NOVEL IMAGE STEGANOGRAPHY TECHNIQUES: A CASE STUDY

[1]Mr. Kamble S.V, [2]Mr. Sakhare V. C
[1,2]Assistant Professor
[1]Department of Information Technology, [2]Department of Electronics
DKTE'S Textile & Engineering Institute, Ichalkaranji

Abstract— Steganography is an important area of research in recent years; it is a technique that usually prevents unauthorized users to have access to the important data. The steganography and digital watermarking provide methods that embedding information into the cover images viz. text, video, and images that users can hide and mix their information within other information that make them difficult to recognize by attacker.

In this paper, we review on different Steganography methods, algorithms, and schemes in image steganography is conducted in order to analyze and investigate them.

Keywords— Image Steganography Techniques, Data Embedding and Extracting, Data Hiding, Image Steganography

I. INTRODUCTION

Steganography comes from the combination of the Greek words Stegano means sealed and Graphy referring to writing which means secret writing. Steganography is a very old art of embedding personal information into other data by using some rules and techniques [13].

Image steganography is the art of information hidden into cover image, is the process of hiding secret message within another message. The word steganography implies "Covered Writing", the information hiding process in a steganography with different techniques includes identifying a cover mediums redundant bits. As a result, unauthorized users are not able to see and recognize the embedded information.

Steganography is managing a secret path for sending information invisibly.

As shown in Figure 1, the aim of steganography is to hide the message under cover files, concealing the very existence of information exchange. Indeed, among a variety of files types, an image steganography is the preferred, since the altered image with slight variations in its colors will be indistinguishable from the original image by human eye [14].

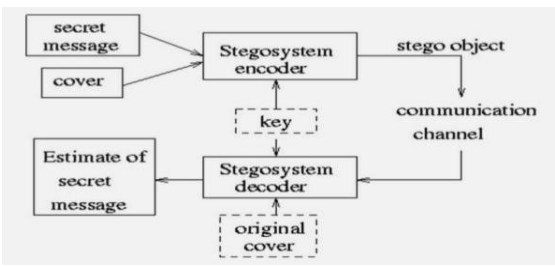

Figure 1: A Typical Steganography Technique [14]

Main objective of steganography is to communicate securely in such a way that the true message is not visible to the observer. Today steganography is mostly used on computer with digital data being the carriers and networks being the high speed delivery channel [5][18].
During the process of hiding the information there are three factor must be considered, that includes ***capacity*** it indicates the amount of information that can be hidden in the cover medium. ***Security*** implies to detect hidden information and ***Robustness*** to the amount of modification the stego medium can withstand before an adversary can destroy hidden information [6].

In General, Steganography is classified into four types as follows.

1. *Audio steganography*: In audio steganography digital sound files are used to hide a secret message using sequence of different sound file.

2. *Video steganography*: In this steganography technique, Video files can be defined as a collection of images and sounds combined together, amount of secret data that can be embedded inside the video files, since the video file is a moving stream of images and sounds

3. *Text steganography*: Text steganography consist of the information that is hidden in text files

4. *Image steganography*: It is a process of hide the secret image inside the cover image in such a way that the existence of the secret image is disappeared and the cover image seems to be original[14].

In cryptography techniques scrambles a message so it cannot be understood. Where as in steganography hides the message, so it cannot be seen. Watermarking and finger printing that seem hold promise for copyright protection. It becomes
Problematic when this technology is misused.

Steganalysis is a technique is used for detecting secret information hidden in a given image using Steganographic tool. The art of steganalysis plays a major role in the selection of features or characteristics to test for hidden message [11].

Rest of paper includes Literature review in section II, steganography techniques in section III and section IV conclusion.

II. LITERATURE REVIEW

Neil F. Johnson,Sushil jajodia et. Al [1] , They discuss different techniues of steganography and file compression, masking & filtering techniques.

Feng Pan, Jun Li et al[7] , They present an image steganography method which utilize horizontal pixel & verticle pixel difference, in the horizontal direction they use high quality model function method for two pair of pixel embed message they use PVD method.

Mamta janesa, Parvinder sing sandhu et.[3] ,They discuss the design of a roboust image steganography technique based on LSB insertion & RSA encryption technique.

Piyush marwaha, Paresh marwaha[4], They propose the concept of multiple cryptography where the data will be encrypted into a cipher & the cipher will be hidden into a multimedia image file in encrypted formal, visual steganography algorithm will be used.

Ge Huayong, Huang Mingsheng et. al[11], They illustrate concept and principle of steganography and steganalysis, spatial domain and transform domain embedding method are generalized. Then the performance specification of image steganography is discussed.

Sueed sarreshtedari & shahrokh Ghaemmaghami[12], They proposed steganography algorithm works on the wavelet transform coefficients of the original image to embed the secret data.

Mohammed A. Saleh [14], Author has discussed different techniques like Spatial Domain Techniques, Transform Domain Techniques,
Analyse and investigate them.

Ramadhan Mstafa, Christian Bach [13], Author has discussed some techniques of steganography and digital watermarking in both spatial and frequency domains.

III. STEGANOGRAPHY TECHNIQUES

- *Least Significant Bit (LSB) Embedding:*

Least Significant Bit (LSB) is a simple strategy for implementing steganography. Such as all steganography methods, it embeds the data into the cover, so that it cannot be detected by a casual observer [14].
In this technique the data is hidden in the least significant bit of each byte in the image, the size of each pixel depends on the format of the image and normally ranges from 1 bytes to 3 bytes. An 8 bit pixel is capable of displaying 256 different colors. Given two identical images, if the least significant bits of pixels in one image are changed the two images still looks identical to the human eye [3].

An LSB algorithm replaces the most-right bits of a cover files bytes. In case a bit of the cover image *C*(*i*,*j*) is equal to the bit of a secret massage (*Ms*) that to be embedded, *C(i,j)* stay untouched, otherwise *C(i, j)* is set to bit of a secret massage (*Ms*) [14]. For instance, the letter 'C' is an ASCII code of 67 in decimal, which is 01000011 in binary, and bits of the image pixels before the hiding(embedding) a secret message are:

Pixel 1: 1111100**0** 1100100**1** 0000001**1**
Pixel 2: 1111100**0** 1100100**1** 0000001**1**
Pixel 3: 1111100**0** 1100100**1** 00000011

Least Significant Bit (LSB) algorithm hides (embeds) bits of letter 'A', which are **01000001**, into image pixels to produce:

Pixel 1: 1111100**0** 1100100**1** 0000001**0** Pixel 2: 1111100**0** 1100100**0** 0000001**0** Pixel 3: 1111100**1** 1100100**1** 00000011

LSB requires that only half the bits in an image be changed [13][14].

Fig.2 LCB Conversion Image

- *Transform Domain Embedding*

In the techniques of transform domain techniques, the carrier object is first transformed from spatial domain to transform domain, and then its frequencies are used to hide the secret data. After embedding the secret data, the object is again transformed into spatial domain. These techniques have lower payload but are robust against statistical attacks [13][14]. The technique includes, Discrete Wavelet Transform (DWT), Discrete Fourier Transform (DFT), Discrete Cosine Transform (DCT).

- *Discrete Wavelet Transform (DWT)*

The use of wavelets in the form of shorthand model lies in a statement that the wavelet transform is obviously splits the high from the low-frequency [16].
The simplest method of wavelet transforms is the Haar wavelet. In Haar, transform the coefficient in the low frequency wavelet was created by take the averaging of the values of two pixels, and it can create the high frequency.
In this techniques coefficients by taking half difference of the similar two pixels. Figure (3) shows four bands approximate, Vertical, Horizontal, and diagonal Bands that represented as LL, LH, HL and HH respectively [16].

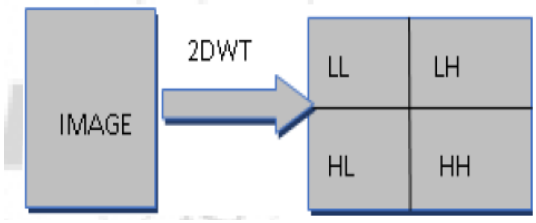

Fig.3 Components of 1-level 2DWT

In figure (4), shows the 2D Haar- DWT on image "Lena". The eyes of a human cannot recognize the small changing on the edges and textures of an image but it is very sensitive to any changes in the smooth parts. By this it can lead to hide the secret image inside high frequency sub-bands and will not be recognized by the human eyes [16]

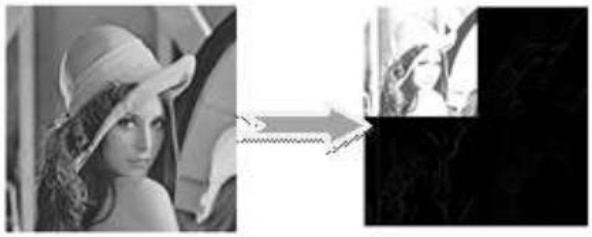

***Fig.4**: ('a') image of LENA before 2-D Haar-DWT, ('b') after the 2-D Haar-DWT*

- *The Embedding Process-Algorithm[16]*

Input: "Cover image" of size n x n and "secret image" of size 'n/2 x n/2'.

1) Read the Cover image of size n x n.
2) Read the 'Secret image' that have a size 'n/2' x 'n/2'.
3) Decompose the Cover image by using "db1" wavelet
transforms. The cover image was decomposed into (LL, LH, HL and HH) sub bands.
4) Permute the secret image by logistic chaotic map method.
5) Embed the encrypted secret image by using HH sub band cover image''.

- *Extraction process-Algorithm[16]*

Input: 'stego image'.
Output: 'secret image'.

1) Load the stego image.
2) Decompose 'the 'stego image'' using Discrete Wavelet transform to get [LL, LH, HL, HH] sub bands.
3) Extract secret encrypted image from the coefficient values of HH sub band
4) Apply the inverse of chaotic map to decrypt the extracted secret image

- *The Discrete Fourier Transform (DFT*)

Discrete Fourier transform is the transform that are purely discrete: discrete-time signals are converted into discrete number of frequencies. DFT converts a finite list of equally spaced samples of a function into the list of coefficients of a finite combination of complex sinusoids ordered by their frequencies. It can be said to convert the sampled function from its original domain often time or position along a line to the frequency domain. The Discrete Time Fourier transforms uses the discrete time but it converts into the continuous frequency [15].

- *Vector Embedding*

A vector embedding techniques that uses robust algorithm with codec standard (MPEG-1 and MPEG -2).In this techniques audio information embeds into the pixels of frames in host video. It is based on the H.264/AVC Video coding standard. The algorithm designed a motion vector component feature to control embedding, into the secret carrier. The information embedded will not significantly affect the video sequence's visual invisibility and statistical invisibility. The algorithm has a large embedding capacity with high carrier utilization, and can be implementing fast and effectively [15].

- *Statistical Technique:*

In the statistical technique information or message is embedded by changing several properties of the cover. It involves the splitting of cover into blocks and then embedding one message bit in each block. The cover block is modified only when the size of message bit is message bit is one otherwise no modification is required.

- *Vector Quantization :*

Vector Quantization (VQ) is one of the techniques based on the principle of block coding. It has been long used for compress media in such way that it is useful or efficient to use of network bandwidth and data storage space in the process of image compressing.
The codewords of the codebook are used to substitute the closest pixel block. The resultant compressed image is a table of indexes of the codewords. Some stegnographic methods for VQ compressed images have been reported in the recent years. A common feature of the methods is that they all partition the codebook into a number of groups or clusters, and then embed the secret message by replacing the codeword indexes of the compressed image with those of the same group /cluster selected according to the corresponding secret bits [17].

IV.CONCLUSION

This paper presented a review on a different methods, algorithms, and schemes for image steganography area in order to analyze and investigate them. All the techniques discussed in this paper are able to secure the hidden data. The algorithm implemented for steganography has a very high time complexity and very less amount of data stored in the images. In the area of image steganography is a need to develop efficient algorithms, either by combining the existing techniques or by developing new techniques.

REFERENCES

[1] N.F Johnson & Suhil Jajodia “Exploring Steganography: Seeing the Unseen”,Survey Paper IEEE-1998

[2] K.B.Raja, C.R.Chowdary,”A Secure Image Steganography using LSB,DCT and compression Techniques on Raw Images”, IEEE -2005.

[3] Mamta Juneja & Parvinder Singh Sandhu,”Designing of Roboust Image Steganography Technique Based on LSB Insertion and Encryption”, 2009 ICARTCC

[4] Piyush Marwaha & Paresh Marwaha,”Visual Cryptographic Steganography in Images”, 2010 Second international conference on computing, communication and networking technologies.

[5] Amitava Nag, Sushanta Biswas,”A Novel Techniques for image steganography based on DWT and Huffman Encoading”,IJCSS,Vol(4):Issue (6)

[6] Hniels Provos & Peter Honeyman,”Hide & Seek : An Introduction to Steganography” IEEE Computer Society Pub-2003.

[7] Feng Pan, & Jun Li,”Image Steganography Method Based on PVD and Modules Function”,IEEE-2011.

[8] Pfitzmann & Wesrfeld.A,”High Capacity Despite Better Steganalysis,” Kluwer Academic Publisher Boston Dodrecht London,2000.

[9] Ming Chen,Z.Ru.N.Xin, “Analysis of Current Steganography Tools: Classification & Features”, Information Security & Tele.Comm. Beijing Dec-2006.

[10] Hassan mathkour,Batool Ai,sadoon, “A New Image Steganography Technology” ,IEEE-2008

[11] Ge Huayong ,Huang ,”Steganography and Steganalysis Based on Digital Image”, International conference & signal Processing-2011 IEEE

[12] Saeed Sarreshtedari & Shahrokh ,”High Capacity Image Steganography in Wavelet Domain”, IEEE CCNC 2010 Proceedings.

[13] Ramadhan Mstafa , Christian Bach,"Information Hiding in Images Using Steganography Techniques",2013 ASEE Northeast Section Conference

[14] Mohammed A. Saleh,"Image Steganography Techniques - A Review Paper", IJARCCE Vol. 7, Issue 9, September 2018

[15] Harpreet Kau, Jyoti Rani,"A Survey on different techniques of steganography", MATEC Web of Conferences DOI: 10.1051/ 57, 02003 (2016) matec 57 conf/2016 0 ICAET 2016

[16] Iman I. Hamid, "Image Steganography Based on Discrete Wavelet Transform and Chaotic Map",(IJSR) ISSN (Online): 2319-7064 Index Copernicus Value (2016): 79.57 | Impact Factor (2015): 6.391

[17] Veerdeep Kaur Maan, Harmanjot Singh Dhaliwal "Vector Quantization In Image Steganography", (IJERT) Vol. 2 Issue 4, April – 2013 ISSN: 2278-0181

[18] S.V.Kamble , B.G.Warvante,"A Review on Novel Image Steganography Techniques", (IOSR-JCE) ISSN: 2278-0661, ISBN: 2278-8727, PP: 01-04

