WATERMARK EMBEDDING AND EXTRACTING SCHEME FOR STANDARD TEST IMAGE IN SPATIAL DOMAIN

Pardeep Kajal*

Kamaldeep Jangra*

Deepak Verma***

Abstract

Digital watermarking has gained a lot of importance for digital media recently. It deals with hiding secret bits of information with a digital content as a cover. This is very useful for many applications like copyright control, authenticity of documents, captioning, broadcast monitoring etc. Various techniques for watermarking have been proposed in the recent past. In the first part of this paper we introduce an overview to digital watermarking: The general framework, its embedding process and extraction process of watermarking scheme. In the second part we introduce an overview of watermarking in spatial domain. We define LSB invisible watermarking scheme for embedding and extraction of watermark in standard test image. We add the noise in watermarked image and calculate the value of MSE and PSNR at different levels. At the receiver end we extract the watermark from the watermarked image. Finally we introduce human visual system.

Keywords: Watermarking, spatial domain, Gaussian noise, salt & pepper noise, human visual system, LSB, n LSB-MSB

* Jind Institute of Engineering, Jind, Haryana.

*** RPIIT, Bastara, Karnal, Haryana.

I INTRODUCTION

With the ever-growing expansion of digital multimedia and the Internet digitizing of visual data such as images and video has become increasingly popular. However, this advancement in technology has double impact While, on one hand, it has enabled faster and more efficient storage, transfer and processing of digital data; on the other hand, duplication and manipulation of digital contents has also become very easy and undetectable., which enable fast and error-free movement of any unauthorized digital data and possibly manipulated copy of such information, grow in popularity in the recent years, security concerns over copyright protection of digital multimedia data have also been increasingly emphasized. One of the most promising solutions appears to add author information (watermark) into the visual data as a secondary signal that is not perceivable and is bonded so well with the original data that it is undividable[10] Techniques to embed and recover such secondary information, or stamps (called watermark) is digital watermarking.

II DIGITAL WATERMARKING

Digital watermarking emerged as a tool for protecting the multimedia data from copyright infringement. "Digital Watermarking can be defined as a technology of embedding watermark with intellectual property rights into images, videos, audios and other multimedia data by a certain algorithm." This kind of watermark contains the author and the user's information, which could be the owner's logo, serial number or control information. Digital Watermarking is very common in our daily lives; watermarking in currency, government documents, stamps and many other common documents detection of the watermark. The main use of watermarking is to provide a level of confidence about the authenticity or ownership of a document. The basic idea in watermarking is to add a watermark signal to the cover image to be watermarked image such that the watermarked signal is reserved and secure in the signal mixture but can partly or fully be recovered from the signal mixture later on if the correct cryptographically secure key needed for recovery is used.

Embedding Process -The standard process of invisible data watermarking is given as:

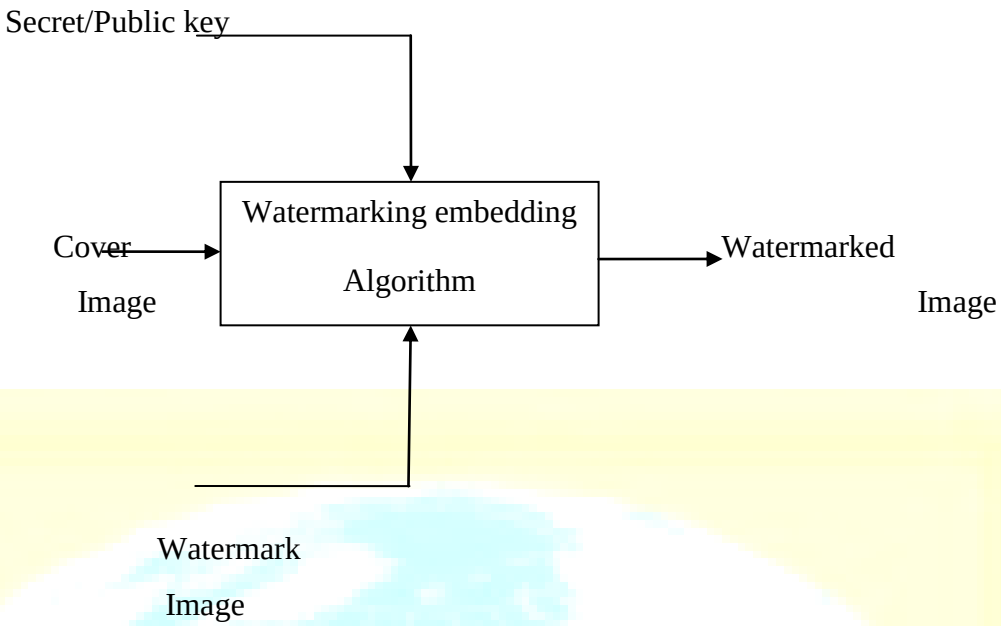

Figure 1 Watermarking Embedding Scheme

As we can see Figure 1 in the defined system the first work is to get the watermarked image and the cover image. After this to store data will be converted to the raw data format i.e. Represent bit system. Now the actual watermarking approach will be defined to hide data over the image. Finally we will get the output watermarked image. In data conversion the given data is converted into its binary values and those binary values are changed into numeric streams because if a hacker tries to get the data behind the image it cannot be understandable to him this process makes the project more secured.

Extraction Process-In watermarked image with data hidden inside in which the hidden data is extracted by giving a correct watermark image the watermark image the extracted data will be in the form of numeric stream so they are converted into binary values and using those binary values the data is formed. In this extraction process the first work is to extract the watermarked image.

Now perform the algorithm in reverse order to scan it and to retrieve the data back. Once the data is retrieved in binary format the will be stored to the specified location.

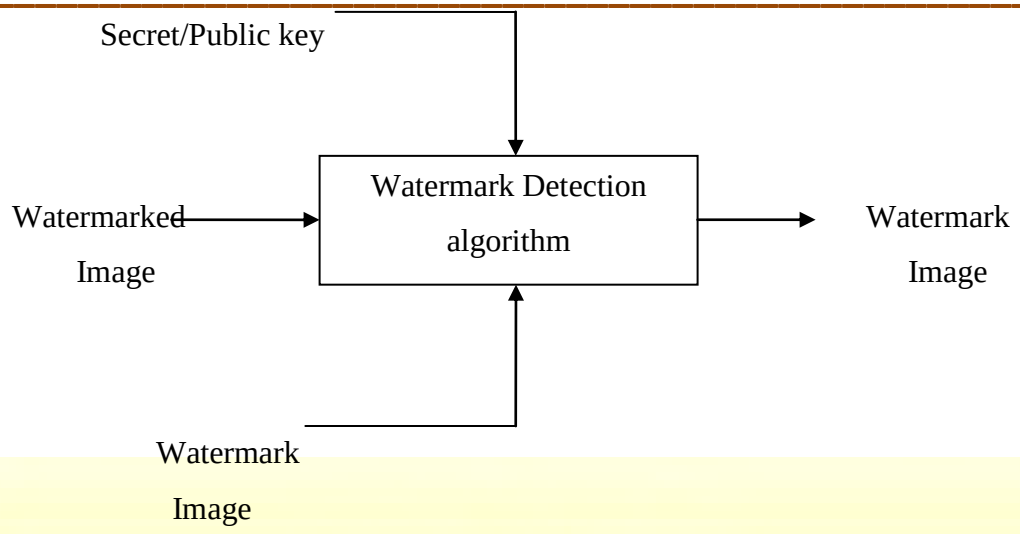

Figure 2 Watermarking Detection Scheme

II SPATIAL DOMAIN TECHNIQUES SCHEMES

Spatial domain watermarking slightly modifies the pixels of one or two randomly selected subsets of an image. Modifications might include flipping the low-order bit of each pixel. However, this technique is not reliable when subjected to normal media operations such as filtering or loss compression [7]

Least Significant Bit Coding (LSB)

One of the techniques in digital watermarking is in spatial domain using two dimensional arrays of pixels in the container image to hold hidden data using the least significant bits (LSB) method. Note that the humane eyes are not very attuned to small variance in colour and therefore processing of small difference in the LSB will not noticeable.

Embedding of invisible watermark

n LSB-MSB hiding algorithms Where n is the number of bits used. In LSB-MSB algorithms, the least significant bits of the original image is masked and Substituted by the most significant bits of the watermark image. It is quite obvious that smaller the value of n, lesser is the deterioration in the quality of the image. As we increase the number of bits, the image quality further degrades and becomes more visible to the naked eye**.**

Algorithm for LSB embedding watermarking scheme

(1) Read image i.e. cover image.

(2) Calculate its size let $m_1 * m_2$.

(3) Read watermark image i.e. CS image.

(4) Calculate its size let $n_1 * n_2$.

(5) If the $((n_1 * n_2) > (m_1 * m_2))$

Print (watermark not fit in to cover image.

Else

(6) Set the LSB of cover image to the value of the MSB of watermark image.

(7) Add Gaussian noise in watermarked image.

(8) Add salt & pepper noise in watermarked image.

(9) Calculate MSE and PSNR between cover image and watermarked image.

(10) Calculate MSE and PSNR between cover image and watermarked image with Gaussian noise.

(11) Calculate MSE AND PSNR between cover image and watermarked image with salt and pepper noise.

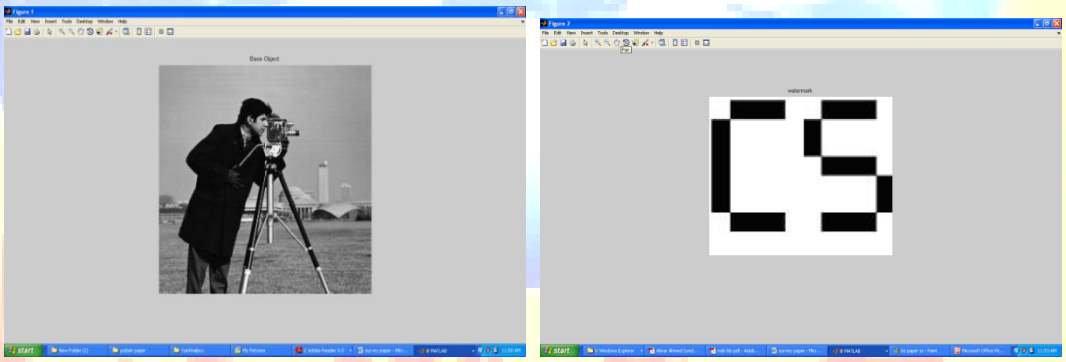

Figure 3(a) Cover Image (b) Water Mark Image

Figure 4 Water Marked Image Using Bit 1

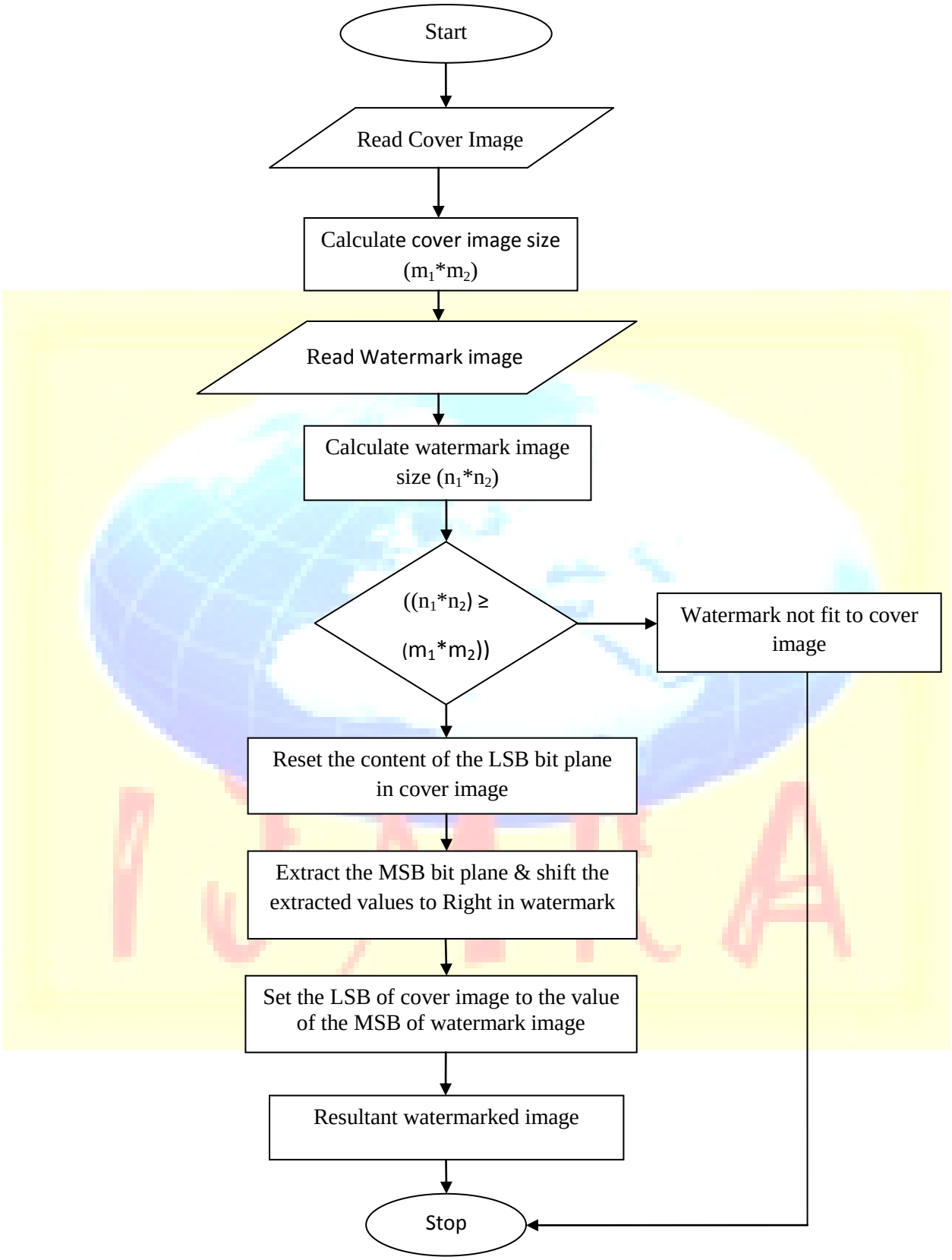

Figure 5 Flow Chart of LSB Watermark Embedding

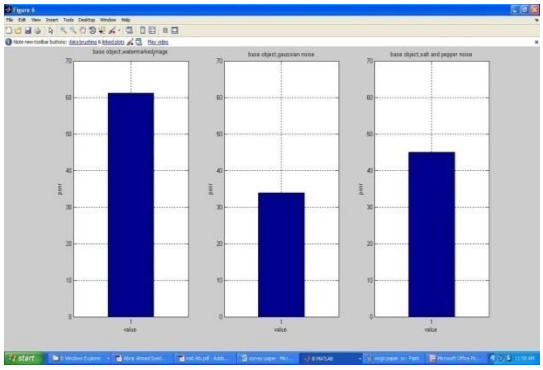

Figure 6 PSNR Graph Using bits 1.

This shows psnr of watermarked image without any attack ,psnr of watermarked image with gaussian noise and psnr of watermarked image with salt&pepper noise.

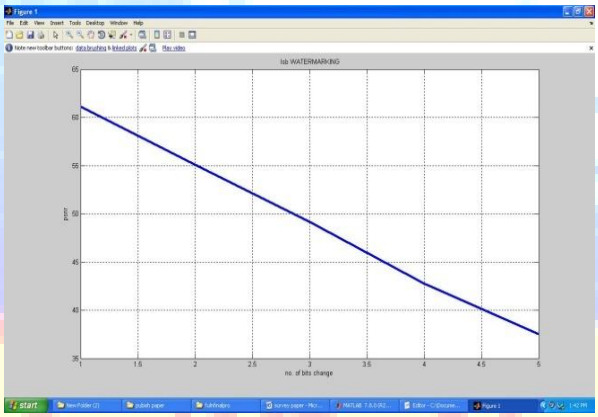

Figure 7 PSNR v/s number of using bits.

Approaches	Watermarked Image without any attack	Watermarked image with Gaussian noise		Watermarked image with Pepper &salt noise		
	MSE	PSNR	MSE	PSNR	MSE	PSNR

1 LSB-MSB	0.050	61.11	26.95	33.82	2.025	45.05
2 LSB-MSB	0.201	55.08	26.92	33.83	2.117	44.87
3 LSB-MSB	0.788	49.16	26.51	33.89	2.660	43.88
4 LSB-MSB	3.446	42.75	25.75	34.02	5.201	40.96
5 LSB-MSB	11.54	37.50	23.87	34.35	12.95	37.00

Figure 8 Result Analysis

This figure shows that when we increase numberof using bits then the value of psnr is decreases.

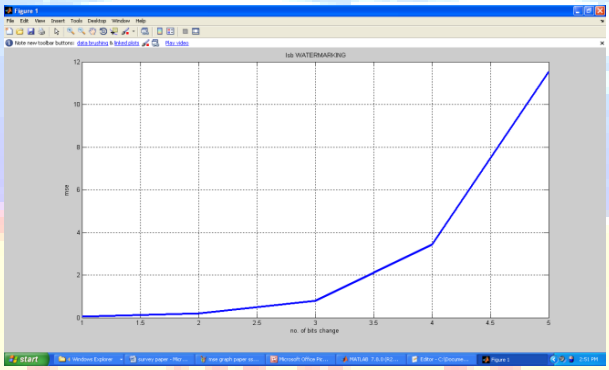

Figure 9 MSE v/s number of using bits.

This figure shows that when we increase numberof using bits then the value of psnr is increases.

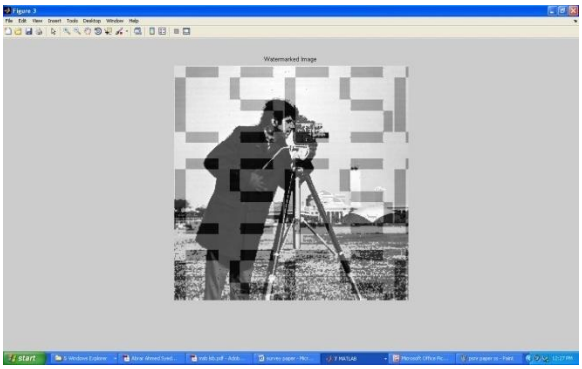

Figure 10 Watermarked Image, using bits=5

This is a visible watermarking scheme, both base and watermark images are seen in the watermarked image.

Extraction of watermark:-after embedding the watermark in the cover image it is necessary to extract the watermark from the watermarked image.

Algorithm for LSB extraction watermarking scheme

(1)Read image i.e. watermarked image.

(2) Calculate size i.e. $m_1 * m_2$.

(3) Read image i.e. watermark image.

(4) Calculate size i.e. $n_1 * n_2$.

(5) Get the LSB of watermark image.

(6) Read resultant image i.e. extracted watermarked image.

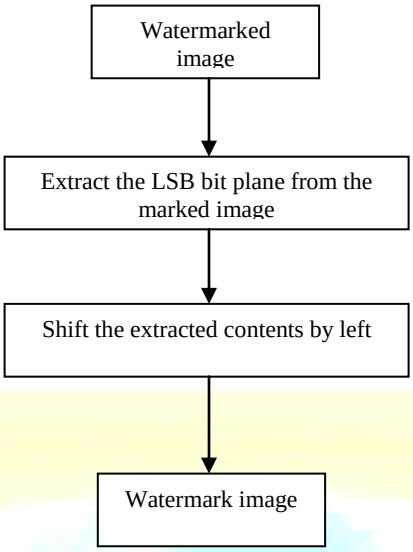

Figure 11 Flow Chart of LSB Watermark Extraction

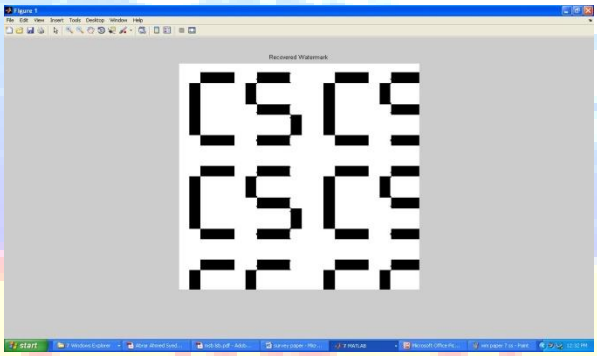

Figure 12 Extracted watermark.

Parameters for Evaluation of a Watermarking technique

Peak Signal to Noise Ratio (PSNR) is hugely used in image compression and image modification where the signal is the original data and the noise is the error introduced by compression. For images, the definition of the PSNR is the same except the Mean Squared Error (MSE) is the sum over all squared value differences divided by image size and by three. When two images are

identical, the Mean Squared Error will be zero. So, PSNR will be undefined. It is expressed in logarithmic decibel scale. Here, the calculation of Mean Squared Error and Peak Signal to Noise Ratio is done for different color levels when watermarked image without any attack, watermarked image with Gaussian noise and watermarked image with salt &pepper noise.

The peak signal to noise ratio (PSNR) is used to evaluate the image quality by calculating the mean square error (MSE) between the images to compare.

$$MSE = \frac{1}{N}\sum (X_P - Y_P)^2$$

Where p is the unity of N pixels in the image. X and Y are the grayscale of the images to compare. With above information we calculate PSNR by equation where X max is max luminance (i.e. For 8-bit image, X max = 255).

$$PSNR = 10\log_{10}\frac{(X\ \max)^2}{MSE}$$

We calculate PSNR between original watermark and watermark that is extracted from host image after attack. The higher the PSNR shows the better quality of extracted watermark. So, if we have bigger PSNR, it shows least difference between original and extracted watermark and more robustness against attack.

REFERENCES

[1] Samanta, S. Dutta, S. Sanyal, **"An Enhancement of Security of Image using Permutation of RGB- Components"** Electronics Computer Technology (ICECT), Proceedings of 3rd International Conference, Volume 2, Page: 404-408, 2011.

[2] Dubolia, R.Singh, Bhadoria, SS Gupta, **"Digital Image Watermarking By Using Discrete Wavelet Transform and Discrete Cosine Transform and Comparison"**, Communication Systems and Network Technologies (CSNT), Proceeding of International Conference, Page: 593-596,2011.

[3] J. Jeedella and h. Al-ahmad, **"An algorithm for watermarking mobile phone color images bch Using code"**, GCC Conference and Exhibition (GCC), 2011 IEEE, Publication Year: 2011, Page: 303 -306

[4] Manjit Thapa, Dr.Sandeep Kumar Sood, A.P Meenakshi Sharma, **"Digital Image Watermarking Technique Based on Different Attacks"** JACSA - International Journal of Advanced Computer Science and Applications, Volume 2, page 14-19,2011.

[5] Guo, Chengqing; Xu Guoai; Niu Xinxin; Yang Yixian Li Yang, **"A Color Image Watermarking Algorithm Resistant to Print-Scan"** Wireless Communications, Networking and Information Security (WCNIS), 2010 IEEE International Conference, Issue Date: 25-27 June 2010, page: 518-521

[6] Satyanarayana Murty, Dr.P. Rajesh Kumar, **"A Robust Digital Image Watermarking Scheme Using Hybrid DWT-DCT-SVD Technique "**Journal of Computer Science and Network Security (2010), Volume: 10, Issue: 10

[7] Na Li Xiaoshi, Zheng, Yanling Zhao, Huimin Wu , Shifeng Li ,**"A Robust Algorithm of Digital Image Watermarking Based On Discrete Wavelet Transform"**, Electronic Commerce and Security, 2008 International Symposium, Issue Date: 3-5 Aug. 2008, page: 942 - 945

[8] Khaled Mahmoud, Sekharjit Datta & James Flint, **"Frequency Domain Watermarking "**The International Arab Journal of Information Technology, Vol. 2, No. 1, January 2005

[9] Yongjian hu , sam kwong and jiwu huang, **"Using invisible watermarks to protect visibly Watermarked images"** Circuits and Systems, 2004, ISCAS'04. Proceedings of the 2004 International Symposium, Volume: 5, Publication Year: 2004, Page: V-584 - V-587

[10] M.Xiufen Liu, Fraunhofer IPK Berlin, Germany, **"Content-Based Watermarking using Image Texture Koppen"**, Signal Processing, 2002 6th International Conference, Volume: 2, Publication Year: 2002, Page: 1576-1579

[11] Jiang Du, Choong-Hoon Lee, Heung-Kyu Lee, Youngho Suh, **"BSS A New Approach for Watermark Attack"**, Multimedia Software Engineering, 2002, Fourth International Symposium, Issue Date: 2002, page: 182-187.

[12] Tsai Cheng LiChih Kai Chuang**, "High Adaptive Multiple-Encryption of Hidden Information Technology "**IEEE Transactions, Issue Date**:** Aug 2000, Volume: 46 Issue: 3, page: 415-421