Volume 4, Issue 11, November 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Survey on Digital Watermarking – A Digital Forensics & Security Application

Sharbani Bhattacharya

Department of Information Technology, IEC-College of Engg & Tech.,

Uttar Pradesh Technical University, Uttar Pradesh, India

Abstract— This article presents an overview of various watermarking types and techniques. This is a survey paper which categories watermarking methods into seven parts. Watermarking method depends upon visibility, document type, robustness , watermarking application areas, various techniques of watermarking, availability of original image for extraction of watermarks and after extraction of watermark. The paper focus on watermarking as digital forensics and security application.

Keywords— Watermarking, Visibility, Digital Forensics , Security, Robustness.

I. INTRODUCTION

Watermark is used for authentication, identification and preservation of originality of an image. There are two concepts watermarking and fingerprinting. Watermarking is for adding or embedding some context to the base image which is used for its identification and authentication. While fingerprinting traces the source of copying the image. Fingerprinting, thus, provides necessary information to enable taking action against piracy of the image or context. On the other hand, watermarking is used for restricting the piracy. Digital watermarking is done in the image, audio, video or other multimedia files. It is also used in forensic department in various ways. In other words, we can also say that fingerprints are embedded in an image by using watermark algorithm. Once the authorized copy of digitized context is available, to identify the series guilty, who created those unauthorized copy can be identified. This is also called forensic watermarking. Another, concept is Visual Cryptography Scheme (VCS). In this process encoded secret image are distributed into n number of shared participants [1]. This is used for watermarking purpose. Reversible Watermarking is also called lossless or distortion free watermarking. It completely removes the watermarking and exactly recovers the original signal image [2]. In forensic analysis sometimes patterns of skin colour are matched to analyse the culprit. Here, various watermarking algorithms with knowledgebase are used to identify the skin colour pigmentation of criminals [3]. In this paper, we have used the concept of visual cryptography, reversible watermarking in small picture like logo or file containing signature of a person. If we can find robust methods for watermarking then in digital media we can authenticate signatures, logo and many important documents.

II. DIGITAL FORENSICS

"Digital forensics has been approached differently for supporting criminal and civil proceedings. The earliest digital forensics support for civil matters was usually focused only on recovering e-mail or financial data whereas criminal investigations took a more in-depth approach to identification, collection, and analysis. As the profession becomes more formalized, the distinction in methodologies used between civil, criminal, and corporate investigations is becoming less differentiated. The collection phase of digital forensics is when evidence to be identified and collected. Normally, these are digital data in the form of disk drives, flash memory drives, or other forms of digital media and data, but they can include corporate security policies and backup methods. The preservation phase of digital forensics focuses on preserving original reliable, complete, accurate, and verifiable digital documents. Cryptographic hashing, checksums, and documentation are all key components of the preservation phase. The reliable, complete, accurate, and verifiable contribute to potential evidence. In this phase investigators will attempt to *filter-out* data which is determined not to contain any desirable evidence and *filter-in* potential evidence. A wide array of tools and techniques are used in this filtering phase, some of which include comparing cryptographic hash values of known good and known suspect files against a known dataset. The final phase of digital forensics is when the potential evidence are presented in a variety of forms. Presentation normally starts with the investigator extracting the evidence from the original media, and then staging and organizing them on CD-ROM or DVD-ROM or pen drive. The investigator's reports, supporting documentation, declarations, depositions, and testimony in court can all be considered the presentation phase of digital forensics" [4]. Here, we are discussing watermarking as an application of digital forensics and for embedding watermark using various techniques.

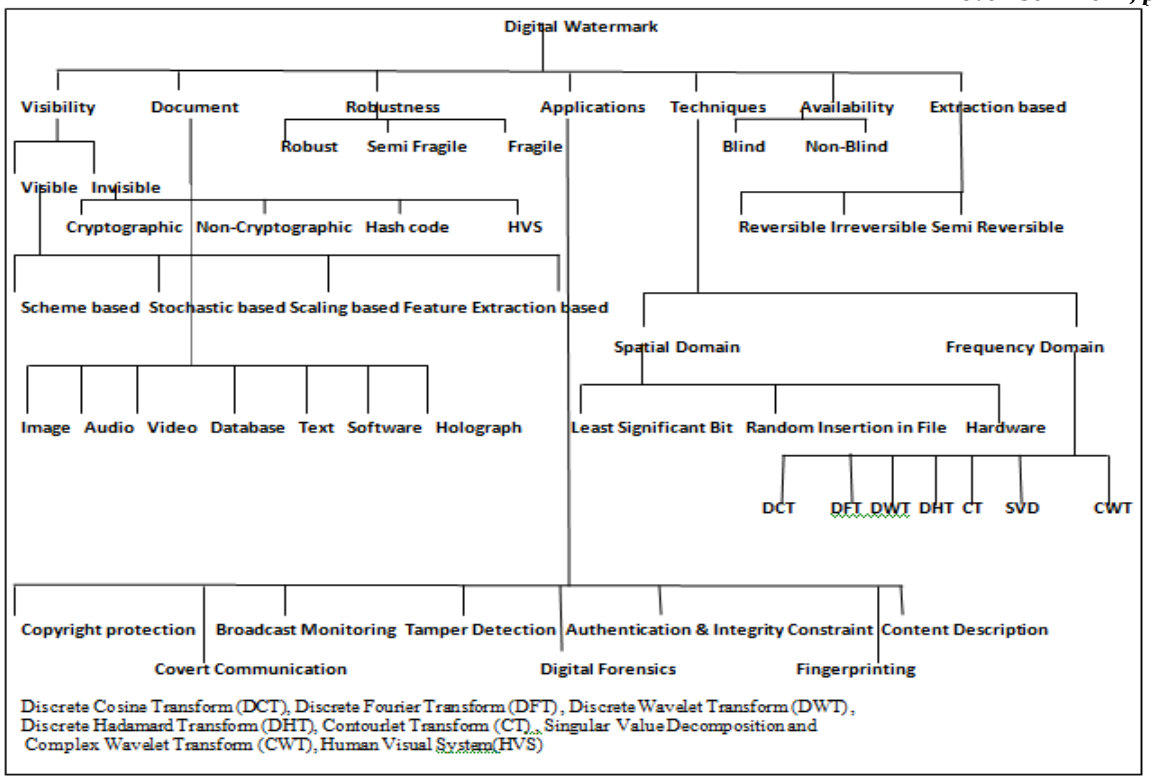

Figure 1 Categorization of various type Watermarking

III. ON THE BASIS VISIBILITY

There are various types of watermarking. In a broader way, we divide it into two categories, viz.

A. Visible
B. Invisible

A. Visible Watermark

These are watermarking used for identification of an image or text embedded in some context. There are various kinds of Visible Watermarking

1) Scheme based Watermarking
2) Stochastic Watermarking
3) Scaling based Watermarking
4) Feature Extraction Watermarking

1) Scheme Based Watermarking

"These are based on some kind of scheme like diagonally visible watermarking throughout the image on a line segment or on the top or bottom of an image" [8].

2) Stochastic Watermarking

Here, watermarking is added to an image using some algorithm and stochastic function like addition, multiplication, mean median mode etc.

Additive watermarking - Cox et al. [5] have proposed an additive watermarking technique which is based on spread spectrum concept which is resistant to noise and cropping attacks [4] and Multiplicative Watermarking [7] are based on using local optimum decoders in Multi resolution transform domains.

3) Scaling Based Watermarking

These are used in image using scaling algorithm i.e. on the basis of size and resolution of an image [9].

4) Feature Extraction Watermarking

Here, certain features or patterns are defined and are used for watermarking [10].

B. Invisible Watermarking

The covert watermarking are those where watermarking is hidden in context. There can be various kinds of covert watermarking.

1. Cryptographic Watermarking
2. Non- Cryptographic Watermarking
3. Hash Code Watermarking
4. Human Visual System Watermarking

1) Cryptographic Watermarking

The watermarking done in this category is in the form of cipher text. It can be algorithm based like RSA, AES, DES or secret key based like public key or private key. Thus, the cipher text is added in the context which needs to be deciphered after retrieval. These kind of watermarking are used in forensic analysis and referred to as forensic watermarking.

2) Non-Cryptographic Watermarking

This watermarking method is hidden in the context. The hidden text, image, program or context is not a cipher text. It is in the readable form but is not visible or easily identified. One needs appropriate program or algorithm or key to extract it from the base image and read it.

3) Hash Code Watermarking

The hash function is created which takes arguments as text file and returns hash code and hash file. Hash file consists of definition of the text file in unreadable format. Hash code and hash file are need to use to get original file from hash file. The hash code is to be embedded in digital content. The authorized party has hash file and extracting hash code can generate original text. The importance of hash code watermarking is various documents are converted into hash code and hash file and only hash code which is small in size is inserted into image. Thus, many hash code can inserted in one image file [20].

4) Human Visual System

"Uniform areas of the image are very sensitive to watermark addition so they only support extremely small embedding depth, whereas edge areas, for instance, support deeper watermark addition. The new spatial masking is built according to the image features such as the brightness, edges, and region activities. With the same watermark embedding, the quality of watermarked image using the proposed adaptive masking is much better than the one without using the adaptive masking. The human visual system has been characterized with several phenomena that permit pixel element adjustments to elude perception".[17].

IV. ON THE BASIS OF DOCUMENT

The documents for digital watermarking is image, audio , video, text, software , databases and holographs.
Digital documents for watermarking is widely divided into various categories like

A. Digital Image Watermarking- An image available in the internet or in primary and secondary storage.
B. Digital Video Watermarking- A video sequence consists of still images. The watermarking is carried out in each image of video and thus whole video is watermarked.
C. Digital Audio Watermarking- Audio watermarking is based on embedding one or more key dependent watermark signals below the audibility threshold.
D. Software Watermarking- Software watermarking is a technique used to protect software from piracy. Software watermarking embeds a unique identifier watermarking S into program P. If S uniquely establishes the author of P then S is considered a copyright notice.
E. Text Watermarking- Text is available in digital media are also prone to be copied. Therefore, hidden text or key is inserted in between letters or words in text. When copied the hidden words are revealed and entire text will changed and become unreadable.
F. Database Watermarking- Databases are also watermarked in order to protect its unauthorized usage.
G. Holographs- Holographs are used for logos and copyright authentication. It is watermarked using 3D visualization.

V. ON THE BASIS OF ROBUSTNESS

Robust method is for identification where semi fragile and fragile is for authentication [5]. In other words, we can say that robust watermarking is also visible. It is used for identification. Semi fragile and fragile is for covert watermarking. Generally, covert watermarking is used for authentication and forensic watermarking. Using covert watermarking unauthorized copying can be traced out from some hidden program embedded in the base image. Watermarking is a valid and useful method for preserving authenticity and authorizing the use of digital image. There are various method of watermarking. Each method has its own pros and cons. Performance of watermarking system is based on three criteria i.e. Invisibility, Robustness and Capacity [12].
Invisibility means watermark should embedded in such a way that it is not identified by unauthorized uses.
Robustness is concerned about tracing or tampering of watermark by attacker. A good watermark should be against filtering process, noise addition, lossy compression, geometry transformation such as rotation, scaling and translation.
Capacity means maximum amount of information the embedded watermark can carry and those information can be detected reliably for the purpose of copyright protection and authentication.
An image authentication system should satisfy following criteria

A. Sensitivity- The system must be sensitive to malicious attacks, tampering, deletion or reduction of watermarking. Modification includes cropping or altering specific part of image.
B. Tolerance- The system must tolerate some loss of information and generally non-malicious manipulation.
C. Reconstruction of altered region- The system may need the ability to restore, even partially, altered or destroyed regions.

D. Localization of altered region- The system should be able to locate precisely any malicious alteration made to the image and verify other areas as authentication.[13].

VI. ON THE BASIS OF APPLICATIONS

There are diverse applications of image watermarking. These are listed as follows .

A. Copyright Protection -When a new image is created, copyright information can be inserted as a watermark. In case of dispute of ownership, this watermark can provide evidence.

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 destroyed or degraded, it indicates presence of tampering and hence digital content cannot be trusted.

D. Authentications and Integrity Verification -Content authentication is able to detect any change in digital content. This can be achieved through the use of fragile or semi-fragile watermark which has low robustness to modification in an image.

E. Fingerprinting -Fingerprints are unique to the owner of digital content and used to identify when an illegal copy appeared where and which point of leakage.

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

G. Covert Communications -It includes exchange of messages secretly embedded within images. In this case, the main requirement is that hidden data should not be identified.

H. *Digital Forensics* -It includes application in forensics science to assure that digital image is doctored or not.

I. Device Control- In this scenario, the media player is controlled by the digital watermark. If the desired copyright information cannot be detected from the host contents, the player refuses to play and record the unauthorized contents. If all device manufacturers abide to these device control policies, the piracy can be discouraged. However, in real scenarios, it is difficult to implement these policies due to the difficulty of global cooperation [22].

VII. ON THE BASIS OF TECHNIQUES

Watermarking algorithms can also be classified based on the domain used for watermark embedding. Accordingly, there are two popular techniques, namely spatial domain watermarking and transform domain watermarking techniques.

A. Spatial Domain Watermarking

This techniques are useful for higher data embedding applications.

1. Least Significant Bit
2. Random Insertion in File
3. Hardware Watermarking

1) Least Significant Bit (LSB)

"The most common method of watermark embedding is to embed the watermark into the least significant- bits of the covert object. LSB substitution also has drawbacks. Although, it can restrain transformations like cropping, any addition of undesirable noise or lossy compression but a more sophisticated attack that could simply set the LSB bits of each pixel to one can fully defeat the watermark with negligible impact on the cover object. Once the algorithm is known to a hacker, the embedded watermark could be easily modified by him without any difficulty'[26].

2) Random Insertion in File (RIF)

"Some small code or text can be randomly inserted in image file which becomes invisible watermark. These watermarks are in general used for digital forensics and security purpose" [27].

3) Hardware based Watermarking-

" A hardware-based implementation is one where the algorithm's operations are fully implemented in custom-designed circuitry. The overall advantage is that hardware consumes less area and less power. In a FPGA based invisible robust spatial domain watermarking. The watermark insertion is carried out by replacing original image pixel value by watermark encoding function. The original image is required for watermark detection "[24][25].

B. Transform Domain Watermarking

This techniques are suitable in applications where, robustness is of prime concern.

"Spread-spectrum techniques are methods in which energy generated at one or more discrete frequencies is deliberately spread or distributed in time. This is done for a variety of reasons, including the establishment of secure communications, increasing resistance to natural".[23].

There are several transform domain watermarking schemes available in the literature.

1) Discrete Cosine Transform (DCT)
2) Discrete Fourier Transform (DFT)

3) Discrete Wavelet Transform (DWT)
4) Discrete Hadamard Transform (DHT)
5) Contourlet Transform (CT)
6) Singular Value Decomposition(SVD)
7) Complex Wavelet Transformation(CWT)

1) Discrete Cosine Transformation (DCT)

"The popular block-based DCT transform segments image non-overlapping blocks and applies DCT to each block. These results in giving three frequency sub-bands: low frequency sub-band, mid-frequency sub-band and high frequency sub-band. DCT-based watermarking is based on two facts. The first fact is that much of the signal energy lies at low-frequencies sub-band which contains the most important visual parts of the image. The second fact is that high frequency components of the image are usually removed through compression and noise attacks. The watermark is therefore embedded by modifying the coefficients of the middle frequency sub-band so that the visibility of the image will not be affected and the watermark will not be removed by compression" [16].

2) Discrete Fourier Transformation (DFT)

"Basically, the Fourier transform is a most popular technique for signal analysis, signal study and synthesis to define the effect of various factors on signal. Sometime, the Fourier transform is use to transform the signal from time domain to frequency domain or signal from frequency domain to time domain. This transformation is reversible and that maintaining the same energy" [18].

3) Discrete Wavelet Transform (DWT)

"Discrete Wavelet Transform (DWT) is a mathematical tool for hierarchically decomposing an image. It is useful for processing of non-stationary signals. The transform is based on small waves, called wavelets, of varying frequency and limited duration. Wavelet transform provides both frequency and spatial description of an image. Unlike conventional Fourier transform, temporal information is retained in this transformation process. Wavelets are created by translations and dilations of a fixed function called mother wavelet. This section analyses suitability of DWT for image watermarking and gives advantages of using DWT as against other transforms. For 2-D images, applying DWT corresponds to processing the image by 2-D filters in each dimension".[16].

4) Discrete Hadamard Transform

"The Hadamard transform is a non-sinusoidal, orthogonal transformation that decomposes a signal into a set of orthogonal, rectangular waveforms called Walsh functions. The transformation has no multipliers and is real because the amplitude of Walsh (or Hadamard) functions has only two values +1 or -1. The Hadamard matrix is a square array of plus and minus ones whose rows (and columns) are orthogonal to one another. If H is an N x N Hadamard matrix then the product of H and its transpose is the identity matrix. Hadamard transformation not only offers a significant advantage in shorter processing time and ease of hardware implementation but also has more useful middle and high frequency bands available, for hiding the watermark"[14].

5) Contourlet Transform (CT)

"CT gives two important properties [14].
- Directionality. The representation should contain much more directions.
- Anisotropy. To capture smooth contours in images, the representation contains basis elements using a variety of elongated shapes. These two properties are useful for image compression, image watermarking, and Content Based Image Retrieval" [19].

6) Singular Value Decomposition (SVD)

"SVD as a general linear algebra technique is used in a variety of applications. SVD is an optimal matrix decomposition in a least square sense packing the maximum signal energy into a few coefficients as possible (Ganic *et al* 2003) and (Liu & Tan 2002). The SVD theorem decomposes a digital image A of size $M \times N$, as: $A = USVT$, (1) where U and V are of size $M \times M$, and $N \times N$ respectively. S is a diagonal matrix containing the singular values. In watermarking trial, SVD is applied to the image matrix; then watermark resides by altering singular values (SVs)" [15].

7) Complex Wavelet Transform (CWT')

has been introduced as an efficient approach to shift invariant properties. This transform gives much better directional selectivity when it uses the multi-dimensional signal filtering. Some useful properties of CWT have been emphasized as:
• Approximate shift invariance.
• Good directional selectivity in two-dimensions (2D) with Gabor-like filters (also true for higher dimensionality, m-D).
• Perfect reconstruction (PR) using short linear-phase filters (Selesnick & Li 2003)".

VIII. ON THE BASIS OF AVAILABILITY OF ORIGINAL IMAGE

Based on the availability of the cover image and watermark image at the receiver, the watermarking schemes are classified as

1. Blind (oblivious)
2. Non blind (non oblivious)

"A watermarking technique is said to be blind, if it does not require original image to recover the watermark from the watermarked image. Conversely, a watermarking technique is said to be nonblind , if it needs original image for extracting the watermark from the watermarked image. The blind technique is also referred as oblivious. The non-blind watermarking systems are more robust than blind watermarking systems due to availability of original cover image at the time of detection. However, blind or oblivious watermarking systems are more popular. The oblivious watermarking systems decrease the overhead of cost and memory for storing original images" [21].

IX. ON THE BASIS OF EXTRACTION

There are various kind of watermark. After removal of watermark there are three kinds of situation one is original image is completely retrieved i.e. reversible, semi reversible i.e. little bit tampered or completely tampered i.e. irreversible.

X. CONCLUSIONS

There are various types watermarks and these have uses and applications. It depends upon which application area one is looking for according to that watermark type is chosen. There are mix and match of techniques, applications and documents on which watermarking are categorized and studied. This paper shows an overview of various kinds of watermark and its implementation area.

REFERENCES

[1] IEEE Transactions on Information Forensics and Security, vol. 6, no. 2, June 2011 307 Embedded Extended Visual Cryptography Schemes Feng Liu and Chuankun Wu.

[2] IEEE Transactions on Information Forensics and Security, Vol. 6, No. 3, September 2011 873 Improved Embedding for Prediction- Base Reversible Watermarking Dinu Coltuc, Member, IEEE.

[3] IEEE Transactions on Information Forensics and Security, vol. 6, No. 3, September 2011 Using a Knowledge-Based Approach to Remove Blocking Artifacts in Skin Images for Forensic Analysis.

[4] L.T. Brown ,(2006) "Computer Evidence and Collection Preservtation and Preservation" , Thomson/Delmar Learning. Published by Charles River Media, Inc.

[5] I. Cox, J. Kilian, F. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia," IEEE Trans. Image Process., vol. 6, no. 12, pp. 1673–1687, Dec. 1997.Mohammad Ali Akhaee,

[6] S. M. E. Sahraeian, M. A. Akhaee, and F. Marvasti, "Distribution independent blind watermarking," in Proc. IEEE Int. Conf. Image Processing, Cairo, Egypt, Nov. 2009, pp. 125–128.

[7] M. Barni, F. Bartolini, A. De Rosa, and A. Piva, "A new decoder for the optimum recovery of non additive watermarks," IEEE Trans. Image Process., vol. 10, no. 5, pp. 755–766, May 2001.

[8] S. M. E. Sahraeian, M. A. Akhaee, and F. Marvasti, "Distribution independent blind watermarking," in Proc. IEEE Int. Conf. Image Processing,Cairo, Egypt, Nov. 2009, pp. 125–128.

[9] J. Seitz, Digital Watermarking For Digital Media. Arlington, VA: Information Resources, 2005.

[10] C.-W. Tang and H.-M. Hang, "A feature-based robust digital image watermarking scheme," IEEE Trans. Signal Process., vol. 51, no. 4,pp. 950–959, Apr. 2003.

[11] Mohammad Ali Akhaee, Sayed Mohammad Ebrahim Sahraeian Craig Jin "Blind Image Watermarking Using a Sample Projection Approach", IEEE Transactions on Information Forensics and Security, vol6 No3 Sep 2011.

[12] A Survey of RST Invariant Image Watermarking Algorithms**,** Dong Zheng, Yan Liu, Jiyang Zhao, and Abdulmotelab El Sadikk **,***University of Ottawa* ACM Computing Surveys, Vol. 39, No. 2, Article 5, Publication date: June 2007.

[13] A Survey Watermarking Algorithm for image Aurhentication, EURASIP Journal on Applied Signal Processing 2002: Hindawi Publishing Corporation by Christian Ley & Jean Luc Dugeley.

[14] Franklin Rajkumar.V Manekandan.GRS V. Santhi, (2011), "Entropy based Robust Watermarking Scheme using Hadamard Transformation Technique", International Journal of Computer Applications (0975 – 8887) ,Volume 12– No.9, January 2011.

[15] A Mansouri, A Mahmoudi Aznaveh And F Torkamani Azar ,"SVD-based digital image watermarking using complex wavelet transform'Vol. 34, Part 3, June 2009, pp. 393–406.

[16] Navnidhi Chaturvedi1, Dr.S.J.Basha2, "Comparison of Digital Image watermarking Methods DWT & DWT-DCT on the Basis of PSNR",
International Journal of Innovative Research in Science, Engineering and Technology *Vol. 1, Issue 2, December 2012* IJIRSET www.ijirset.com Page no 147.

[17] Sameh Oueslati1 and Adnane Cherif1 and Bassel Solaiman ,"Maximizing Strength Of Digital Watermarks Using Fuzzy Logic", Signal & Image Processing : An International Journal(SIPIJ) Vol.1, No.2, December 2010.

[18] Awanish Kr Kaushik ,"A Novel Approach for Digital Watermarking of an Image Using DFT", International Journal of Electronics and Computer Science Engineering 35 Available Online at www.ijecse.org *ISSN-2277-1956*, ISSN- 2277-1956/V1N1-35-41.

[19] Kilari Veera Swamy 1 B.Chandra Mohan 2 Y.V.Bhaskar Reddy 3 S.Srinivas Kumar, "Image Compression Watermarking Scheme Using Scalar Quantization", International Journal of Next Generation Network,(IJNGN), Vol 2, No.1 , March 2010.

[20] Sharbani Bhattacharya(2014) , "Watermarking Digital Images Using Fuzzy Matrix Compositions and Fuzzy Max-n-Min Set", accepted in International Journal of Advanced Computing, Recent Science Publications, United Kingdom. ISSN Number : 2051-0845 assigned by The British Library, UK.

[21] Nisar Ahmed Memon (2010), "Watermarking of Medical Images of content Authentication and Copyright Protection", PhD Thesis.

[22] Jidong Zhong, (2006) "Watermark Embedding and Detection" , PhD Thesis.

[23] Manpreet Kaur, Sonika jindal and Sunny Behal, "A study on Digital Watermarking",International Journal of Research Engineering & Applied Sciences, Volume 2 , Issue 2 2012.

[24] Nebu John Mathai, Deepa Kundur,and Ali Sheikholeslami, "Hardware Implementation Perspectives of Digital Video Watermarking Algorithm", IEEE Transaction on Signal Processing, Vol 51, No.51 April 2003.

[25] Elias Kougianos, Saraju P. Mohanty, Rabi N. Mahapatra," Hardware Assisted Watermarking for Multimedia", Elsevier, November 2007.

[26] Puneet Kr Sharma and Rajni," Analysis of image Watermarking Using Least Significant Bit Algorithm", International Journal of Information Sciences and Techniques (IJIST) Vol.2, No.4, July 2012.

[27] Sharbani Bhattacharya , "Additive Watermarking in Optimized Digital Image" in **IEEE Beacon**, IEEE (Delhi Section) publication in March **2012** Volume 31 No.1 , Page 79 www.ieeebeacon.com.

