An Introduction to the Digital Watermarking

Kavitha K. J.[1], Dr. B. Priestly Shan[2]

[1]PhD (Scholar), Sathyabama University, Chennai, Tamil Nadu, India
[2]Principal, Royal College of Engg., Trissur, Kerala, India

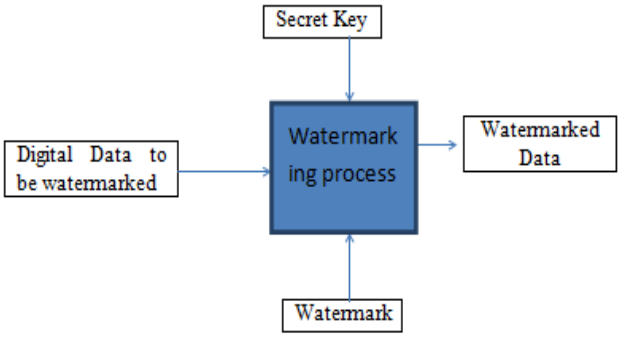
Abstract— *Digital watermarking is the process of embedding a message pertaining to the digital content itself and contains information about its author, buyer etc. It is same as that of steganography; only the difference is in the process of hiding the information. In digital watermarking the information is hided pertaining to the digital content itself whereas the message embedded in a digital content in the case of steganography is the secret message that has to be transmitted over the communication channel. Hence digital watermarking can be used for many applications like ownership assertion, copy right prevention, fingerprinting, data authentication (medical field) etc.*

Keywords— Steganography, digital watermark, fingerprint.

I. INTRODUCTION

During the past one decade, digital watermarking has fascinated the attention of various researchers. As a consequence, hundreds of work has been published regarding the different methods for watermarking. Digital watermarking is an encouraging technology to insert message as imperceptible signals in digital contents [1]. The information inserted as a watermark can be almost anything. It can be a bit string, sequential number, plain text, logo etc. However the major practical challenge is to design an extremely robust digital watermarking technique, which disables copyright violation by making the process of watermarking removal tedious and expensive [2]. The process of watermarking is as shown in Figure 1 and the result obtained after the process is called watermarked data.

This paper was submitted on 07-10-2015. An Introduction to the Digital watermarking gives the introduction to digital watermarking technique, types of DWM , requirements in the watermarking technique etc.



Fig,1: Digital Watermarking System

Digital watermarking can be classified into different types based on characteristics and applications. Based on the characteristics, the digital watermarking can be classified as [3]:

1. *Perceptible watermark*: If the embedded information in a digital content is visible to the human eye is referred to as perceptible watermark. It is defined by the equation
   Fw= (1-α) F+αw
   Where, Fw=watermarked image
   F=original image
   W=watermark
   If α=0, No watermark
   A=1, Watermark is present
2. *Imperceptible watermark*: If the embedded information is not visible to the human eye is referred to as imperceptible watermark [15]. It is defined by the equation
   Fw=4(α/4) +w/64.
   Imperceptible watermark can be further classified into 3 types:
   a. Robust watermark
   b. Fragile watermark
   c. Semi fragile watermark

Based on the applications, digital watermarking can be classified as:

1. *Copyright Protection Watermarks*
2. *Data Authentication Watermarks*
3. *Fingerprint Watermarks*

4. *Copy Control Watermarks*
5. *Device Control Watermarks*

II. WATERMARKING REQUIREMENTS

Watermarking systems can be branded by a number of important properties including embedding effectiveness, trustworthiness, data payload, public or informed detection, false positive, capacity, strength, perceptual transparency, safekeeping, encryption and watermark keys, alteration and numerous watermark, cost, fiddle resistance, unobtrusiveness, explicit, sensitivity, and scalability. Some of them are common to more practical applications [4] , [14] and [5].

a. *Embedding effectiveness:* the effectiveness of a digital water mark system should be 100% but it is often not possible because of the requirement of perceptual similarity conflicts.
b. *Trustworthiness:* The digital watermark system should be trustworthiness /robust against various malicious attacks.
c. *Data payload:* It is the number of bits that can be encoded in a message. As the data payload increases it affect the fidelity of the system and vice-versa.
d. *Public or Informed detection*: Public detection requires information about the original message whereas an informed detection requires no information.
e. *False positive*: It is defined as the detection of non-marked image and it should be a very few.
f. *Capacity*: It is the number of bits that can be encoded within the message.
g. *Strength*: It must be robust against additive noise, filtering etc.
h. *Perceptual transparency*: It tells about how much degradation in image quality is suffered by addition of a watermark.

III. PRINCIPLES OF DIGITAL WATERMARKING

The digital watermarking embedding and extraction can be divided into three major classes: spatial domain, transform domain and hybrid domain.

A. *Spatial Domain***:** Spatial domain techniques hide data in the intensity of the original image pixels directly. The most commonly used spatial domain method is least significant bit (LSB) method in which the message bit is embedded in the least significant bit of the original image [6] and another method.

B. *Transform Domain:* Transform domain converts the spatial amplitude domain to frequency domain and hence it is also called as transform domain. And in the transform domain the watermark is embedded. The most popular techniques used under this category is DCT (Discrete Cosine Transform), DWT (Discrete Wavelet Transform) and DFT (Discrete Fourier Transform) [8] and [13].

Wavelet transform is a time domain confined investigation method with the windows size fixed and forms translatable. There is quite good time discriminated rate in high frequency part of signals DWT transformed. Also there is quite good frequency discriminated rate in its low frequency part. It can extract the information from signal effectively [9].

The DCT technique operates in the frequency domain by embedding a pseudo-random generated sequence of real numbers in a particular set of DCT coefficients [9].

The discrete Fourier transform is the one of the mostly used tool for signal analysis. It breakdowns a signal into componential sinusoids of different frequencies. It has very useful frequency content. During the transforming a signal in to frequency domain signal the time domain information is lost. The watermark is inserted into particular frequency bands of the figured magnitude domain of the DFT, thereby creating a watermarked magnitude domain [5].

C. *Hybrid domain***:** More than one transform domain can be combined and can get the more benefits [7].

IV. ATTACKS AND THREATENING TO THE DIGITAL WATERMARKING

The digital watermarking techniques we employ to the various type of information must be robust against various attacks and these attacks can be classified as [11]:

Active Attacks: In this the hacker tries to remove the watermark or make it undetectable.

Passive Attacks: In this type of attack the hacker tries to identify whether the data is been tampered.

Collusion Attacks: The aim of this type of attack is same as that of active attack but the method used is different. In this the hacker uses several copies of same media and each media is provided with a different watermark in order to construct a copy with no watermark.

Forgery Attacks: In this type, the hacker tries to embed the watermark of their own instead of removing one.

Distortive Attacks: Here hackers use some alterations over the entity to destroy/damage the watermark so that it cannot be detectable.

Whatever the watermarking techniques or algorithms we develop it must be resistive to such attacks and threats.

V. BENCH MARK TOOLS FOR DIGITAL WATERMARKING

Although we are provided with many signal processing tools to alter the digital contents without any perceptible trace of the changes, in some cases we may require to make ensure that the data is authentic i.e. it is originated from the correct source. For example, in the case of medical field the doctor want to make sure that the US images or any other reports related to the patient is authentic, because even a small mistake in the diagnosis leads to dangerous situations. Therefore to avoid all such cases, we need to evaluate the watermarking techniques or algorithms. To evaluate the system we have two well-known benchmark tools [10] viz. Stir mark and JEWELS. Stir mark and JEWELS are used to evaluate the watermarking techniques against the various attacks like image compression, geometric attacks etc. Stirmark and JEWELS both are referred to as single image attacks and JEWELS is provided with only one plural attack called as "Composite".

VI. QUALITY METRICS

To measure the quality of the watermarking system the various quality metrics can be used such as Peak signal to noise ratio (PSNR), Mean Square Error (MSE), Structural Similarity Index Measure (SSIM), NORMALISED CORRELATION COEFFICIENT (NC) and BIT ERROR RATE (BER) etc.

Peak signal to noise ratio: It is in short abbreviated as PSNR and can be defined as the ratio of maximum probable power of an image to the power of noise that affects the reliability of its image [12]. 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.

VII. CONCLUSION

The digital watermarking technique is employed in various applications like: ownership assertion, copyright prevention and control, fingerprinting, legal cases, military, medical field, commercial applications and also adopted by the government sectors.

Many watermarking techniques have been developed using spatial domain as well transform domain and tested against the various attacks and threats. The transform domain techniques are more efficient than that of spatial domain as the watermark is embedded in the frequency components which are very difficult to identify. Moreover the efficiency of the watermarking techniques can be increased by coupling more than one transform domain.

ACKNOWLEDGEMENT

We would like to thank my Guide Dr. Priestly B. Shan for his constant support and encouragement. We also extend our thanks to all our friends and colleagues for their support.

REFERENCES

[1] S. Cheung, D. K. W. Chiu, and C. Ho, "The Use of Digital Watermarking for Intelligence Multimedia Document Distribution," vol. 3, no. 3, pp. 103–118, 2008.

[2] R. Mishra, "Digital Security using Watermarking Techniques via Discrete Wavelet Transform," vol. 476444, pp. 1–8, 2012.

[3] S. Bhattacharya, T. Chattopadhyay, and A. Pal, "A Survey on Different Video Watermarking Techniques and Comparative Analysis with Reference to H . 264 / AVC," pp. 0–5, 2006.

[4] G. V Mane and G. G. Chiddarwar, "Review Paper on Video Watermarking Techniques," vol. 3, no. 4, pp. 1–5, 2013.

[5] H. Shojanazeri, W. Azizun, W. Adnan, S. Mumtadzah, and S. Ahmad, "Video Watermarking Techniques for Copyright protection and Content Authentication," vol. 5, pp. 652–660, 2013.

[6] C. Science and S. Engineering, "An Overview of Different Type of Data Hiding Scheme in Image using Steganographic Techniques," vol. 4, no. 1, pp. 746–751, 2014.

[7] B. Mathur, "Study on high Performance and Effective Watermarking Scheme using Hybrid Transform (DCT-DWT)," pp. 170–176, 2013.

[8] S. Liew, S. Liew, and J. M. Zain, "Tamper Detection And Recovery With Run Length Encoding Compression," pp. 799–803, 2010.

[9] B. Ram, "Wavelet Transform And Discrete Cosine Transform," vol. 2, pp. 19–27, 2013.

[10] K. A. Navas, M. Sasikumar, and S. Sreevidya, "A Benchmark for Medical Image Watermarking," no. 91.

[11] A. Darwish and A. Abraham, "The Use of Computational Intelligence in Digital Watermarking : Review , Challenges , and New Trends Overview of

computational intelligence and digital watermarking," pp. 1–21, 2008.

[12] K. Pal, G. Ghosh, and M. Bhattacharya, "for Data Security Using Bit Replacement and Majority Algorithm Technique," 2002.

[13] Yatindra pathak, "A More Secure transmission of medical images by Two Label DWT and SVD based watermarking technique", IEEE International Conference on Advances in Engineering & Technology Research (ICAETR - 2014), August 01-02, 2014, Dr. Virendra Swarup Group of Institutions, Unnao, India.

[14] Shaifali Bhatnagar," An Approach of Efficient and Resistive Digital Watermarking using SVD", 978-1-4799-3080-7/14/$31.00_c 2014 IEEE.

[15] Arijit Kumar Pal," A Hybrid Reversible Watermarking Technique for Color Biomedical Images", 978-1-4799-1597-2/13/$31.00 ©2013 IEEE.