High Security Text Message and Digital Image using Discrete Shearlet Transform

Bhagyashree Patil[1], Dr. L. K. Vishwamitra[2]

[1]M. Tech. Scholar, [2]Professor

OCT, Bhopal

Abstract - During the past few years with the starting of the Internet and the explosion of the information revolution contemporary across the world has become a computer use at the present time means the most important and prevalent in the storage, retrieval, control and transfer of information across networks of different local, international emails and mobile phones via digital media such as texts, image, audio and video. It has become easy to intercept the information sent across the networks or access to a various computers, whether it is independent or linked with the network, the purpose of access to content, theft of important information or tampering with it. Therefore, the science of information security has become the interest to many researchers who strive to develop solutions, techniques and ideas to ensure the transfer of information safely without any breakthrough or detection of information. It currently uses techniques and methods of protecting the security of information in a variety of setting such as passwords, encryption techniques and hiding the cover information.

I. INTRODUCTION

Digital information and data are transmitted more often over the internet now than ever before. The availability and efficiency of global computer networks for the communication of digital information and data have enhanced the popularity of digital media [1]. Hence, information security is becoming more and more important for information intercommunication and transmission among people. In order to secure information against unauthorized illegal access, diverse methods such as symmetric and asymmetric encryption systems are used [2]. Traditionally, protection of digital data has been provided by a variety of encryption methods. However, encryption alone does not provide an adequate solution as it only provides for robust delivery of the content. Once the content is decrypted, it is no longer protected and the content may be illegally replicated or copied without any prevention [3]. Thus, piracy in the presence of internet and computers is a major concern [4]. To deal with piracy and counterfeiting of the multimedia data, digital watermarking technique has an edge over the other available techniques. As a result, a variety of algorithms, such as fragile watermarking, robust watermarking and reversible watermarking, have been proposed for the digital content. Out of these categories,robust watermarking is an important technique as it demands that the embedded watermark can be extracted and identified in presence of different attacks like JPEG encoding, noise, cropping etc.

Figure 1.1: Watermark in Mark and Dollar Bank Notes

II. LITERATURE REVIEW

Devices such as I-pod, Mobile phone, Web Camera, Personal Digital Assistant, Digital camcorder and others allow the users in an interactive way to create, modify, delete and view digital data. A new invention provides more features in a single device and provides very high portability. These inventions and developments create an electronic environment where the user can share and deliver the multimedia content, but it also decreases the authenticity of the content. Also with the rapid growth of Internet technologies and wide availability of multimedia computing facilities, the enforcement of multimedia copyright protection becomes an important issue. Digital information can be perfectly copied and is easily stored which makes it onerous to enforce the negotiated rights and conditions for use of the data. In this situation, protection of digital.

NazirA. Loan et al. [1],they have proposed DCT domain watermarking can be classified into global DCT watermarking and block based DCT watermarking. Applying global DCT on image segregates the image into different frequency bands. He proposed spread spectrum based approach for watermark embedding using global DCT transform. Signal energy present in any frequency band is undetectable if a narrowband signal is transmitted over a much broader bandwidth. In this approach watermark is a narrow band signal which is spread over all frequencies so that the energy in any single frequency component is very small and is undetectable.

BaharakAhmaderaghi et al. [2], dazzle watermarking focuses on the testing recuperation of the watermark when

the host isn't accessible amid the identification organize. This paper proposes Discrete Shearlet Transform (DST) as another implanting area for visually impaired picture watermarking. Our tale DST daze watermark discovery framework utilizes a non-added substance conspire dependent on the measurable choice hypothesis. It initially processes the Probability Density Function (PDF) of the DST coefficients displayed as Laplacian dissemination.

AlekseiZhuvikin et al. [3], a novel selective image authentication system based on the robust digital watermarking is proposed. The discrete shearlet transform is performed in order to extract the feature vector from the image. The cone-adapted version of the transform is used to calculate the shearlet coefficients more precisely and to avoid the biased treatment. The proposed approach allows using conventional cryptographic digital signature for the image feature vector verification and makes the authentication scheme more secure. In order to embed watermark (WM) into the image the areas HL3 and LH3 of the Haar wavelet transform coefficients are used.

MortezaHeidari et al. [4],they have proposed digital watermarking based on DCT technique. Every day, people share their digital media on the virtual networks; therefore, protecting them against piracy is worthy of consideration. Digital watermarking is a method to achieve this goal. The propose a watermarking method in Discrete Cosine Transform (DCT) domain. For this purpose, DCT coefficients of the whole image are calculated. It helps to present a system without blockiness effects. Then, singular values of the watermark image are added to the low frequencyDCT coefficients of cover image that is located on the main diagonal.

N. Senthil Kumaran et al. [5],they have proposed DWT has been used in digital image watermarking more frequently due to its excellent spatial localization and multi-resolution characteristics, which are similar to the theoretical models of the human visual system. With the standardization process of JPEG 2000 and the shift from DCT to wavelet based image compression method, watermarking schemes operating in the wavelet transform domain have become even more interesting. Wavelet transforms use wavelet filters to transform the image.

BaharakAhmaderaghi et al. [6],this paper presents a new perceptual watermarking model for Discrete Shearlet transform (DST). DST provides the optimal representation of the image features based on multi-resolution and multi-directional analysis. This property can be exploited on for watermark embedding to achieve the watermarking imperceptibility by introducing the human visual system using Chou's model. In this model, a spatial JND profile is adapted to fit the sub-band structure. The combination of DST and the Just-Noticeable Distortion (JND) profile improves the levels of robustness against certain attacks while minimizing the distortion; by assigning a visibility threshold of distortion to each DST sub-band coefficient in the case of grey scale image watermarking.

III. DIGITAL WATERMARKING

The idea of data hiding is an old technique. But, Tirkel et al.[8, 9] first introduced digital watermarking in 1993. They have proposed techniques to embed data by modifying the LSB of the pixel values in an image. A digital watermark is a signal permanently embedded into digital data that can be detected or extracted later by means of computing operations in order to make assertions about the data. The watermark is embedded in the host data in such a way that it is inseparable from the host and is resistant from the attacks used to degrade the document. Therefore, we can say that "through watermarking technique, the host data is still accessible but permanently marked with the watermark" [10, 11]. Digital watermarking technique is derived from steganography. Steganography is the technique in which the secret message is hidden inside the harmless message in such a way that a user can't detect the presence of the secret message.

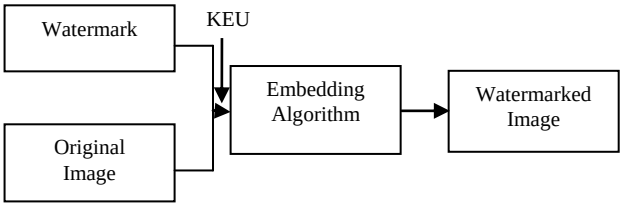


Figure 3.1: Watermark Embedding Model

Watermark information can be the serial number of the author, company logo, or the text with special significance, etc., which can be used to identify a file, the source of image or music products, version, original author, owner, publisher, the ownership of legitimate user to the digital product [13].

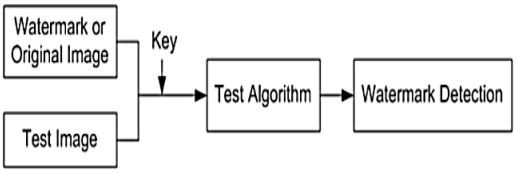


Figure 3.2: Watermark Detection Model

With the wider applications of data embedding in digital sources, associated activities like steganography, digital watermarking and data hiding have also come up. Steganography refers to the art and science of data hiding, it spans broader class of applications than watermarking, and it includes hiding of information in text and non-digital media.

3.1 Types of Digital Watermarking :- Based on the domain of usage, the watermarking techniques are grouped

as spatial and frequency domain watermarking. Based on the content type of digital documents, the watermarking techniques are classified as text, image, audio and video watermarking. Also based on Human Perception the watermarking techniques are further classified as visible and invisible watermarking, the invisible watermarking is further classified as robust and fragile watermarking. Robust watermarking is further classified as Private, Public, Invertible, Non-Invertible, Quasi-invertible and Non-quasi-invertible watermarking.

3.2 Properties of Digital Watermarking :- Digital watermarking systems are characterized by a number of properties such as Imperceptibility or Fidelity, Payload or Capacity, Robustness and Security. Fidelity or Imperceptibility and Payload can be associated with the embedding process and Robustness, Security is associated with the blind and informed detection. Artifacts introduced through a watermarking process are not only annoying and undesirable, but may also reduce or destroy the commercial value of the work.

3.3 WATERMARKING SYSTEM WITH COMMUNICATION SYSTEM :- The Watermarking System can be compared to a communication system. Like the Communication System the watermarking system consists of three parts. The analogy of communication system and watermarking system is shown in figure 3.3 and figure 3.4.

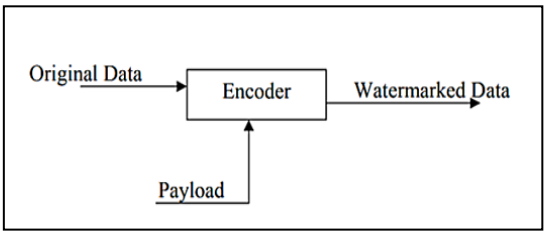


Figure 3.3: Watermark Encoder (Embedder)

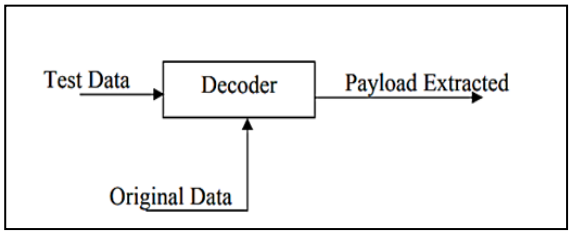


Figure 3.4: Simple Decoding Process

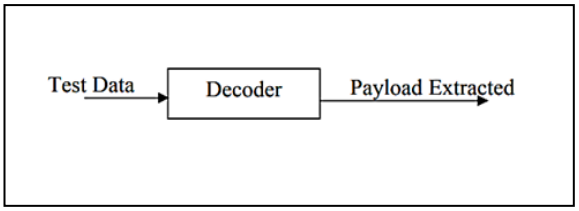


Figure 3.5: Blind Decoding Process

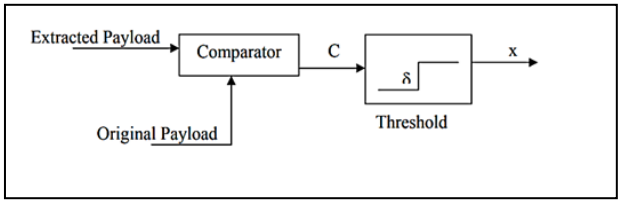


Figure 3.6: Comparing Process

3.4 CLASSIFICATION OF WATERMARKING ATTACKS :- A wide variety of attacks both incidental and malicious should be survived by a robust watermark. Some of the best known attacks are introduced as under [19].

3.4.1 Simple Attacks :- Attacks like waveform or noise are aiming at damaging the fixed watermarks by manipulating the data as of whole watermark (watermark with host data) without any effort to identify & isolate the watermark.

3.4.2 Attacks of Detection-disabling :- The attacks of synchronization are used to break the correlation. A watermark detector finds it impossible or infeasible to recover the watermark. It is done by the synchronization attacks mostly by geometric distortion like, rotation, pixel permutations, shift in direction (for video).

3.4.3 Ambiguity Attack :- Fake watermark data occur on attack, inserting fake watermark, these fake watermarked data create some confusions. An inversion attack which tries to discredit the authority of the watermark by fixing one or several extra watermarks from which one cannot know the first authoritative watermark.

3.4.4 Removal Attacks :- To discard only the watermark, to separate the watermark data into host data and watermark to estimate the watermark or the host data and to analyze the watermark data, the removable attacks are attempted for the above fulfillment. Examples are collusion attacks, de-noising, certain filter operations, or compression attacks using synthetic modeling of the image.

IV PROPOSED METHODOLOGY

4.1.1 Watermarking Embedding Procedure :- The procedure for embedding the watermark that following in this work is given as follows:

- Select the host and the watermark image.
- Apply DST transform on both original and the watermark image.
- Apply SVD on the LL sub band of both original and the watermark image.
- Embedding process

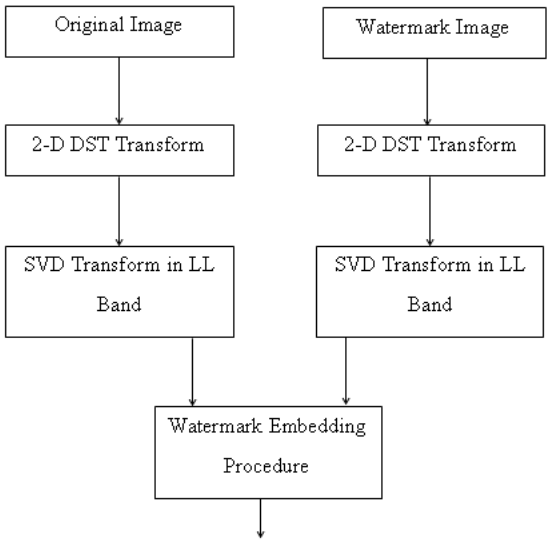


Figure 4.1: The Watermarking Embedding Procedure

4.1.2 Extracting Embedded Image :- The procedure for extracting embedding the image that following in this work is given as follows:

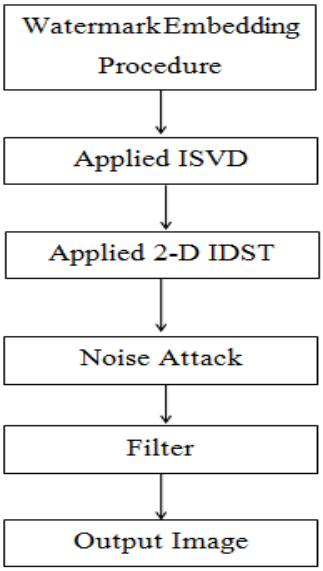


Figure 4.2: The Watermarking Extracting Embedded Procedure

- Select the watermark embedding procedure.
- Apply ISVD transform on embedding watermark image.
- Apply 2-D IDST on the IDST image.
- Applied Noise Attack in 2-D IDST Image
- Applied median filter in Noise attack Image
- Get output Image

V. PROPOSED ALGORITHM

Step 1: Take host image as input and convert it into Resize image original (RIO).

Step 2: Apply 2-D DST on resize image original (RIO) to decompose it into seven sub-bands.

Step 3: Select sub-band LL_2 of RI.

Step 4: Then apply SVD to sub-bands LL_2 to get UR, ΣR and V^TR.

Where U is real unitary matrix, Σ is rectangular diagonal matrix, V is complex unitary matrix, V^T is the conjugate transpose of **V** and R is Resize Image

Step 5: Take watermark image as input and convert it into Resize image watermark (RIW). Apply 2-D DST on resize image watermark (RIO) to decompose into seven sub-bands.

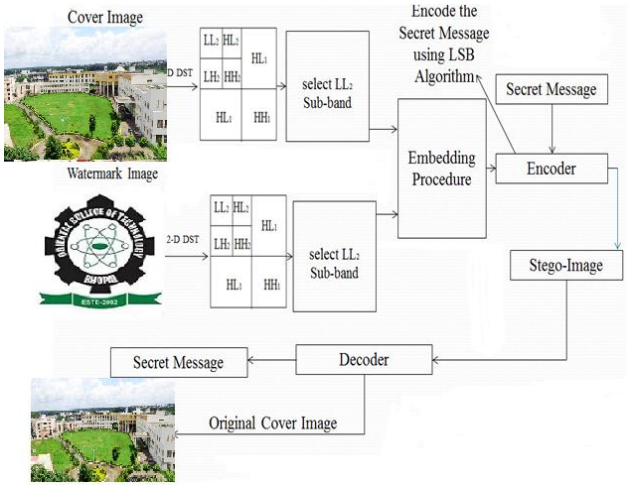


Figure 4.3: Flow Chart of Proposed Methodology

Step 6: Select sub-bands LL_2 of Wi.

Step 7: Then apply SVD to sub-bands LL_2 to get UW, ΣW and V^TW.

Step 8: Modify UR, ΣR and V^TR by using equation

$UR^* = UR + (0.10*UW);$

$\Sigma R^* = \Sigma R + (0.10* \Sigma W);$

$V^TR^* = V^TR + (0.10* V^TW);$

Step 9: Construct modified SVD matrix UR*, ΣR* and V^TR^*.

Step 10: Apply inverse SVD.

Step 11: Apply inverse DST and finally get output image and secret message.

5.1 Discrete Shearlet Transform

Shearlet transform is an affine function containing a single mother Shearlet function that is parameterized by scaling, shear and translation parameters with the shear parameter capturing the direction of the singularities. An important advantage of this transform over other transforms is due to the fact that there are no restrictions on the number of

directions for the shearing. There are also no constraints on the size ofthe supports for the shearing, unlike, for instance, directional filter banks where using a small window size would result in a performance loss.

5.2 Single Value Decomposition :- SVD is a mathematical tool used for reduction of any two dimensional matrix problems. picture can likewise be spoken to by two dimensional lattices. In this way, SVD can be utilized as a part of picture handling because of its properties, for example, transpose, solidness and so forth.

$$M = U \sum V^T$$

5.3 LSB Technique :- This technique works best when the file is longer than the message file and if image is grayscale. When applying LSB technique to each byte of a 24 bit image, three bits can be encoded into each pixel. If the LSB of the pixel value of cover image C(i, j) is equal to the message bit SM of secret message to be embedded C(i, j) remain unchanged; if not, set the LSB of C(i, j) to SM.

Message embedding procedure is given below:

S(i, j) = C(i, j)-1, if LSB (C(i, j)) = 1 and SM = 0

S(i, j) = C(i, j)+1, if LSB (C(i, j)) = 0 and SM = 1

S(i, j) = C(i, j), if LSB (C(i, j)) = SM

Where LSB (C(i, j)) stand for LSB of cover image C(i, j) and "SM" id the next message bit to be embedded. S(i, j) is the Stego image.

5.4 Modified LSB Technique :- The proposed method follows a directional embedding technique for achieving maximum image quality in the stego image. The proposed method performs a selection of suitable direction for secret byte embedding so as to minimize the bit changes in the cover image when a secret data is embedded.

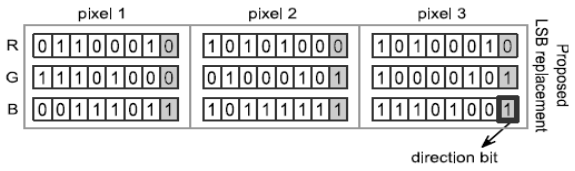


Figure 4.4: LSB Embedding of the Byte 11110000 in the Cover Image using

VI RESULT SIMULATION

6.1 Gaussian Noise Attack :- The original Baboon image of 512×512 pixel value. The random image of the original image is resized 512×512image

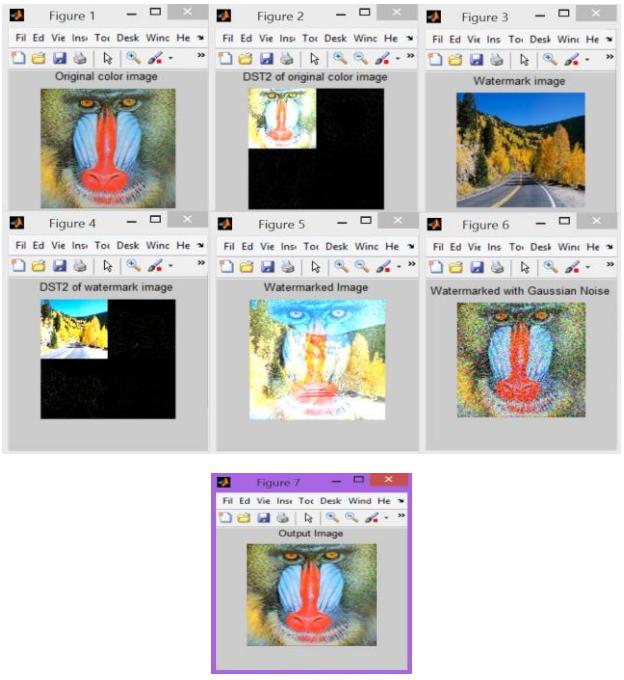


Figure 5.2: Experiment Baboon Image with Gaussian Noise

The original resize image is passing through 2-D DST and 2-D DST original resize image is shown in figure 5.2 (b). The watermark image is 512×512 pixel value is shown in figure 5.2 (c) and watermark image is passing through 2-D DST and 2-D DST watermark resize image is shown in figure 5.2 (d).

6.2 Salt and Pepper Noise Attack :- The original Pepper image of 512×512 pixel value. The random image of the original image is resized 512×512image, resize image is shown in figure 5.3 (a).

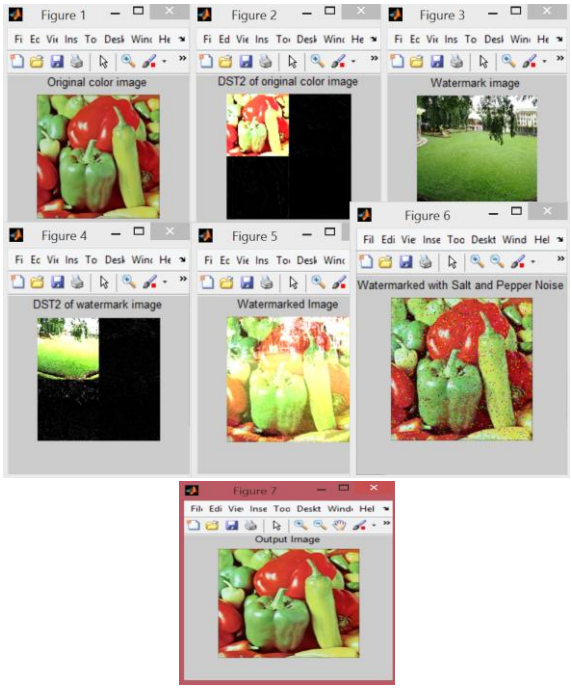
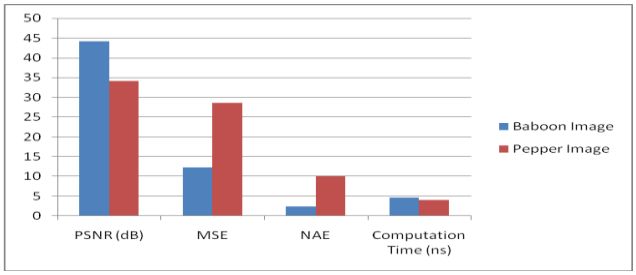


Figure 5.3: Experiment Flower Image with Salt and Pepper Noise

6.3 Result for Different Imageswithout Noise Attack :-

Image	PSNR (dB)	MSE	NAE	Computation Time (ns)
Baboon Image	44.206	12.334	2.376	4.682
Pepper Image	34.069	28.519	10.005	4.093

The proposed DST-SVD technique gives a highest PSNR 44.206 dB for Baboon image and lower PSNR 34.069 dB for Pepper image.



VII CONCLUSION FUTURE SCOPE OF WORK

The emerging techniques in the field of transform domain such as DST and adaptive Steganography are not an easy target for attaches, especially when the concealed messages are small. We have proposed a new framework for enhancing security system by combining text and image, in which a new digital watermark and steganography method based on DST, shows the effectiveness and robustness of the proposed system. As future work more focus can be on improvement of compression ratio by using new techniques. The proposed technique can be experimented on various kinds of datasets like audio, video, text as till now it is only restricted to images. New methods can be combined and proposed to decreases the time complexity incurred in creating dictionary in LZW Algorithm. The experimental dataset in this research is limited; so applying the developed method on a larger dataset could be a subject for future research which may lead to new observations and conclusions.

VII REFERENCES

[1] Nazir A. Loan, Nasir N. Hurrah, Shabir A. Parah, Jong Weon Lee, Javaid A. Sheikh, and G. Mohiuddin Bhat, “Secure and Robust Digital Image Watermarking Using Coefficient Differencing and Chaotic Encryption”, Received January 4, 2018, accepted February 7, 2018, date of publication March 16, 2018, date of current version April 25, 2018.

[2] BaharakAhmaderaghi ; FatihKurugollu ; Jesus Martinez Del Rincon ; Ahmed Bouridane, “Blind Image Watermark Detection Algorithm based on Discrete Shearlet Transform Using Statistical Decision Theory”, IEEE Transactions on Computational Imaging, Volume: 4 , Issue: 1, Page s: 46 – 59, IEEE 2018.

[3] AlekseiZhuvikin, “Selective Image Authentication usingShearletCoefficients Tolerant to JPEG Compression”, Page s: 681 – 688, IEEE 2017.

[4] Morteza Heidari1, Nader Karimi, and Shadrokh Samavi, “A Hybrid DCT-SVD Based Image Watermarking Algorithm”, Iranian Conference on Electrical Engineering (ICEE), IEEE 2016.

[5] N. SenthilKumaran, and S. Abinaya, “Comparison Analysis of Digital Image Watermarkingusing DWT and LSB Technique”, International Conference on Communication and Signal Processing, April 6-8, 2016, India.