A SURVEY ON INFORMATION HIDING TECHNIQUE DIGITAL WATERMARKING

TARUN AGRAWAL

Department of Electronics and Communication Engineering
G.L.A. University Mathura
UP, India
E-mail: tarun.agrawal_ec12@gla.ac.in

Abstract — In today's scenario the use of the internet increased to availability of data such as image, text, audio and video files to the public. In today's worlds Digital Watermarking is the technology that being developed to ensure and provide authentication data, protection from copyright of digital media Digital watermarking is the technology that can be easily applied to text, image, audio and video files. This report on topic "Digital Watermarking" contains brief study of Digital Watermarking, concept, main points in this area. It starts with overview, classification based upon different parameters, architecture, techniques, properties, attack's, application, Advantages and Disadvantages, requirements, Limitations and challenges, and evaluate performance metric of Digital Watermarking

Keywords – Applications, Attacks, Challenges, Techniques, Digital Watermarking, Steganography, Information hiding, Robustness, spatial domain, Frequency domain, Spread spectrum, LSB, DFT, DCT, DWT.

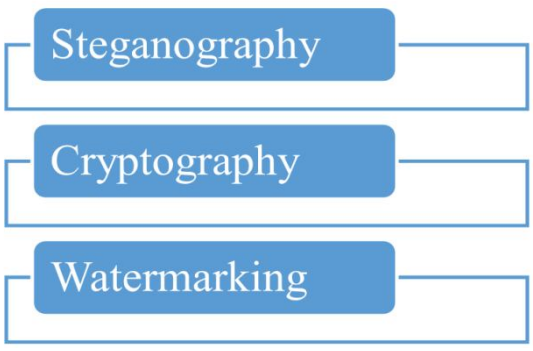
I. INTRODUCTION

As the use of internet is increasing day by day with this the insecurity of protection of copyright material, illegal copying of data, distribution and modification of data is also increasing. Due to this copyrighting economic losses occurring, because of Digital piracy of movies and music. So there is a need of some technique that rise protection, security against piracy, copyrighting. So Digital Watermarking is that technology which provides security, data authentication and protection from copyright to the digital media. Watermarking is the technique of inserting signal that is any secret information such as password key etc. into any digital media such as digital image, audio or video. That also identifies the files copyright information (name of author, rights etc.). Sometimes this techniques that is Digital Watermarking is known as "Data embedding". It has several applications in protection, distribution, and certification, anti-counterfeit of digital media and label of user information. In Image Processing digital watermarking become very important study area in hiding information. This report is organized as follows:

- Section 2 describes main information hiding technologies in detailed description.
- Section 3 describes how the digital watermarking is different from the information hiding technologies that is steganography and cryptography.
- Section 4 describes the Architecture of Digital Watermarking and its modules.
- Section 5 describes the classifications of digital watermarking techniques.
- Section 6 describes the comparison between the Discrete Cosine Transform and Discrete Wavelet Transform.
- Section 7 describes comparison between transform (Frequency) domain and spatial (pixel) domain.
- Section 8 describes backdrops of watermark technique systems and other technique.
- Section 9 describes the properties of Digital Watermarking.
- Section 10 describes the Attacks on Digital Watermarking.
- Section 11 describes the Applications of Digital Watermarking.
- Section 12 describes the Advantages and Disadvantages of Digital Watermarking.
- Section 13 describes the Requirements of Digital watermarking.
- Section 14 describes the Limitations and challenges in Digital Watermarking.
- Section 15 describes the Performance evaluation Metric.

II. INFORMATION HIDING TECHNIQUES

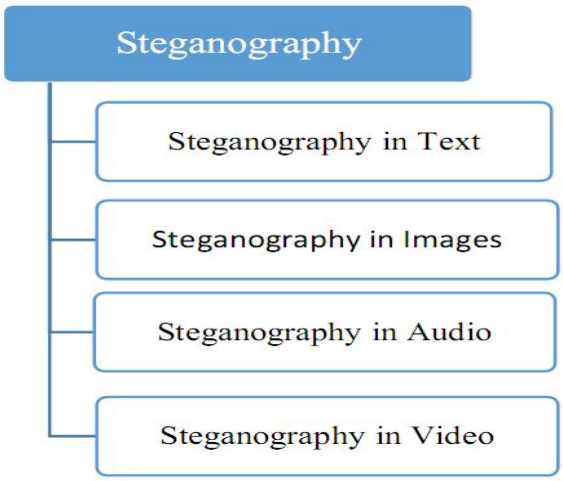
In Image processing for Hiding Information mainly the techniques which are used:



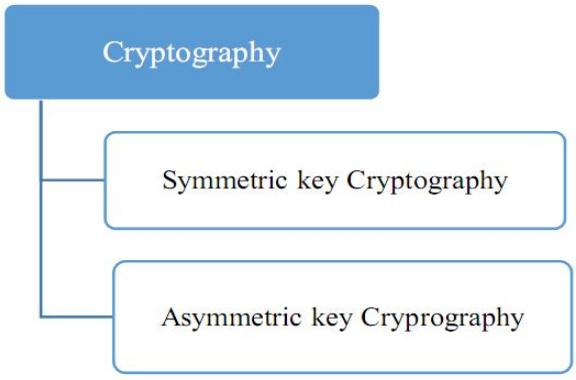
A. Steganography

"Steganography" word is the combination of two Greek words that are "Steganos" (covered or protected) and "graphia" (writing). Steganography is the art of writing hidden data in such a way that no one apart from the sender and intended recipient know about the existence of data.
Example: "Since everyone can read, encoding text in neural sentences in doubtfully effective".
Since everyone can read, encoding text in neural sentences in doubtfully effective.

"Secret Inside"

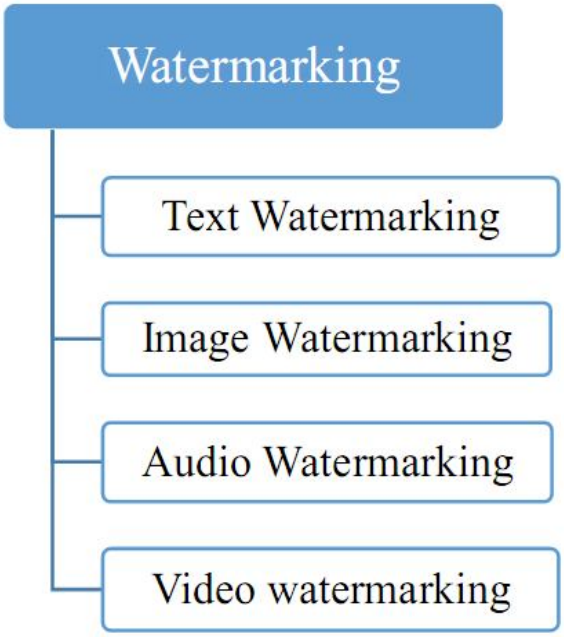


B. Cryptography
"Cryptography" word derived from Greek word "Kyptos" (mean Hidden Secret). Cryptography is the study of hiding the information. It is the art or science of converting original data into secret data code. This technology uses mathematics for encrypt and decrypt data.
In real Life the use of cryptography is to share any secret information when other people are listening.
Cryptography can be classified into two categories.



C. Watermarking
Watermarking is also a technique of hiding the information.Digital watermarking is the technology that provides and ensures security, data authentication and copyright protection to the digital media.[1]
Digital Watermarking can be classified into various categories based upon different parameters.

C.1 Classification of Digital watermarking based upon the host signal



C.1.1 Text Watermarking
In the text watermarking watermark is used to operate as a watermark text image.it can be visible or not. It can be applied in the layout and background of appearances of the image [2].
C.1.2 Image Watermarking
Image watermarking is used to hide any secret information into the image/photo and later this watermark can be detect/extract as proof for author's ownership.
C.1.3 Audio Watermarking
In audio watermarking additional signals are inserted as watermark into the audio signals.
C.1.4 Video Watermarking
In this type of watermarking initially the host video is divided into the different video shots and after that from each shot select one video frame, this video frame in image processing is named as identical frame.
C.2 Classification of Digital watermarking based upon the perceptivity
C.2.1 Visible Watermark
Visible watermarks are those watermarks which are embedded into the content in such a way that they can easily viewed when the content is seen. It can be semitransparent text or image that overspread into the image.
Example- Logo of any television channel which is on the corner of the television screen. Which is easily visible to the viewer.
C.2.2 Invisible Watermark
In Invisible Watermarks the watermark is embedded in such a way that this embedded watermark cannot visible to the viewer just by seeing. But can be detected with the correct decoding tool. It provides to

image authentication and also protect the image from being copied.

III. HOW THE STEGANOGRAPHY AND CRYPTOGRAPHY IS DIFFERENT FROM WATERMARKING

A. Watermarking vs. cryptography

The information hiding technique that is cryptography is totally different from the other information hiding technique that is watermarking. Cryptography technique provides only security by encryption and decryption. Cryptography cannot protect data after decryption but watermarking can protect the data after they are decoded.

B. Watermarking vs. steganography

The technique of hiding the information that is steganography the main aim of it is to hide any information I in any audio or video data V to obtain another new data V' , practically it is indistinguishable from V, by people in such a way that an eavesdropper cannot detect the presence of information I in V'. The main aim of watermarking is to hide any information s in any audio or video data V, to obtain new data V', practically indistinguishable from d, by people, in such a way that can eaves dropper cannot remove or replace S in V'.

IV. ARCHITECTURE OF DIGITAL WATERMARKING

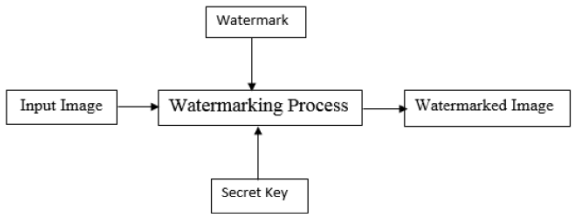


Figure 5 Architecture of Digital Watermarking

A Digital watermarking technique is a technique for embedding the information into an image. Which can be detected later by using some algorithm or code.

A general digital watermarking technique consists two module.

I. Watermarking embedding module

II.Watermarking detection module Watermarking Embedding Module

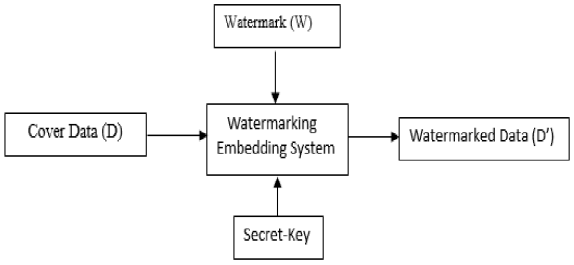


Figure 6 Watermarking Embedding Module

In embedding Module an input algorithm accepts the host and the data is to be embedded and after process it produces a watermarked data.

Watermark detection and extraction module

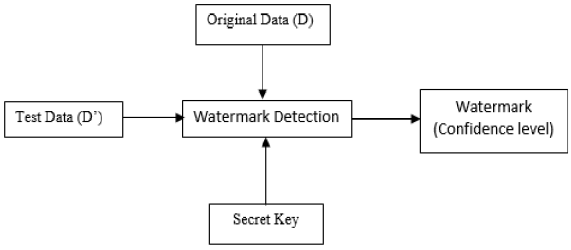


Figure 5 Block Diagram of Watermark extraction module

Watermark extraction is a type of algorithm which is applied to the attacked signal to extract the watermark or confidence measure from it.

V. CLASSIFICATION OF DIGITAL WATERMARKING TECHNIQUES

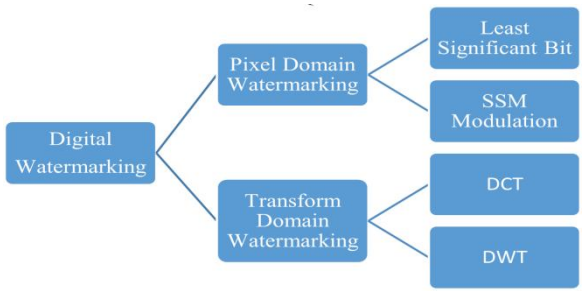


Figure 7 Classification of Digital Watermarking Techniques

Digital watermarking techniques are classified into categories based on the different domains that is Frequency domain or Transform domain watermarking and pixel or spatial domain watermarking.

These techniques are based on their domains are again classified into different categories, that are given above in figure 7.

A. Spatial domain or Pixel domain Watermarking

In spatial domain watermarking, watermark is embedded by directly revamp the pixel values of the host image/videos [2].these methods are generally used in video watermarking. Pixel domain methods are conceptually easy and having very less computational complexities.

There are two types of spatial domain watermarking.

A.1 SSM-Modulation Based Technique

Spread spectrum techniques are methods in which energy is generated at single or more than one discrete frequencies is deliberately spread or distributed in frequency domain or in time domain.

A.2 LSB (Least Significant Bit) technique

Least significant technique is the easiest technique under pixel domain watermarking. The earliest work

of digital watermarking scheme inserts watermarks in the LSB of Pixels. Each pixel is represented by sequence of 8-bit.

Example-

Image	Watermark	Watermarked Image
11110000	1	1111000**1**
00001111	0	0000111**0**
11000011	1	1100001**1**
00111100	0	0011110**0**

B. Frequency Domain or transform domain watermarking technique

As compared to pixel domain watermarking methods the frequency domain is widely used. In transform domain watermarking technique mainly Discrete Fourier Transform and Discrete Wavelet Transform are used. The reason for using frequency domain watermarking is that the characteristics of HVS is better captured by the spectral coefficients. Mainly there are two types of transform that comes under this category.

B.1 DCT (Discrete Cosine Transform)

DCT is generally used in watermarking. This transform provides very accurate result. Discrete cosine Transform represents data in terms of frequency space rather than an amplitude space as Fourier transform [1]. Discrete cosine Transform is faster. In this transform image get decomposed into various band of frequency and mainly focused on middle band of frequency. The reason is in middle band of frequency watermark information can easily embedded so in DCT after decomposition of different frequency band, focused on middle frequency band. Discrete cosine Transform is very important tool for video processing. DCT improves SNR (Signal to Noise Ratio) and it is also more robust to noise.

B.2 DWT (Discrete Wavelet Transform)

Wavelets mean small waves, Discrete Wavelet transform is based upon the small waves which is called wavelets. DWT is the mathematical tool for decomposition of an image and hierarchal. Currently this transform is used in several variety of signal processing application such as Data compression (Audio or video), removing the noise etc. Small Waves that is wavelets which has their energy concentrated in time varying signals.

The advantage of this transform is that it captures both frequency and location information.

VI. COMPARISSION BETWEEN DCT AND DWT

- Discrete wavelet transform has special frequency locality whereas discrete cosine transform are full frame transform.
- DWT is more robust to noise as compared to Discrete Cosine Transform.
- Latest image compression standard JPEG2000 is based on DWT. It is the other advantage of DWT as compared with DCT [2].
- Discrete wavelet transform understand the Human Visual System (HVS) more closely as compared with Discrete Cosine Transform.
- Computation simplicity of discrete cosine transform more than discrete wavelet transform.

VII. COMPARISSION BETWEEN TRANSFORM (FREQUENCY) DOMAIN AND SPATIAL (PIXEL) DOMAIN

S.N.	Parameters	Frequency Domain	Spatial Domain
1.	Capacity	Low	High
2.	Computational Time	More	Less
3.	Computational complexity	More	Less
4.	Robustness	More	Less
5.	Computation Cost	More	Less

VIII. BACKDROPS OF ABOVE MENTOINED WATERMARKING TECHNIQUE SYSTEM

- Insecurity
- Inseparability
- Scope
- Tamper proofing
- Transparency

Fast Hadamard Matrix

The technique that Fast Hadamard Matrix is having various advantages over the other technologies such as DCT, DWT, DFT etc.

- Increased watermark energy that leads to the more robustness.
- Invisibility of watermark guaranteed.
- Less Processing Time.

IX. PROPERTIES OF DIGITAL WATERMARKING

There are many properties of Digital Watermarking. Some of them are given below.

A. CBR

CBR stands to “Constant Bit Rate”. Watermarking should not increase the bit rate in the bit stream domain [2].

B. Imperceptibility

C. The watermark must not degrade the quality of input or original signal, thus it should be invisible to human eyes or inaudible to human ears.

D. Loyalty

A watermark can be considered to be having higher reliability if it is not easy for the viewer to recognize the degradation caused by it.

E. Robustness

Robustness defines the amount of noise or attack tolerable in the system. Watermark should be more robust.

F. Security

The watermark should only be detected by authorized party not any unauthorized party.

X. ATTACKS ON DIGITAL WATERMARKING

There are various types of attacks that are subjected to digital watermarking.

A. Simple Attack

Simple attacks are those attacks in which attempt are made to damage the embedded watermarking during making some modifications and the image without trying to isolate and identify the watermark. These attacks includes additive noise, D to A conversion, Correction, Cropping etc.

B. Removal Attack

Removal Attacks are those attacks in which attempts are made to analyses the watermarked data after estimating the watermark. After that watermark is separated from the original watermarked data to remove it over the object to degrade the watermark to make it undetectable/unreadable.

C. Forgery Attack

Forgery Attacks are those attacks in which the hacker attempts embed a new watermark that is legimate except removing it.

D. Ambiguity Attack

Ambiguity attacks are those attacks in which the attempts are made to confuse the detector by producing a fake/duplicate watermarked data.

E. Subtractive Attack

Subtractive attacks are those attacks in which efforts are made to detect the location, presence of the watermark and to extract it.

F. Collusion Attack:

Collusion attacks are those attacks in which hacker uses various copy of same data with each copy is having various types of watermark to construct a new copy without any watermark.

G. Geometric Attack

All the operations in the image like cropping, rotating, flipping etc. Affects the geometry of the image and should be detectable.

H. Interference Attack

Interference Attacks add the noise (additional noise) to the watermarked object. The example of interference attacks are collusion, remodulation, lossy compression, noise storm, quantization etc.

I. Oracle Attack

A Non-watermark object is constructed when the public watermark detector device is available. Oracle attack is s similar to the Cryptographic attacks.

J. Security Attack

In security attacks suppose watermarking algorithm is known, attacker can again try to do some type of modification to give invalid watermark or to modify the watermark.

K. Image Degradation Attack

Image degradation attacks are those attacks which damage the robust watermarks by removing some parts of image. These parts that are removing, it may contain Watermark information. For example partially cropping, removal of column, removal of row etc. In Image Degradation Attack the noise comes in the picture that is Gaussian Noise.

L. Image Compression

In order to reduce the space in memory and to serve the cost of required bandwidth from transmission of images, images are generally compressed. Due to compression the quality of image may rise to degrade the quality. Generally Image Compression is done by JPEG2000 and JPEG compression techniques. These are lossy compression Methods. These methods are more harmful as compared to other lossless compression methods.

M. Distortive Attack

In distortive attacks an hacker try to apply some distortive transformation over the object to worsen the watermark to make it undetectable.

XI. APPLICATION OF DIGITAL WATERMARKING

A. Authentication

The Aim of this application is to detect the modifications and alternations in a picture. Suppose there is an image of car that has been protected with Digital watermarking technology if the same picture is shown, the some small modifications then say the number on the license plate has been changed. After the watermark detection program on the tampered photo, the tampered area will be indicated in different types of color and then can easily say that the detected area in picture corresponds to the clipped modifications on the original image.

B. DRM

DRM stand to Digital Right Management. DRM can be defined as the description, identification, protecting, monitoring and trading on tracking of all form of usage over intangible and tangible assets.

C. Certification

Certification is the most important for official documents like. Watermarking technology allows to mutually linked content on the documents. It means some information or data is written twice on the document. For example in passport the name of

owner of passport is printed in text and name of passport owner is also hidden as an invisibility watermarked in the photo of the passport owner. So if one will try to make duplicated passport by changing the original photo, it will be easily detected by scanning the passport and verifying the passport owner name hidden in the photo doesn't matter more the name printed on the passport in written text.

D. Copyrighting Protection

The technology that is Digital Watermarking can be used to identify, protect copyright ownership. It inserts the copyright information into the digital object without the loss of quality.

E. Tamper Proofing

Digital watermarking can be used for tamper proofing. Digital watermarks are fragile by nature. Digital content can be inserted with fragile watermark that get destroyed whenever any changes in made to the content. Such type of watermark can be used to authenticate the content.

F. Fingerprinting

In copyright Protection application for fingerprinting watermark is used to trace authorized user who distribute the copyrighted material illegally and violates the license agreement. Thus the embedded information in content is mainly about the customer's identification number.

G. Medical Application

The name of the patient is printed on the medical report such as X-Ray reports and MRI scanning using the visible watermarking technology. For the correct treatment of any patient medical report plays a very important role.

H. Audio/Video Content protection

Modern digital formats employed for sale of commercial audio, video content to the consumers such as CD, DVD, Blu-Ray Disc etc. content protection technology that controls access to and use of content and limit its unauthorized redistribution and copying. Parties are seeking to engage in Distribution of unauthorized and copying of protected commercial audio, video content should circumvent the content protection to obtain the decrypted copy of content.

I. Image and Document Security

Consider the image and documents that are generated in the support of a launch major product. The corporate communication professions faces the significant challenges in the managing channels and very complex sales. Documents and Images are distributed to the agencies, remote offices, distributors etc. and must be managed to ensure the confidential information should not leaked before the launching date.

J. Measurement of Audience

In the world of media instable content consumption, measurements of audience is becoming more and more critical. Beyond the number of peoples are accessing the program, knowing who is watching , how they are engaged with content and though which media is essential for the content providers and broadcasters to better tailor their offering and maximizing impact.

K. Locating Online Content

The volume of any content is being uploaded to web to grow up as more and more on the internet for sharing the information, research and communication. It has also become a primary sale tool and selling environment, providing an opportunity to show our product and services and attract the buyers from around the world [1].

XII. ADVANTAGES AND DISADVANTAGES OF DIGITALW ATERMARKING

Advantages of Digital Watermarking

a) It is easy to embed the watermark.
b) Easily detection of Tampering in image.
c) Identifies the author uniquely.
d) It is possible of implementation on PC platform.

Dis-Advantages of Digital Watermarking

a) It vanishes if anyone manipulates the image.
b) Some operations like compressing, resizing of photo from one type to another type it may lead to diminish the watermark and it may become unreadable.
c) Original watermark is required during the extraction process.
d) It doesn't prevent copying of image but can track down and detect the ownership of copied image file.

XIII. REQUIREMENTS OF DIGITAL WATERMARKING

There are several requirements in Digital watermarking. Which are given below:

A. Security

In Digital Watermarking security means that the watermark must be difficult to extract out or alter without affecting the quality of host signal.

B. Imperceptibility

The watermark should not be noticeable to the human viewer nor should the watermark degrade the quality of content [1].

C. Transparency

The quality of inserted watermark must be very clear and transparent. The insertion of watermark must not diminish the quality of final image.

D. Capacity

It describes the maximum number of bits that can inserted into the image, audio, video. The capacity requirements always struggle again the two other important factor of requirements that is robustness and imperceptibility.

XIV. LIMITATIONS AND CHALLENGES IN DIGITAL WATERMARKING

After performing various researches it is found that in Digital Watermarking there are various technical challenges. For robustness the watermark can added only to the low frequency component of the original signal. Thus the scheme that is Digital Watermarking may become successful if the low frequency components of the original signal is used the host for embedding watermark.

CONCLUSION

Digital Watermarking is very active rapidly evolving field of research and development with various applications. In Digital Watermarking for hiding any message, embedding the signals is done by different algorithm, MATLAB code etc. with algorithm it also contains some Transformations like DCT, DWT, DFT etc. In this field of Image Processing today there is also research is going on for more betterment of robustness, transparent and secure watermarking techniques for different digital media such as images, audio, video. The common requirement application for the watermark is that they resist attacks that will remove it. There is also other technique that is blind watermarking, blind watermarking uses multiple number of watermarks and also there is no need of original image at the watermark recovery. This technology uses watermark encryption and nesting. There are various methods to hide the information, protecting of copyright but from the result of research papers, from the research results, survey it is found that for hiding the data, copyright protection the technology that is “Digital Watermarking” is more effective, simpler, easier technique. And also it is found that Digital Watermarking is more capable, robust because of having better efficiency as compared to other hiding data techniques. Basically Digital watermarking is focusing on providing security to user. In now a days the demand or need of security in raising day by day. Digital Watermarking technique provides security not only image/photo but also for text, audio and video files. Hence can say that Digital Watermarking is the easy and simple technique by using it Data can be protected from unauthorized duplication of data.

REFERENCES

[1] Prabhishek Singh, R S Chadha “A Survey of Digital Watermarking Techniques, Applications and Attacks”, 2013 International Journal of Engineering and Innovative Technology (IJEIT).

[2] Ekta Miglani, Sachin Gupta “Digital Watermarking Methodologies-A survey”, 2014 International Journal of Advanced Research in Computer Science and Software Engineering.

[3] Dr. Ajit, Preeti Kalra, Sonia Dhull “DIGITAL WATERMARKING”, 2013 International Journal of Advanced Research in Computer Science and Software Engineering.

[4] Gurpreet kaur, Kamaljeet kaur “Image Watermarking Using LSB (Least Significant Bit” International Journal of Advanced Research in Computer Science and Software Engineering.

★★★