International Journal of Engineering Research and General Science Volume 4, Issue 1, January-February, 2016
ISSN 2091-2730

Secure Multimedia Data using Digital Watermarking: A Review

Varsha Yadav*, Prof. Neha Verma**

M.Tech Research Scholar*, Department of Electronics & Communication, Trinity Institute of Technology & Research

emailvarshayadav@gmail.com*, 8602560028*

Abstract— Due to the excessive use of multimedia application in our daily life it becomes very much crucial for us to secure our multimedia information and copyright protection. Digital watermarking is a technique which is used to protect the information from illegal allocation of audio, video or image. This technique is used in so many applications such as authentication, copyright protection, medical application etc. Various techniques has been developed yet to protect the copyright information and also for authentication like wavelet transform, least significant bit(LSB), SVD and SVD-DWT etc. In this paper we present the literature study about previously work done and also discuss the benefits and drawbacks of the digital watermarking techniques with their explanation.

Keywords— Watermarking, DWT, LSB, Copyright, Authentication, DFT, PSNR

INTRODUCTION

Few year earlier, there have seen an outburst in the make use of digital media. Industry is making noteworthy investments to transport digital audio, image, and video information to consumers and clients. A novel infrastructure of digital audio, image, and video recorders and players, on-line services and electronic business is hastily being deployed. At the same time, major corporations are converting their audio, image, and video library to an electronic form. Digital media suggest numerous different benefits over analog media: the worth of digital audio, image, and video signals is higher than that of their analog counterparts. Editing is simple because one can access the accurate discrete locations that should be changed. Copying is simple with no loss of loyalty. A copy of a digital media is identical to the original. Digital audio, image, and videos are simply transmitted over networked information systems.
These benefits have opened up many novel possibilities. Generally, it is probable to hide data (information) inside digital audio, image, and video files. The information is secreted in the sense that it is perceptually and statistically imperceptible. With many methods, the concealed information can still be improved if the host signal is compressed, edited, or transformed from digital to analog layout and back.

Digital data embedding has many applications. Foremost is submissive and vigorous copyright protection. Most of the inherent advantages of digital signals enhance tribulations associated with copyright enforcement. For this reason, originators and distributors of digital data are hesitant to make available access to their intellectual property. Digital watermarking has been proposed as a means to recognize the owner or distributor of digital data [1]. As per the entrenching domain of the host image, digital image watermarking system can be classified into two domains namely spatial and transform domain. The easiest method in the spatial domain methods is to put in watermark image pixels in the least significant bits of the host image pixels [2]. In capability of data hiding is high in these methods but barely vigorous. Watermarking in transform domain is more protected and vigorous to different attacks. In frequency domain, watermark is not added to the image intensities or pixels, but to the values of its transform coefficients. After that to get the watermarked image, one should carry out the transform inversely. It consists of DCT (Digital Cosine Transform), DFT (Digital Fourier Transform), and DWT (Digital Wavelet Transform). The process of watermarking for digital data is shown in fig. 1.

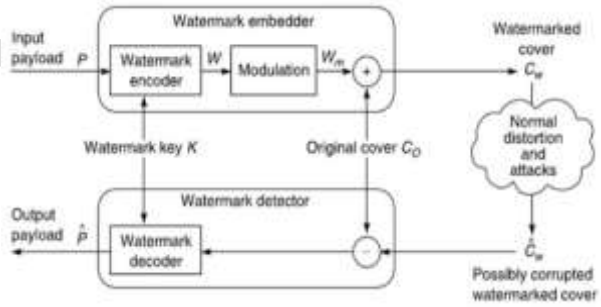

Fig.1 Digital watermarking process

Characteristics of digital watermarking

The watermarking provides different features to protect multimedia data which is describing below:

A. Robustness

A digital watermark is called "fragile" if it be unsuccessful to be noticeable after the slightest alteration. Fragile watermarks are generally used for tamper discovery (integrity confirmation). A digital watermark is called semi-fragile if it contests temperate transformations, except not succeed exposure after malevolent transformations. Semi-fragile watermarks generally used to perceive malevolent transformations.

B. Perceptibility

A digital watermark is called discernible if its presence in the discernible signal is conspicuous (e.g. Digital On-screen graphics like a network logo, content virus codes, opaque images). On videos and images, a few are made apparent/translucent for convince for people due to the actuality that they block segment of the view.

C. Capacity

The length of the embedded message concludes two dissimilar major modules of digital watermarking schemes: The message is theoretically zero-bit long and the system is considered in order to sense the presence or the absence of the watermark in the noticeable object.

D. Embedding method

A digital watermarking method is referred to as spread-spectrum if the marked signal is obtained by an additive amendment. Spread-spectrum watermarks are known to be discreetly robust, although also to have a low information capability due to host interference.
Digital watermarking method is used in different applications such as copyright protection, source tracking, broadcast monitoring, video authentication and software crippling. The objective of this paper is to present the review of literature of previously work done to hide or secure digital data. We also discuss watermarking technique with their advantages and disadvantages. The rest part of the paper, we arrange in this way: In section II literature survey about the previous work done is discussing. In section III explaining different digital watermarking scheme. In section IV discusses the different performance measuring parameter and in last section gives overall conclusion of the paper.

RELATED WORK

Akter et al. [3] anticipated a novel embedding algorithm (NEA) of digital watermarking. The algorithm is executed for digital image as data. The performance is evaluated for NEA and well established Cox's modified embedding algorithm. The watermarking is based on discrete wavelet transforms (DWT) and discrete cosine transforms (DCT). The reception of the novel algorithm is measured by the two necessities of digital watermarking. One is imperceptibility of the watermarked image, measured by peak signal to noise ratio (PSNR) in dB; an additional one is robustness of the mark image, measured by correlation of source mark image and recovering mark image. Now a 512×512 gray scale "Lena" and "Cameraman's" image is taken as host images, and a 128×128 gray scale image is taken as smudge image for 2 level of DWT. The simulation consequences for dissimilar attacking conditions such as salt and pepper attack, Additive White Gaussian Noise (AWGN) attack, jpg compression attack, gamma attack, histogram attack, cropping attack and sharpening attack etc. Subsequent to dissimilar attacks the changing tendency PSNR for both algorithms are comparable. However the mean square error (MSE) value of NEA is forever less than Cox's modified algorithm, which means that after embedding the amendment of the host image property lower for NEA than Cox's algorithm. From the simulation consequences it can be said that NEA will be a replacement of modified Cox's algorithm with better performance ***Singh et al. [4]*** proposed as a novel method to entail ownership verification and defend data from tempering by illegitimate user. To make digital watermarking more proficient digital signature or message authentication code is inserted in the whole message. This paper proposed a method using both Digital Watermarking and Signature so that data reliability can be demonstrated at the receiver end of the network.

Zafar et al. [4] recommended that, the progressing world of digital multimedia communication is faces troubles related to protection and legitimacy of digital data. In the context of multimedia communication, digital images and videos have abundant applications in entertainment world like TV channel broadcasting. Digital watermarking Algorithms used to defend the copyright of digital images and to authenticate multimedia data security. Most watermarking algorithms transform the host image and embedding of the watermark information by vigorous way. ***Roux et al. [8]*** proposed a joint encryption/watermarking system for the purpose of protecting medical images. This system is based on an approach which combines a substitutive watermarking algorithm, the quantization index modulation, with an encryption algorithm: a stream cipher algorithm (e.g., the RC4) or a block cipher algorithm (e.g., the AES in cipher block chaining (CBC) mode of operation) objective is to give access to the outcomes of the image integrity and of its origin even though the image is stored encrypted.

Rehman et al. [5] presented digital images watermarking approach to sustain the ownership and true authentication. To secure intellectual belongings of images, audio and videos, watermark W is converted into a sequence of bits and in order to encrypt the watermark, sequence of size R is selected randomly. Additionally, a pseudo random number is generated to calculate pixels for selection key generation. Finally, 2-level discrete slanlet transform (DST) on the host image is applied to divide it into Red, Green and Blue channels. The results thus produced from proposed methodology exhibit robustness against the existing state of the art. Further, proposed approach effectively extract watermark in the absence of the original images.

Guru et al. [6] adopted the usage of a mixed (hybrid) transformation to fulfill these objectives, The opinion behind applying a hybrid transform or mixed transformation is that the cover image is modified in its singular values rather than on the DWT sub-bands and also PSNR values of both cover image and watermark can be change, therefore the watermark makes it vulnerable to vivid attacks and maintains its original state by checking the robustness. To support the methods and relative study some simulation results are available.

Mishra et al. [9], proposed a novel vigorous watermarking procedure for color images was performed. In this paper, the RGB image is transformed to HSV and watermarked by using discrete wavelet transform. Watermarking embedded phase and extraction phase is designed using an additional low power invisible watermarking algorithm. In this work, the host signal is an image and later than embedding the secret data a watermarked image is obtained and then taken out secret image and original image separately. In future the resulted watermarked image was tested with several attackers to substantiate the robustness and VLSI implementation of invisible watermarking algorithm using VHDL code and also confirm various performances like power, PSNR and tamper detection and area, etc

.

Singh et al. [10] proposed a classification based on their intrinsic features, inserting methods and extraction forms. Many watermarking algorithms are reviewed in the literatures which show advantages in systems using wavelet transforms with SVD. In this paper they also have presented a review of the significant techniques in existence for watermarking those which are employed in copyright protection. Along with these, an introduction to digital watermarking, properties of watermarking and its applications have been presented. In future works, the use of coding and cryptography watermarks will be approached. ***Malipatil et al. [11]*** paper covered, a novel scheme of protecting hidden transmission of biometrics using authentication watermarking. The proposed scheme uses watermark embedding algorithm. Evaluated with traditional personal identification system such as passwords and personal identification number codes, automated biometrics confirmation makes available a well-located and reliable method in diverse application but their validity must be guaranteed. Watermarking technique provides solution to ensure the validity of biometrics; proposed scheme is composed of three parts: watermark embedding, data embedding and data extraction. One of the applications of their proposed method is verifying data integrity for images transferred over the internet.

Ram et al. [12] described a digital image watermarking techniques based on Discrete Wavelet Transform (DWT) and Discrete Cosine Transform (DCT), where the method operates in the frequency domain embedding a pseudo random sequence of a real numbers in a selected set of DCT coefficients and watermark added to this selected DCT coefficients.

DIGITAL WATERMARKING TECHNIQUE

In the area of digital watermarking, digital image watermarking has fascinated a lot of consciousness in the research area for two causes: one is its simple accessibility and the other is it express adequate redundant information that could be used to embed watermarks [13]. Digital watermarking includes different techniques for protecting the digital content. The complete digital image watermarking techniques forever works in two domains either spatial domain or transform domain. The spatial domain approach works directly on pixels. It entrenches the watermark by modifying the pixels value. The most normally used spatial domain approach is LSB. Transform domain approach embed the watermark by transforming the transform domain coefficients. Most generally used transform domain approach is DCT, DWT and DFT.

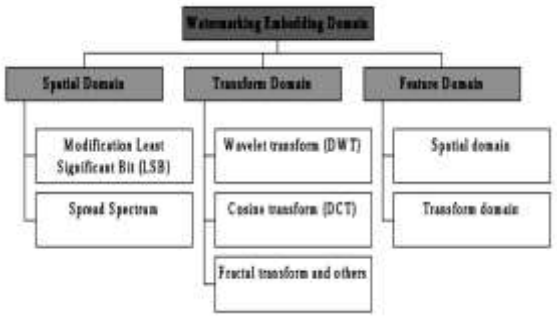

Fig. 2 Classification of Digital Watermarking technique

Spatial Domain Approach

The spatial domain represents the image in the form of pixels. The spatial domain watermarking embeds the watermark by modifying the intensity and the color value of some selected pixels. The strength of the spatial domain watermarking is Simplicity, Very low computational complexity and less time consuming.

Least Significant Bit

Least Significant Bit [14] is a spatial domain technique which is an incredibly unsophisticated and straight forward. It acquires less time to embed image (watermark).The watermark is entrenches into the least significant bits of the original image. This technique has many weaknesses, even uncomplicated attacks can get rid of or annihilate watermark but sometime it may endure beside some of the transformations. Different enhancements on LSB substitution has also been proposed in current times like embed watermark at single bit rate, multi bit rate or by means of a pseudo-random number generator. Pixel can also be preferred with help of key. Whichever addition of noise [15] and performing lossy compression can simply disgrace the image quality or eliminate or obliterate or disrupt watermark. It lacks the basic robustness. In case, if the algorithm is revealed, it becomes simple for attacker to change or eliminate watermark. The advantages of LSB are that it is easy to understand, easy to implement and provide high visual fidelity. Drawback of least significant bit (LSB) is that the transformed pixel is lost, it is less robust to various attacks and cropping or shuffling destroys the coding.

Spread Spectrum

The use of the spread spectrum technique for digital watermarking first appeared in a patent in [16] where the least significant bit of samples of an audio stream are periodically replaced with a random- looking signature, but very little. Since then, increasingly sophisticated algorithms have been developed for embedding messages within digital data in multiple dimensions for audio, image, and video. For the most part the common denominator of these methods has been the use of pseudo-noise (PN) sequences in various forms to embed (or scramble) the message. Advantages of this technique are that it opposes intentional and unintentional interference and can share the same frequency band with other users. It is also able to maintain the privacy, due to the pseudo random code sequence. Drawback of this scheme is that the original audio signal is needed and it is also very susceptible to noise.

Predictive Coding Schemes:

Predictive coding scheme was proposed by Matsui and Tanaka for gray scale images. In this method the correlation between adjacent pixels are exploited. A set of pixels where the watermark has to be embedded is chosen and alternate pixels are replaced by the difference between the adjacent pixels. This can be further improved by adding a constant to all the differences. A cipher key is created which enables the retrieval of the embedded watermark at the receiver. This is much more robust as compared to LSB coding [17].

Patchwork Techniques:

In patchwork watermarking, the image is divided into two subsets. One feature or an operation is chosen and it is applied to these two subsets in the opposite direction. For instance if one subset is increased by a factor k, the other subset will be decreased by the same amount [17]. The advantage of spread spectrum is that it provides High level of robustness against most type of attacks and drawback is that it is not able to hide big amount of information.

Transform or Frequency Domain Approach

The transform domain watermarking is accomplishing extremely much achievement as compared to the spatial domain watermarking. In the transform domain watermarking, the image is represented in the form of frequency. In the transform domain watermarking techniques, initially the original image is converted by a predefined conversion. After that the watermark is embedded in the transform image or in the transformation coefficients. Lastly, the inverse transform is performed to acquire the watermarked image. The example of transform domain of digital marking is DWT, DCT etc.

Discreet Wavelet Transform

Discrete Wavelet transform (DWT) is a mathematical tool for hierarchically decomposing an image [7]. It is useful for processing of non-stationary signals. The transform is based on small waves, called wavelets. Wavelet transform provides both frequency and spatial domain 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. The filters divide the input image into four sub-bands LL1, LH1, HL1 and HH1. The sub-band LL1 represents the coarse-scale DWT coefficients while the sub-bands LH1, HL1and HH1 represent the fine-

scale of DWT coefficients. To obtain the next scale of wavelet coefficients, the sub-band LL1 is further processed until some final scale N is reached. When N is reached we will have 3N+1 sub-bands consisting of the multi-resolution sub-bands LLN and LHx, HLx and HHx where x ranges from 1 until N. Due to its excellent spatio-frequency localization properties, the DWT is very suitable to identify the areas in the host image where a watermark can be embedded effectively[7]. The advantages of DWT are that it is suitable for localization is time and spatial domain and it also provides high compression strength which is helpful for human discernment. The drawback is that it requires much compression and designing time. It also include blur in the edge of images.

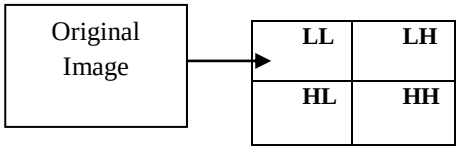

Fig. 3 DWT Decomposition of Image Using 1-Level Pyramid

Discrete Fourier Transform (DFT)

Transforms a continuous function into its frequency components [19]. It provides robustness against geometric attacks like scaling, cropping, rotation, translation etc. DFT of an original image is generally complex valued, which results in the magnitude and phase representation of an image. DFT shows translation invariance. Spatial shifts in the image affects the phase representation of the image but not the magnitude representation, or circular shifts in the spatial domain don't affect the magnitude of the Fourier transform. DFT is resistant to cropping because effect of cropping leads to the blurring of spectrum. If the watermarks are embedded in the magnitude, these are normalized coordinates, there is no synchronization are needed. The advantages of this are that it is very helpful in geometric distortions. Drawback is that it is complex to implement and require much computing time.

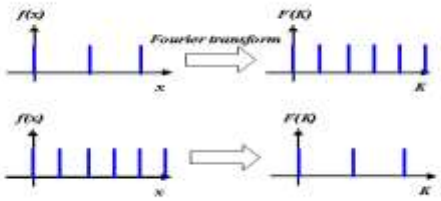

Fig.4 Fourier Transform activity

Discreet Cosine Transform

Discrete Cosine Transform [9] is a very popular transform domain watermarking technique. In this technique, an image is divided into different frequency band as low (FL), medium (FM) and high (FH). It allows selecting the band to embed data or watermark into the image. Figure 5 represents Discrete Cosine Transform Frequency 8X8 block , where low frequency band FL appears at upper left corner, if modification performed here, the watermark can be caught by human eyes. High frequency band FH lies at lower and right edges, if modification performed here, it may lead to local distortion along with edges. Medium frequency band FM is considered best region for modification, it cannot affect the image quality. Thus, a middle frequency band is the best band to embed watermark. DCT is a faster technique [17], with complexity O (n log n). This technique can survive attacks like compression, noising, sharpening and filtering. This technique is considered to be better than spatial domain watermarking technique.

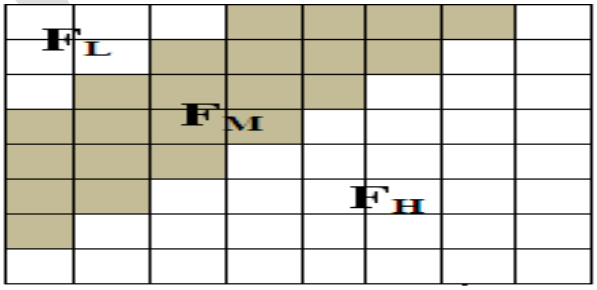

Fig. 5 Discrete Cosine Transform

PERFORMANCE MEASURING PARAMETER

In order to calculate the performance of the watermarked images, there are some performance measures such as ET, NCC, SNR, PSNR, MSE, and BER [20].

Execution Time

It is one of the important parameter to compute the working and performance of the watermarking algorithms in relation with time. It evaluates the amount of time required in embedding process and extraction process of watermark. To measure of execution time CPU cycles are used. General formulae can be used as:

$$Initial\_Time = CPUtime$$
$$Time\_Taken = CPUtime - Initial\_Time$$

Normalized Cross Correlation

It is used to measure the similarity between the cover image and the watermarked image as well as original watermark and recovered watermark. Higher the value of NCC will result in better technique. It is calculated by the formula:

$$NCC = \frac{\sum i \sum j [I(i,j) - Iw(i,j)]}{\sum i \sum j [I(i,j) + Iw(i,j)]}$$

MSE (mean square error)

It is defined as average squared difference between a reference image and a distorted image. It is calculated by the formula given below X and Y is height and width respectively of the image.

$$MSE = \frac{1}{MN} \sum \sum (W_{ij} - H_{ij})^2$$

PSNR (Peak Signal to Noise Ratio)

It is used to find out the degradation in the embedded image with respect to the host image .It is calculated as:

$$PSNR = 10log_{10} L * \frac{L}{MSE}$$

Where L is the peak signal value of the cover image which are equivalent to255 for 8 bit images.

BER (Bit Error Rate)

The **bit error rate** (**BER**) is the amount of **bit** errors per unit time. The **bit error** ratio (also **BER**) is the number of **bit** errors separated by the total number of transferred **bits** during a studied time interval. **BER** is a unitless performance measure, frequently expressed as a percentage.

$$BER = \frac{P}{H * W}$$

Where H and W are height and width of watermarked image is the count number initialized to zero and it incremented by one if there is any bit difference among cover and embedded image.

CONCLUSION

For copyright protection and authentication nowadays watermarking technique is extensively used. In this paper we discusses various digital watermarking technique like spatial and transform domain technique which is very efficient in providing security to our information but some are complex to implement and some included noise or blur in the images. So in future work design the system using the best features of both the technique of watermarking due to which we can provide more security or hide essential information from attacks.

REFERENCES:

[1]. Mitchell D. Swanson, Mei Kobayashi, and Ahmed H. Tewfik "Multimedia Data-Embedding and Watermarking Technologies", Proceedings of IEEE, Vol. 86, No. 6, June 1998.
[2]. C.I. Podilchuk and E. J. Delp, "Digital Watermarking: Algorithms and Applications", IEEE Signal Processing Magazine, pp.33-46, July 2001.
[3]. Afroja Akter, Muhammad Ahsan Ullah, "Digital Watermarking with a New Algorithm", International Journal of Research in Engineering and Technology eISSN: 2319-1163 | pISSN: 2321-7308
[4]. Shukla, S.S.P. Singh, S.P. , Shah, K. and Kumar A., "Enhancing security & integrity of data using watermarking & digital signature" Recent Advances in Information Technology (RAIT), 2012 1st International Conference on 15-17 March 2012 Page(s):28 - 32 Print ISBN: 978-1-4577-0694-3.
[5]. Myasar Mundher, Dzulkifli Muhamad, Amjad Rehman, Tanzila Saba and Firdous Kausar, "Digital Watermarking for Images Security using Discrete Slantlet Transform", Appl. Math. Inf. Sci. 8, No. 6, 2823-2830 (2014).
[6]. Jaishri Guru, Hemant Dhamecha and Brajesh Patel, "Fusion of DWT and SVD digital watermarking Techniques for robustness", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 9, September 2014 ISSN: 2277 128X.
[7]. Raval, K. and Zafar, S. ―Digital Watermarking with copyright authentication for image Communication‖, in Intelligent Systems and Signal Processing (ISSP), 2013 International Conference on March 2013,pp. 111 - 116 .
[8]. Dalel Bouslimi, Gouenou Coatrieux, Michel Cozic, and Christian Roux―A Joint Encryption/Watermarking System for Verifying the Reliability of Medical Images‖ IEEE Transactions On Information Technology In Biomedicine, Vol.16, No. 5, September 2012 Pp.891-899.
[9]. Manoj Ramaiya Richa Mishra, " Digital Security using Watermarking Techniques via Discrete Wavelet Transform", National Conference on Security Issues in Network Technologies August 11-12, 2012.
[10]. Y. Shantikumar Singh, B. Pushpa Devi, and Kh. Manglem Singh, "A Review of Different Techniques on Digital Image Watermarking Scheme", International Journal of Engineering Research, ISSN:2319-6890, Volume No.2, Issue No.3, pp:193-199, 01 July 2013.
[11]. Shubhangi D.C1, Manikamma Malipatil, "Authentication Watermarking for Transmission of Hidden Data using Biometrics Technique", International Journal of Emerging Technology and Advanced Engineering Website: www.ijetae.com (ISSN 2250-2459, Volume 2, Issue 5, May 2012).
[12]. B Ram, "Digital Image Watermarking Technology Using Discrete Wavelet Transform And Discrete Cosine Transform", International journal of Advancements in Research & technology, Volume 2, Issue 4,April 2013.
[13]. V. M. Potdar, S. Han and E. Chang, "A Survey of Digital Image Watermarking Techniques", 2005 3rd IEEE International Conference on Industrial Informatics (INDIN).
[14]. D. Samanta, A. Basu, T. S. Das, V. H. Mankar, Ankush Ghosh, Manish Das and Subir K Sarkar, SET Based Logic Realization of a Robust Spatial Domain Image Watermarking," Proc. in 5th International Conference on Electrical and Computer Engineering-ICECE 2008, Dhaka, Bangladesh, pp. 986-993, Dec. 2008.
[15]. J. L., Dugelay, S. Roche, C. Rey, G. Doërr, "Still-image watermarking robust to local geometric distortions," IEEE Trans. on Image Proc., vol. 15, no. 9, pp. 2831-2842, 2006.
[16]. L. F. Turner (1989), Digital Data Security System, Patent IPN WO 89/08915.
[17]. Sasmita Mishra, Amitav Mahapatra,Pranati Mishra, "A Survey on Digital Watermarking Techniques", International Journal of Computer Science and Information Technologies, ISSN:0975-9646, Vol. 4 , 2013, 451-456.
[18]. Chaturvedi Navnidhi and Basha S.J, "Comparison of Digital Image watermarking methods DWT and DWT-DCT on the basis of PSNR," International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET), ISSN: 2319-8753, Vol. 1, Issue 2, December 2012.
[19]. Jalpa M. Patel, "A brief survey on digital image watermarking techniques" ,International Journal For Technological Research In Engineering Volume 1, Issue 7, March-2014.
[20]. S Sahar Afshan Andrabi, Sheenam, "A Review: Information Hiding Using Watermarking Techniques", International Journal of Computer Science and Engineering (SSRG-IJCSE) – EFES April 2015