A. Robustness

Robustness refers to that the watermark inserted in data has the capability of detecting watermark after a variety of processing operations and attacks. In other words the ability to survive. The watermark should not removed by simple processing techniques. This watermark used to resist normal processing.

B. Security

This means that only authorized user can access the information ,or unauthourized person cannot remove the watermark without having full knowledge of embedding algorithims. This is most important factor of watermarking in this only authourized user can detect the watermark.

C. Fidelity

This means that hiding or transparency is the most important need in watermarking system. Watermark cannot be detected by human eyes ,only be detected through special operations of watermark detector. It can be accessed or detected by an authorized person only. Such watermarks are used for content or author validation and for detecting unauthorized copies of the data. The digital watermark should not affect the quality of the original image after it is watermarked.

D. Computational Complexity

It is defined as the amount of time taken by the watermarking algorithm for inserting and extraction process. More computational difficulty is required for the strong protection and validity of the watermark. On the other hand, real-time applications require both speed and efficiency.

E. Computational Cost

It depends on the method which is used for watermarking. If the watermarking method is more difficult, then it contains complex algorithm, need of more software and hardware, so computational cost increases and vice versa.

F. Capacity

Watermark capacity or data payload refers the amount of secret information present in watermark image. It simply means that how much amount of information, we able to insert in the image. Data payload or capacity is the number of bits a watermark encodes within a unit of time.

IV. Classification of Watermarking

In this section Digital Watermarking and its techniques are classified and segmented into various categories.

A. According to Human Perceptivity

Digital watermarking is divided into two main categories: visible and invisible.

1. Visible Watermark

When a visible transparent image is overlaid on the original image it is called visible watermark. It can be easily seen by human eye. Visible watermark is used so that it can be read by receiver. It is

equal to stamping a watermark on paper. Examples are Name or company's logo or any copyright data.

Invisible Watermarking

Invisible watermark is hidden in the original content. It can be observed by an authorized person only. Watermark is inserted in such a way that changes made the pixel value are perceptually not noticed and it can be recovered only with appropriate decoding mechanism.

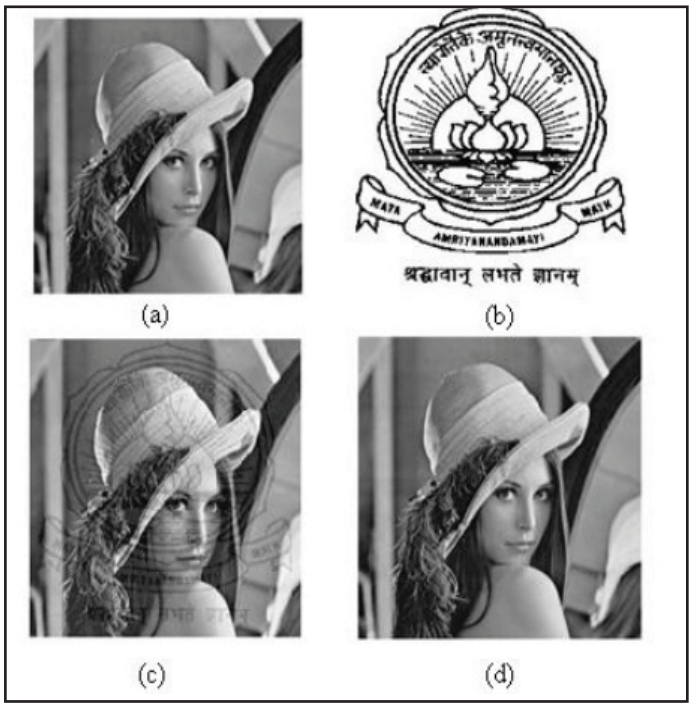

Fig. 2: [11] (a) the Original Lena Image (b) the Logo to be Watermarked (c) Visible Watermarked Image and (d) Invisible Watermarked Image

B. According Host Signal or Attached Media

1. Text Watermarking

This adds watermark to the text file to check the alteration made to text files. The watermark is inserted in the font shape and the space between font, characters and line spaces.

2. Image Watermarking

In this the image is used to hide the digital data. It is used to protect the photos over internet .This inserts special information to an image and detects or take out it later for ownership confirmation.

3. Video Watermarking

In video watermarking the watermark are inserted to the video stream to control video application. This method needs real time extraction and robustness for reduction (compression). It is an extension of image watermarking.

4. Audio Watermarking

This application area is one of the most common , in demand and hot matter due to internet composition of tunes, MP3.

5. Graphic Watermarking

It adds the watermark to 2D or 3D computer generated graphics to specify the copyright.

C. According to Robustness

Watermarks need robustness to protect the ownership from various attacks. The followings show the classification dependent on the robustness of a watermark.

1. Robust

Resist various attacks, without affecting embedded watermark. Robustness watermarking is mainly used to sign copyright information of the digital works, the embedded watermark can protect against the common edit processing, image processing and lossy compression, and the watermark is not cracked after some attack.

2. Semi-Fragile

Is capable of tolerating some degree of the alterations to a watermarked image, such as the addition of quantization noise from lossy compression. Semi fragile watermarking is capable of tolerating some degree of the change to a watermarked image.

3. Fragile

Fragile watermark is designed to be easily destroyed if a watermarked image is manipulated in the slightest manner. This watermarking method be used for the protection and the verification of original contents. Fragile watermarking is mainly used for reliability protection, which must be very responsive to the changes of signal. We can determine whether the data has been tampered according to the state of fragile watermarking.

D. According to Watermark Type

Watermark types can be classified into two types: noise type and image type.

1. **Noise:** Have pseudo noise, Gaussian random and chaotic sequences.
2. **Image Format:** There are binary image, stamp, logo and label.

E. According to Detection Process

1. Visual Watermarking

It is known as private watermarking . In visual watermarking the original data are required. It is most robust method of watermarking. This requires at least an original media. It extracts a watermark from the possibly distorted image and the original media.

2. Semi Blind Watermarking

It does not require an original media for detection. It is also known as semi private watermarking. In this watermarking scheme the original data are not required for detection of watermark.

3. Blind Watermarking

It requires neither an original media nor the embedded (inserted) watermark. Blind watermarking is also known as public watermarking. This is the most demanding type of watermarking

V. Applications of Digital Watermarking

There are various applications of Digital Image Watermarking. Digital watermarking is used in several applications. The aim of every application is to providing security of the digital information. Following are the most important applications.

A. Copyright Protection
The one of the most important application of watermarking is copyright protection from the unauthorized user. Ownership of digital media can be established in the case of a copyright dispute by using the embedded data as a proof.

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

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

D. Data Authentication and Verification
The watermark is inserted to detect if the image has customized or not, this process can be used for verification. Integrity verification can be achieved by using fragile or semi fragile watermark which has low robustness to modification in an image.

E. Fingerprinting
The main purpose of fingerprinting is to protect clients. If someone got a legal copy of a product, but redistributed illegally, fingerprinting can prevent this. This can be achieved by tracing the whole transaction by inserting single robust watermark for each receiver.

F. Content Description
This watermark can contain some detailed information of the host image such as labeling and captioning. The capacity of watermark for this kind of application should be relatively large and there is no strict requirement of robustness.

G. Medical Applications
In medical field the watermarking is important for the purpose to protect the hospital's information from unauthorized people such as patient's report etc. Security and verification of such data are now becoming very significant in medical field where the digital data are easily distributed over the internet.

VI. Watermarking Techniques
Digital watermarking is very much common now a days because it is easily available and it secure our data from illegal use. It has two major techniques i.e. spatial domain .In the spatial domain techniques, we insert the watermark by modifying the pixel values.

Transform domain watermarking:The watermark is inserted into the coefficients of transform domain. Various types of transform domain techniques are DCT, DWT and DFT. From robustness and hiding (imperceptibility) point of view, transform domain techniques are better than spatial domain techniques.

A. Spatial Domain Watermarking
In this the image is made up of pixels. we insert the watermark in some specific pixels of image . In the extraction phase, we extract the watermark from these specific pixels. This technique is very much easy to use, less complex and also takes less time. But it is not robust for various types of attacks.

1. LSB (least significant bit)
LSB is the most commonly used technique in spatial domain. It selects the some random pixels of the cover image to insert the watermark.

Steps:
1. Conversion of RGB image to Gray scale image.
2. Find double precision for image.
3. Transfer most significant bits to low significant bits of watermarked image.
4. Make least significant bits of host image zero.
5. Add shifted version (step 3) of watermarked image to modified (step 4) host image.

2. Advantage
It is easily performed on images. It provides high perceptual Transparency. When LSB technique is used to insert the watermark, quality of image will remains same. Easy to implement.

3. Drawback
LSB technique is less robust to common signal processing operations Sensitive to noise.

B. Transform (Frequency) Domain Watermarking
This technique is also called as frequency domain watermarking. The transform domain watermarking is better as compared to the spatial domain watermarking. The image is represented in the form of frequency in the transform domain watermarking. In this firstly conversion of the original image is done by a predefined transformation. Then we insert the watermark in the transform image or in the transformation coefficients. Finally, we take the inverse transform to get the watermarked image . Some commonly used transform domain methods are Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), and Discrete Fourier Transform (DFT).

1. DCT
It is commonly used for the signal processing. In this we transform the image into the frequency domain. It is used in many areas like pattern recognition, data compression, and image processing. This technique is more robust than spatial domain watermarking techniques.

The main steps used in DCT are:
- Firstly, take the image and divide it into non overlapping 8*8 blocks.
- Calculate forward DCT of each of the non overlapping blocks.
- Use HVS blocks selection criteria.
- Now use highest coefficient selection criteria.
- Then embed watermark in the selected coefficient.
- Now take inverse DCT transform of each block.

2. DWT
It gives a multi resolution representation of the image. This representation provides a simple framework for interpreting the image formation. The DWT analyses the signal at multiple resolution. When we apply the DWT to an image, it divides the image into two quadrants, i.e. high frequency quadrant and low frequency quadrant. This process repeats until the signal has been entirely decomposed. If we apply 1-level DWT on 2D image.

It divides it into four parts.

LL: It consists the low frequency details of the original image. We can say that estimation of the image lies in this part.

LH: It consists vertical details of the original image.

HL: It consists the horizontal details of the original image.
HH. It consists high frequency details of the original image
Since we know that the detail of original image lies in low frequency coefficients, so we embed the watermark into low frequency coefficients. If we apply IDWT, we can reconstruct the original image from the decomposed image.

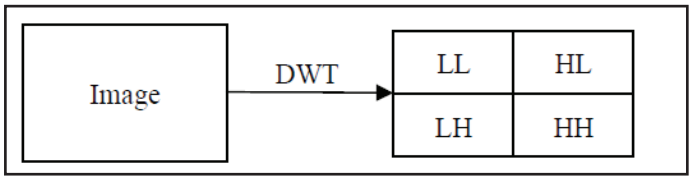

Fig. 3: Level Decomposition

3. DFT

Offers more robustness against geometric attacks like scaling, cropping, translation, rotation, etc. It decomposes an image in sine and cosine form. In this, embedding may be done in two ways: direct embedding and the template based embedding.
In the direct embedding technique we modifying DFT magnitude and phase coefficients and then the watermark is inserted.
The template based embedding technique introduces the concept of templates. In DFT domain, during embedding process, we embed the template, which is used to find the transformation factor. When the image is transformed, firstly this template is searched and it is then used to resynchronize the image. After this, detector is used to extract the embedded spread spectrum watermark.
Cons: Implementation is complex. And the computational cost is also higher.

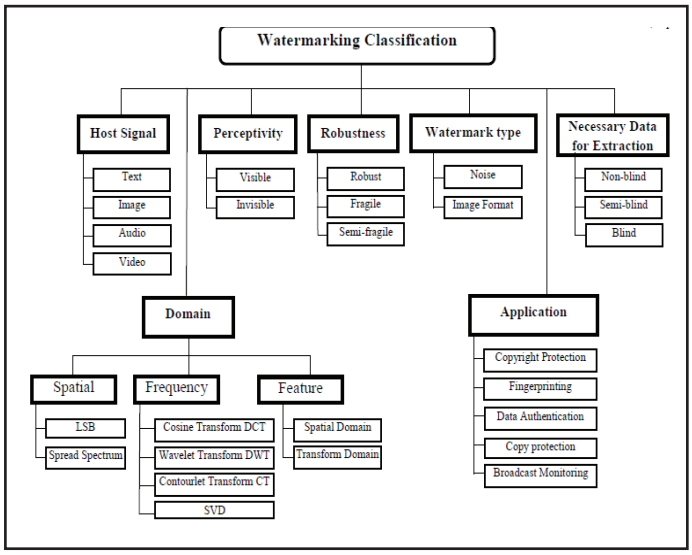

Fig. 4:

VII. Conclusion

In this paper we offered the overall overview of digital watermarking, its properties , classification on the basis of host signal, perceptivity, robustness, watermark type, necessary data for extraction, detection process, its applications and techniques of watermarking used for security purpose .In this paper we have discussed various methods of techniques such as spatial domain and frequency domain in detail .From research point of view this technology is an interesting area, because these techniques are emerging for protection of data .The watermark is needed to prevent the original image and the other document over the internet.

References

[1] R.G. Schyndel, A. Tirkel, C.F Osborne,"A Digital Watermark", Proceedings of IEEE International conference on Image Processing, ICIP-1994, pp. 86-90, 1994.
[2] Christine I. Podilchuk, Edward J. Delp,"Digital watermarking: Algorithms and applications", IEEE Signal processing Magazine, July 2001.
[3] C.-T. Li, F.M. Yang.,"One-dimensional Neighborhood Forming Strategy for Fragile Watermarking", In Journal of Electronic Imaging, Vol. 12, No. 2, pp. 284-291, 2003.
[4] Ruchika patel, Part Bhatt_Ass.professor. Department of IT information technology, The Gujarat Technology university SVIT,Vasad,Gujarat, 388306, India., "A Review paper on digital watermarking and its techniques".
[5] Tejaswita Salunkhe, Chhaya Nayak,"Review of Digital Watermarking Techniques", M. Tech Student, Dept. of CSE, B.M College of Technology, Indore, M.P. India Assistant Professor& HOD, Dept. of CSE, B.M College of Technology, Indore, M.P. India. (An ISO 3297: 2007 Certified Organization) Vol. 3, Issue 9, September 2015.
[6] Sonam Tyagi, Harsh Vikram Singh Raghav Agarwal, Sandeep Kumar Gangwar,"Digital Watermarking Techniques for Security Applications". International Conference on Emerging Trends in Electrical, Electronics and Sustainable Energy Systems (ICETEESES–16).
[7] Ensaf Hussein Senior Teaching Assistant, Mohamed A. Belal Professor, Computer Science Dept.,Faculty of Computers & Information, Helwan Univ.,Cairo, Egypt." Digital Watermarking Techniques, Applications and Attacks Applied to Digital Media: A Survey. (IJERT) Vol. 1, Issue 7, September – 2012.
[8] V. M. Potdar, S. Han, E. Chang,"A Survey of Digital Image Watermarking Techniques", 2005 3rd IEEE International Conference on Industrial Informatics (INDIN).
[9] N. Tiwari, M. K. Ramaiya, Monika Sharma,"Digital watermarking using DWT and DES", IEEE (2013).
[10] S. S. Gonge, J. W. Bakal,"Robust Digital Watermarking Techniques by Using DCT and Spread Spectrum", International Journal of Electrical, Electronics and Data Communication, Vol. 1, No. 2, 2013.
[11] Shraddha S. Katariya,"Digital Watermarking: Review", In International Journal of Engineering and Innovative Technology, 2012