A Review on Digital Watermarking Techniques

Atif Ali Khan[1], Anas Iqbal[2]

Abstract— **Digital Watermarking is the process in which message can be sent to a desired personnel or organization without being hacked or distorted. Malware attacks are zero in digitally watermarked signals. This watermarking can be applied to still images, audio signals and video files. The main idea behind the digital watermarking is to provide data security; the host image is used as a carrier signal which carries the embedded signal that is known as watermarked image. An owner identification key is used which recognizes the sender and the recipient to which the message has to be sent is known as key, without it the message cannot be decrypted. Steganography and cryptography are the two other processes which provide data security. Steganography is the origin of digital watermarking that is securing data by embedding it into other media and then sending it to the desired destination to confirm secure transmission.**

Index Terms— **Digital Watermarking, LSB, DCT, robustness.**

I. Introduction

The main purpose of digital watermarking is to provide data protection using multimedia data. The problem which is caused due to lack of copyright protection of multimedia data in a networked environment is the attack which can harm the file in network [5], the file can be associated to a multimedia file whether it may be image, audio or video [4]. The digital watermarking must authenticate the data creator, owner of the encrypted signal, the consumer for which data is being sent. Digital Communication is a necessity, nowadays even different government and rulers of all countries in the world are now putting stress on digitization because world is now a global village in this village mostly, required element is security od data. The robustness of several digital watermarking techniques needs to be improved the least significant bit (LSB) . There are different techniques which are involved in digital watermarking. This will be more secure version of sending data better than steganography and cryptography.

A. Steganography Process of hiding a file or message or audio-video signal within another media file it is easily visible like in our currency notes, hologram stickers.

B. Cryptography It is the science of sending the information to the concerned recipient so that it is not visible to human eye or to any other cyber attacker easily. There are many algorithm by which we can achieve such level of security for example Data Encryption Standard (DES), IDEA International Data Encryption Algorithm,(IDEA) Rivest, Shamir, Adelman (RSA).

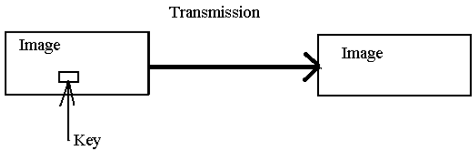


Fig 1 : Extraction of hidden message

II. DOMAINS OF WATERMARKING

The domain is the field in which the watermarking is implemented. There are two fields in digital watermarking which are characterizing as follows: c

A. Spatial Domain: In this domain the watermarking is carried by modifying the pixel values of the host image, the method which is involved for this is known as Least Significant Bit (LSB) in this each pixel is modified to embed the secret message other techniques are also used namely they are Gray scale Watermarking, Texture Block Coding and Patch Work Technique.

B. Transform Domain: This is used to transform the coefficient of the image, there are several techniques which are categorized under transform domain they are Discrete Cosine Transform (DCT), Discrete Wavelet Transform(DWT) and Discrete Fourier Transform (DFT).

III. PROCESS OF DIGITAL WATERMARKING

The process of digital watermarking involves three steps that are embedding, attacking or adding noise or distortion and third one is detection [1]. In embedding, the watermarked signal is embedded in the host image that will be the carrier image in this the pixel values are changed ire the image is transformed in such a way that the changes are not visible to the human eye, the attacks are added on the image which is transmitted as the hidden signal with the image that is the original image. The receiver level involves the detector which decodes the image with the help of key and the host image is separated from the message signal, in this processthere is no loss observed while transmission [6].

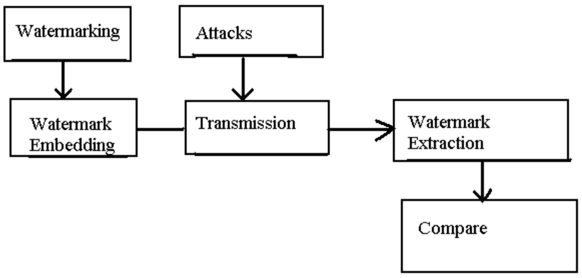


Fig 2 : Process of Digital Watermarking

Manuscript received September, 2017.

Atif Ali Khan, *Department of Electronics and Communication Engineering, ASCT Bhopal.*

Anas Iqbal*, Department of Electronics and Communication Engineering, ASCT Bhopal.*

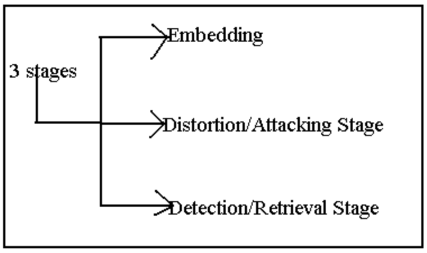


Fig 3 : Stages of Digital Watermarking

IV. DIFFERENT TECHNIQUES OF DIGITAL WATERMARKING

Some techniques which we will discuss in our review are as follows:

1. Least Significant Bit (LSB)

2. Discrete Cosine Transform (DCT)

3. Discrete Wavelet Transform (DWT)

4. Discrete Fourier Transform (DFT)

A.Least Significant Bit (LSB)

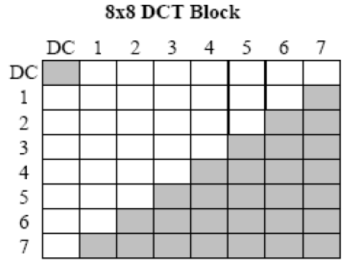
It is commonly used for Spatial domain[2], this technique is performed when we replace the most significant bit that is the right most bit in the image pixel to the lowest pixel value of the next pixel value, ultimately we will be shifting thevalue and changing the bit. This method consumes less time also it is less complex in computing the pixel value for coding and decoding. It is Simplest of all Techniques which are followed, only one disadvantage we came across while carrying out research was that it was not robust to attacks, was prone to hindrances also provided perceptual transparency. This method can be summed up in the following steps:

1. We convert RGB(colored) image to gray scale, make double precision for image.

2. Shift Most Significant Bits to Low Significant bits of watermarked image.

3. Those least Significant Bits of host image are made Zero by using redundancy and parity methods commonly by applying cyclic redundancy check method for determining and changing bits.

Only one limitation offered by this method is low robustness, because of this transform techniques are preferred as that provide more robustness to the signal being sent. B. Discrete Cosine Transform(DCT) It is most commonly used watermarking technique, in this technique the image is broken into three frequency bands that is low, medium and high frequency bands this splitting of image is for providing ease in choosing the frequency band in which we want to work to insert watermark. Middle frequency is chosen as it does not allow watermark to be easily detected as it does not allow watermark information to be scattered onto other visible parts of image that are the low frequency parts of image. This technique compares the middle band coefficients to encode the single bit in the DCT block. Middle band of 8X8 DCT block is regarded as FM, Lower band is depicted by FL and high band is FH in the figure below. The locations in the frequency middle band are selected for embedding region so as to provide resistance to lossy compression also to avoid changes in carrier image[7].



	DC	1	2	3	4	5	6	7
DC	▨							
1								▨
2							▨	▨
3						▨	▨	▨
4					▨	▨	▨	▨
5				▨	▨	▨	▨	▨
6			▨	▨	▨	▨	▨	▨
7		▨	▨	▨	▨	▨	▨	▨

Fig 4 : Watermarking process using the DCT domain.

In DCT method the changes are embedded at several parts of the image the grouping is done in image by treating pixels as pixel blocks and modification of single bit will affect 64 image pixels in that particular blocks. After this the signal is quantized so that human eye cannot distinguishbetween the modifications in brightness that is why the middle band is chosen for transformation. C. Discrete Wavelet Transform (DWT) DWT is the process in which transformation of produces image which represents multiresolution. It divides frequency by dividing image pixels into quadrants of high and low value these low frequency quadrants are again split into smaller parts that are specifically two parts of high and low among them and this process of breaking down is followed till the signal has been entirely decomposed. DWT gives better visual image quality, dividing the input coding into overlapping two dimensional block is not necessary, its higher compression ratios avoid blocking artifacts. DWT allows better localization as compared to the DCT. In this the working of Human Visual System is more clearly taken into consideration that is why multiresolution description of the image so, the image can be shown in different levels of resolution and proceed from low resolution to highresolution. The disadvantage of DWT is more complex also its cost is high and this process is also time consuming therefore most commonly DCT method is used. D. Discrete Fourier Transform (DFT)

It provides robustness against geometric attacks that are rotation, scaling, cropping, translation etc. It decomposes an image in sine and cosine form, the embedding techniques which are used for this transformation are of two types first one is direct embedding and other one is template based embedding. In direct embedding simple and regular embedding rules are followed but in template based the concept of template is added, in this template structure is embedded in DFT domain that to estimate the transformation factor once, the image undergoes any transformation it searches for template that is se for particular image for synchronizing the image and then to the detector is used to extract the watermark. It is used for periodic digital signals that use discrete time function, time f(x). Real image is complex valued which results in the phase and magnitude representation of an image. The main and strongest component of the DFT is the central component which contains low frequency. DFT is also resistant to cropping because it affects leads to blurring of spectrum. The watermark when embedded in magnitude the there is no need of synchronization. Scaling of image results in amplification of extracted signal and can be detected by correlation coefficient.

V. DIGITAL WATERMARKING APPLICATIONS

Digital water marking is hiding the data securing the information this has got many applications some are listed below:

1. Copyright Ownership: The copyright ownership is the embedding of message for identification of the owner of data for identification in host media[8].
2. Archiving Content: Content such as digital media are stored with identification marks like date, time and place name as watermark.It can be used for categorizing and organizing digital subjects [9].
3. Monitoring: This is specially for broadcasts messages in this the message can be monitored so that it can be broadcasted with true periodand real time interval information[10] for example advertisements.
4. Protection of copyright: It is used to protect reallocation of already copyrighted data over the entrusted network such as internet or peer to peer links [8]. As content is watermarked it will be hard to eliminate but can be easily circulated without any fear of attack.
5. Tamper Detection:Tamper recognition is very significant for applications which include medical data [6] so because of being digitally watermarked this delicate information cannot be hindered by the known or unknown attacker.
6. Digital fingerprints: This is used for differentiating the processor of digital content, owner inserts fingerprint in each copy of media [11] as no fingerprint can be similar so it is easy to recognize the data with same fingerprint.
7. Authentication: In this when the watermark media is utilized embedded watermark becomes invisible and undetectable. Hence, the recipient can easily understand that media is inconsistent [9].
8. Distribution over Electronic or physical media : transmission of digital films over electronic media it provides protection to data ,it can be transmitted point to point over optical cables that is for broadcast from single distribution to many receivers via satellites[3].
9. Integrity Verification : The content cannot be modified for its content meaning to be changed, the embedding confirms that original media to be altered if allowed by the authenticator ,only to specified parties

VI. ATTACKS

The several attacks which can be listed as follows:

1. Image Compression
2. Geometric Transformations
3. Image Enhancements
4. Image Composition
5. Information Reduction
6. Image Filtering and the introduction of noise.
7. Digital to Analog conversion

VII. ADVANTAGES

One of the major advantages is robustness the digital watermarking provides security to data to such a level that it does not get disrupted by noise or any other attack. Digital watermarking provides security, perceptual transparency, unambiguity that is it is less tangled the process has got procedural approach like it follows defined steps to carry out implementation.it is a reliable process in this we can rely wholly solely on it for security also it provides the imperceptibility to the image. These techniques are universally acceptable and followed for securing the data this adds on to advantage of digital watermarking.

VIII. CONCLUSION

Digital watermarking is new and latest method it has got several advantages over steganography and Cryptography also it has got numerous applications some are discussed in the paper. Nowadays the need for securing the data has led to the need for using digital watermarking as hiding data in another media so that it is not visible to human eye. There are several methods compared the one which is faster is LSB but is not robust but the methods which is not fast but provides high robustness is DCT method. Ultimately the digital watermarking is main method which is used for securing data and is most popular in terms of data security.

REFERENCES

[1] Jaishri guru, Hemantdamecha, “A Review of Watermarking Algorithms for Digital Image” International Journal of Innovative Research in Computer and Communication Engineering, Vol. 2, Issue 9, September 2014.

[2] TejaswitaSalunkhe, ChhayaNayak “Review of Digital Watermarking Techniques” International Journal of Innovative Research in Computerand Communication Engineering, Vol. 3, Issue 9, September 2015.

[3] Jeffrey A Bloom “Security And Rights Management In Digital, Cinema” Sam off Corporation, Princeton, NJ, IEEE IV - 712 ICASSP, 2003.

[4] Walter Godoy Jr., Charles Way Hun Fung “A Novel Dwt-Svd Video Watermarking scheme Using Side View” , IEEE, 2011.

[5] Frank Hartung, Jonathan K. Su, and Bernd Girod “Spread Spectrum Watermarking : Malicious Attacks and Counter Attacks of Multimedia Contents” International Journal of Research and In Engineering and Technology.

[6] Kazuki Yamato, Madoka Hasegawa, Yuichi Tanaka‡ And Shigeo Kato “Digital Image Watermarking Method Using Between-Class Variance”. 978-1-4673-2533-2/12/$26.00 ©2012 IEEE.

[7] T. C. Lin and C. M. Lin, “Wavelet based copyright protection scheme for digital images based on local features”, Information Sciences: an International Journal, Vol. 179, Sept. 2012.

[8] ChitlaArathi,’’ A Semi Fragile Image Watermarking Technique Using Block Based SVD”,International Journal of Computer Science and Information Technologies, Vol. 3 (2), 3644-3647,2012.

[9] S. Titov"Perceptually Based Image Comparison Method", 2000. http://graphics.cs.msu.su/en/publications/.

[10] ShahzadAlam, Vipin Kumar, Waseem A Siddiqui And Musheer Ahmad . “Key Dependent Image Steganography Using Edge Detection” . Fourth International Conference On Advanced Computing & Communication Technologies, 2014.

[11] Digital Watermarking 4th International Workshop, IWDW 2005, Siena, Italy, September 15-17, 2005. Proceedings.

[12] Natalia Voloshina, Sergey Bezzateev, Konstantin Zhidanov, "Weighted Digital Watermarking Approaches Comparison", 2016 XV International Symposium "Problems of Redundancy in Information and Control Systems" (REDUNDANCY).

[13] Ankit Rajpal , Anurag Mishra, Rajni Bala, "Fast Digital Watermarking of Uncompressed Colored Images using Bidirectional Extreme Learning Machine", IEEE International Joint Conference on Neural Networks (IJCNN) 2017

[14] Jun LV, Xiu-Mei Li, "Digital Image Watermaking Based on Bayesian Compressive Sensing", IEEE Prceedings of International Conference on Wavelet Analysis and Pattern Recognition, Ningbo, China, 9-12 July, 2017.

[15] J.H Saturwar, D.N.Chaudhari, "Review of Models, Issues and Applications of Digital Watermarking Based on Visual Cryptography", IEEE International Conference on Inventive Systems and Control (ICISC-2017).

[16] [6] Tao Wang,"Digital Image Watermarking using Dual-scrambling and Singular Value Decomposition", 2017 IEEE International Conference on Computational Science and Engineering (CSE) and IEEE International Conference on Embedded and Ubiquitous Computing (EUC).