

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE) Vol 4, Issue 6, June 2017

A Review of Digital Watermarking and Its Techniques

^[1] Anu (Assistant Professor [Resource person]) Department of Computer Science and Engineering (UIET) Maharshi Dayanand University, Rohtak, Haryana

Abstract:— This is agreed by one and all that today's era is IT oriented and Internet has reached to every corner of our lives. Communicating over Internet or networks is a routine for us, this leads to the need of transmission security and safety of our confidential information which is being communicated. Digital Watermarking is a medium to assure integrity, piracy detection and knowing any kind of tempering done with the communicated data. It is also used for applications like owner's authentication, copyright maintenance and monitoring broadcasts. In this paper we will review digital watermarking with its techniques, applications, classification and factors effecting watermarking.

Keywords: - Watermarking, steganography, Factors, features, techniques, PNSR, MSE, NC, SNR, BER.

1. INTRODUCTION

Digital watermarking is a technique used by individuals for adding copyrights, exclusive rights notices or other verification information to their digital media [1]. Watermarks were created by Italy long ago in 13th century. Digital watermarking was first used by Andrew Tirkel and Charles Osborne in the year 1992 [2], [3]. Protection of digital information has become a need of today's world due to the popularity and development of multimedia market and technology. This has lead to the evolution of techniques like digital watermarking. Digital watermarking is a process where confidential digital information and signals are embedded within another digital medium such as audio, video, images or texts [4]. At later stage, this embedded information is extracted to find out the identity of the manufacturer or owner of that digital data. It is simply a medium of certification and safeguarding of digital media

(a) Difference between Watermarking and Steganography: -

Sometimes watermarking is confused with steganography as in both techniques Confidential or secret data is embedded within the cover media. But both are huge different from each other. Steganography completely hides the embedded data within cover media where as in watermarking the embedded data may or may not be hidden completely. Watermarking is mainly used for safeguarding copy rights and owner's identity whereas steganography is used to safeguard confidential embedded data. Watermarking focuses on showing the embedded data so that no one tries to capture it without permissions whereas steganography focuses on hiding embedded data so that intruders won't be able to see it at all.

(b) Process of Watermarking



Figure1:- With and without Watermark Images

Above figure (Figure1) shows the way any ordinary image looks before and after performing watermarking process on it. The process of digital watermarking is formed up of following steps: -

- (i) Watermark Embedding
- (ii) Distribution over Network
- (iii) Watermark Extraction
- (iv) Decision Stage



Figure2:- Watermark Embedding at Sender's Side



International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 4, Issue 6, June 2017

At Sender's Side, the cover media is embedded with watermark using some watermark algorithm like LSB, patchwork, DCT, DWT, DFT etc. as shown in figure 2. Then the media is send over the network to the destination like a normal message or signal. At receiver's side the watermarked media is decoded using de-watermarking algorithm as shown in below figure 3. In final stage, the extracted watermark is compared with original watermark to check for differences. A common method used here is Hamming distance [5].



Figure3:- Watermark extraction at Receiver's Side.

(c) Classification of Digital Watermarks

Digital Watermarking can be classified into following 2 types [6]: -

• *Visible Watermark*: - A visible watermark is the translucent text that is placed over cover media and is easily visible to human perception. It could have text like owner's name or company's logo which is placed intentionally on cover media so that it could be seen by everyone.

• **Invisible Watermark**: - This watermark is not visible to human perception as it is embedded inside the cover media and not over it. This is used generally to safeguard data from thefts or intrusions.

(d) Factors Effecting Digital Watermarking

(i) MSE (Mean Squared Error): - MSE is calculated by averaging the squared difference among distorted-image & cover-image. Equation for MSE is given below:-

$$MSE = \frac{\sum(M,N) [I1(m,n) - I2(M,N)]^{2}}{M*N} [7]$$

(*ii*) *PSNR* (*Peak Signal to Noise Ratio*): PSNR is the ratio among powers of any signal to corrupting noise. This corruption due to noise damages the fidelity of its representation [8].

$$PSNR = 10 \log_{10} (256^2 / MSE)$$

(iii) NC (Normalized Correlation) NC is used to calculate and evaluate homogeneity (or non-homogeneity) amongst cover-image and stego-image.

(*iv*) SNR (Signal to Noise Ratio) It represents the ratio of Signal-to-Noise powers in the background of desired image

(v) **BER** (**Bit Error Rate**) It describes ratio of no. of received bits with error to total no. of bits received.

$$\text{BER} = \frac{P}{H * W} [9]$$

H and W are Height and Width.

(e) Comparison of Watermarking Techniques

Table 1 compares different watermarking techniques based on their merits and demerits [1].

Technique	Merits	Demerits
Least Significant Bit	 It is easily understandable and easy to implement. It provides low image quality. Perceptual transparency is high. 	 Here basic robustness is less. Sensitive to noise. Sensitive to scaling, cropping.
Discrete Cosine Transform	 Here we embed the watermark into the middle frequency coefficients because in the middle frequency band, the perceptibility of the image doesn't get effected and if there are attacks on watermarked data, the watermark is not removable. 	 When we proceed to quantization step, higher frequency components present in the image, are suppressed.
Discrete Wavelet Transform	 DWT provides better localization in both time and frequency domain. Here we get higher compression ratio. 	 The computational cost is higher. Compressing time is longer.
Discrete Fourier Transform	 DFT is used to recover from geometric distortions, because DFT is rotation, scaling translation invariant. 	 Implementation is complex. The computational cost is also higher.

Table1: - Comparison of Different Watermarking Techniques [1].

(f) Features of Digital Watermarking

Digital watermarking has following features that make it popular: -

• Invisible and Inaudible: - Watermarked information is embedded without alteration of cover content and the level of embedded data is very small as compared to overall data making it unnoticeable to humans.



International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 4, Issue 6, June 2017

• Unchanged data file size: - The size of cover media is not changed after embedded data and remains same throughout the process.

• Inseparable: - The embedded data is inseparable from cover data and shows up for any kind of unauthorized intrusion. It also survives processes like compressions, format transformation and other processing.

• Robust: - It has the capability to sustain deformations and resists distortions due to data processing.

• Security: - It is very secure as it informs if any kind of suspicious work is done over the cover data. Any kind of detection work or removal work regarding watermark is captured and presented while extraction of watermark at receiver's side.

APPLICATIONS OD DIGITAL WATERMARKING

Watermarking is used almost in every field in one or another way. Some of the important uses of Digital Watermarking are listed below [6]: -

- Copyright control
- Copy protections
- Transmission/ transaction tracking
- Monitoring in broadcastings
- Digital authentication
- User verifications
- Prevention towards forgery
- Lyric sync services
- Digital signatures
- Fingerprinting

• In other applications like medical, military, industries etc.

II. CONCLUSION

Watermarking is a vast spread field with lots and never lasting researches carried out in this context. Depending upon user's requirements and security levels, an appropriate algorithm and technique of watermarking can be selected. In this paper we discussed about basic introduction to Digital watermarking with its techniques, classification, features, factors and applications. We concluded that watermarking is very feasible technique for copyright protection and maintenance of owner's identity. It hence provides a strong mean for safeguarding and protecting our data over networks.

REFERENCES

[1]. Mohan Durvey and Devshri satyarthi, "A Review Paper on Digital Watermarking", International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), ISSN: 2278-6856, Volume 3, Issue 4, July-August 2014.

[2]. Prabhishek Singh and 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.

[3]. R.G. Schyndel, A. Tirkel, and C.F Osborne, "A Digital Watermark", IEEE International conference on Image Processing, ICIP-1994, pp. 86-90.

[4]. Ruchika Patel and parth Bhatt, "A Review Paper on Digital watermarking and Its Techniques", International Journal of Computer Applications, ISSN: 0975-8887, Volume 110, No. 1, January 2015.

[5]. Jaishri Guru and Hemant damecha, "A Review of watermarking Algorithms for Digital Image", International Journal of Innovative Research in Computer and Communication Engineering, ISSN: 2320-9801, Volume 2, Issue 9, September 2014.

[6]. Tejaswita Salunkhe and Chhaya Nayak, "Review of Digital Watermarking Techniques", International Journal of Innovative Research in Computer and Communication Engineering, ISSN: 2320-9801, Volume 3, Issue 9, September 2015.

[7]. Stuti Goel et al., "A Review of Comparison Techniques of Image Steganography", Global Journal of Computer Science and Technology, ISSN- 0975-4350, Volume 13, Issue 4, 2013.

[8]. Banasthali Vidyapith, "Imahe Steganography Techniques: A Review Article", ACTA Technica Corviniensis- Bulletin of Engineering, ISSN: 2067-3809, Fascicule 3, July–September 2013.

[9]. Manpreet Kaur and Sheenam Malhotra, "Review Paper on Digital Image Watermarking Techniques for Robustness", International Journal of Advanced Research in Computer Science and Software Engineering, ISSN: 2277-128X, Volume4, Issue 5, May 2014.