A Review on Image Steganography with its Recent Techniques and Applications

Akansha Bhadoria[1],Anuj Bhargava[2],Prashant Badal[3]
[1, 2, 3] Department of Electronics & Communication
[1, 2, 3] SRCEM, Banmore, Morena, India

Abstract*-Steganography is an art of concealing the fact with the purpose of communication, via hiding info in other data. In steganography, a few multiple service file formats are subjugated present, but the digital pictures are most priceless for hiding data motive of their frequency on internet. There is a huge form of techniques of steganography are existing for data hide into images. Each of them has its strong & weak points. Choice of which steganography technique is used it based on the different necessities of the application. For instance, few applications may have requirement of a larger confidential message to be concealed and few requirement complete invisibility of the confidential message. This paper gives an overview of different techniques used for image steganography. Among these following techniques Spatial Domain Approaches Spread Spectrum Technique, Transform Domain Technique, LSB, DCT, DWT techniques points are widely used because of their efficiency.*

Keywords-Image steganography, LSB,DCT,DWT .

I. INTRODUCTION

The time period steganography is resulting from the Greek phrases stegos meaning cover and grafia which means writing [1] defining it as incorporated writing. Image steganography the knowledge is hidden completely in images. It's the practice of embedding/encoding secret info in a method.g the existence of the info is unseen. The actual files can be mentioned to like the cover image, or cover audio message and cover text. Later add the confidential data it is mentioned to as stego medium. A stego-key has been exploiting for hiding encoding procedure to stop extraction or detection of the embedded data. Fingerprinting and Watermarking both are respective to steganography are essentially exploiting for intellectual assets protection necessary. It is naturally exploiting to discern proprietorship of the copyright of such signal. The embedded info in a watermarked object is a signature refers the proprietorship of the data in sequence to make sure copyright protection. In fingerprinting, specific marks and dissimilar are embedded in the copies of the work which dissimilar consumers get. In this situation, that becomes simple for the property owner to search such consumers who give themselves the right to violate their licensing agreement when they illegally transfer the property to other collections [1].

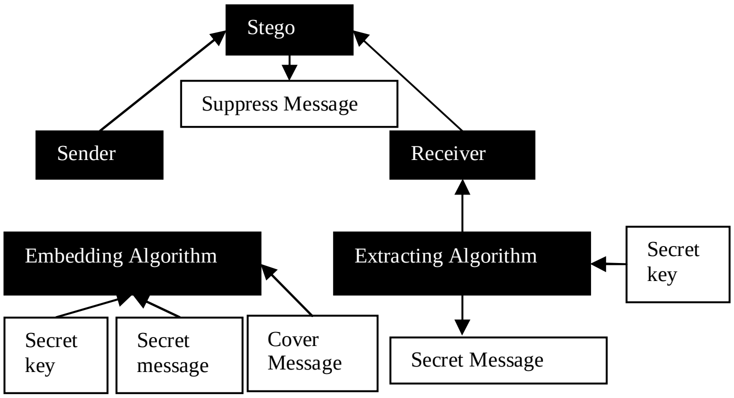

Figure. 1. Steganography System Scenarios

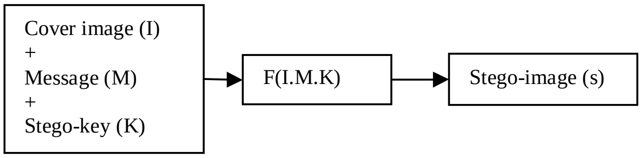

Figure. 2. Simple Steganographic Model

II. IMAGE STEGANOGRAPHY

Taking the cover object like an image in steganography is called as image steganography [2]. Image pixel intensities are exploiting to covertly the info. Dissimilar carrier file formats like audio, video and text can be exploiting but image is more plausible because of its frequency of exploit in the internet. Below shows image steganography model described in Fig 3. Different types of image steganography are

- Spatial Domain Technique
- Transform Domain Technique
- Distortion Techniques
- Masking and Filtering

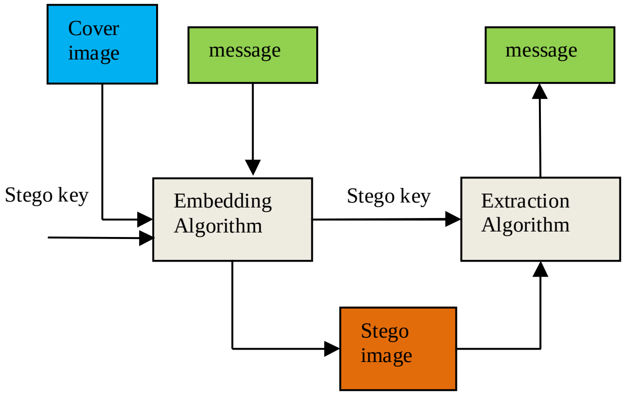

Fig.3: Image Steganographic Model

LSB system is a spatial domain method which exploit the LSB of image pixels to covertly knowledge. In color image 3 bits can be saved in all pixel because red, green and blue plane is represented by 8 bits each respectively. A 300 × 300 pixel picture, can for that reason retailer a total amount of 90,000 bits or eleven,250 bytes of embedded knowledge. A network of 3 pixels of a 24-bit picture can be apparent as follow:

(00101101 00011100 11011100) (10100110 11000100 00001100) (11010010 10101101 01100011)

The number 100, whose binary illustration is 01100100 is embedded into the LSB of above illustrate grid, the outcome is as follows: (00101100 00011101 11011101) (10100110 11000100 00001101) (11010010 10101100 01100011)

The large selection used to be once entrenched into the primary 8 bytes of the grid. Only 5 underlined bits required to be altered pursuance to the embedded message. All primary color has 256 possible intensity. So embedding data in LSB of pixels outcomes in minor modifications in the intensity of the colors. These changes cannot be distinguished by the human eye, thus the message is successfully hidden.

III. TYPES OF STEGANOGRAPHY

Following are the four major types of file formats which may be utilized for steganography.

A. Text Steganography*:*

Message hiding in script is the greatest significant and basic steganography technique. It can be dividing in three categories: format based, random & statistical generation and linguistic method.

B. Image Steganography:

Images are utilized like the popular cover files for steganography. This method deeds the fault of the HVS. Human eyes can’t sense the difference in light of color vectors expressed in terms of 1s and 0s.

C. Audio Steganography:

It engages data hiding within audio files. This technique closes the info in WAV and MP3 audio and AU files. [3]

D. Video Steganography:

It’s a procedure of hiding any files type. In this condition video file is utilized as transporter for conceal the data. Usually DCT change the values that are utilized to covertly the data in every image in the video that is invisible through eye. Mp4, H.264, AVI, MPEG are the formats utilized through video steganography.

E. Protocol Steganography:

It engages hiding the data through the network protocol for example ICMP, IP, TCP, UDP, etc, as envelop item. . Within the OSI layer n/w mannequin there exist covert channels the place steganography can also be exploited [4].

IV. STEGANOGRAPHY TECHNIQUES

1. Spatial Domain Methods:

In this way, the confidential data are embedded straight in the intensity of pixels. It means few pixel values of the image are altered straight during hiding data. Spatial domain methods are categorized into following groups:

I. Mapping pixel to have secreted information procedure
II. PVD
III. EBE
IV. RPE
V. Labeling or connectivity manner
VI. LSB
VII. Pixel power based.

I. LSB: this approach is most generally exploited for hiding info. In this approach the embedding is completed thru exchanging the LSB of image pixels with the bits of confidential message. The image achieved later embedding is similar to the unique image because the modification in the LSB of image pixel doesn't bring too much dissimilarities in the picture.

II. BPCP: In this phase of the picture are exploited thru measuring its complexity. Difficulty is exploited to determine the noisy block In this method noisy blocks of bit plan are changed via the binary patterns mapped from a confidential information.

III. PVD: In this process, two consecutive pixels are elected for embedding the data. The payload is laid down thru checking the dissimilarity amid two consecutive pixels and it serves like a basis for know whether the two pixels pertain to an edge region or smooth region.

2. Spread Spectrum Technique:

The thought of spread spectrum is exploited on this manner. In this method the confidential info is spread over a extensive frequency bandwidth. The ratio of signal to noise in every frequency band must be so small that it's become difficult to detect the existence of data. Even if kind of the data are removed from several bands, there would be still enough information is present in other bands to recover the data. Thus, it is problematic to eliminate the data wholly without fully destroying the cover .It is a very robust technique mostly exploited in military communication.

3. Statistical Technique:

In the technique message is embedded by changing several assets 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 one, otherwise no modification is required.

4. Transform Domain Technique:

In this technique; the confidential message is embedded in the transform domain of the cover. This is a difficult approach of hiding messages in an image. Different transformations and algorithms are exploited on the image to covertly message in it. Transform domain approaches are categorized such as

i) Discrete Wavelet transformation method (DWT)
ii) Discrete cosine transformation method (DCT)
iii) Discrete Fourier transform technique (DFT)
iv) Reversible or Lossless technique (DCT)
v) Embedding in coefficient bits

5. Distortion Techniques:

In this process the confidential data is savedthru distorting the signal. A sequence of modification is applied to the cover thru the encoder. The decoder procedures the dissimilarities amid the distorted cover to detect the sequence of the modifications and consequently recover the secret message.[5]

6. Masking and Filtering:

These procedures hide infothrucreate an image. Steganography only covertly the information where as watermarks become a potion of the image. These techniques embed the info in the more significant areas rather than hiding it into the noise level. Watermarking methods can be applied without the phobia of image destruction cause to lossy compression as they are more integrated into the image. This method is basically used for 24-bit and gray scale images [6]

IV. APPLICATION

Applications for Steganography in an Open Systems Atmosphere In this phase we will look at some of the possible applications for steganography and then close by pointing out some of the more popular steganographic tools available today. The 3 most valuable and studied exploit for steganography in an open techniques surroundings are covert channels, digital watermarking and embedded information.

A. Covert channels in TCP/IP include masking identification info in the Internet when absolute secrecy is required for awhole communication procedure and not just one document as mentioned next.

B. Exploiting containers (cover messages) to embed secret messages into is by far the most use of Steganography today. This process of Steganography is suitable when a party must transfer a private or very sensitive document over an open systems atmosphere for instance the Internet.

C. Thru embedding the hidden data into the cover message and transfer it, you than a harmless message other than the intended receivers.[7]

V. PROBLEM STATEMENT

As we know that steganography is a message hiding technique so that a user can send or communicate to the other user about their secret message securely. LSB is one of the most general techniques that is exploited for hiding the confidential data. LSB hiding method works as it hides the secret message straight in the two LSB in the image pixels, that affects the image resolution, cause to this it decreases the image quality and create the image simple to attack. Therefore there may be one probability to remove this problem and create the secret message more secure and enhance the quality of the image is proposed. The proposed method hides the secret message depend on searching about the identical values amid the image pixels and secret messages. By using this proposed method the image will remain same after encoding or hiding the confidential data in the image. It will not affect the image resolution.

VI. LITERATURE SURVEY

[8] Md. Rashedul Islam (2014) et al present that original Steganography method is being developed to hide big data in Bitmap image exploiting filtering depend algorithm, That make the most MSB bits for filtering intent. This procedure exploits the concept of status checking for retrieval and insertion of message. This procedure is an reform of LSB manner for hiding info in images.

[9] Zohreh Fouroozesh (2014) et al present that Image-steganography is the most appreciable kind of carrier to hold info. Several algorithms have been defined to hide info into digital images. The LSB is one of these algorithms which are broadly exploited in steganography. Many reformation of this algorithm have been defined lately. Analyze the the brink adaptive picture steganography and LSB matching revisited (LSBMR) algorithm depend on LSBMR. observance many experiments on these algorithms on a group of 200 images and we illustrate that an reformation can be create thru exploiting few image processing method known as Sobel edge detection to search edges of the picture which can hold the secret info. Show that the proposed technique can improve the amount of the steganography images where sharper edges are used for low capacity rate.

[10]Present that an improved LSB depend Steganography method for images imparting better info security for hiding confidential info in images. There is a huge form of steganography methods few are more than others and each of them have respective weak and strong points. The eavesdroppers don't have any doubt which message bits are hidden in the regular and image steganography detection approaches can’t estimate the length of the confidential message correctly. Present improved steganalysis methods, depend on the most reliable detectors of thinly-spread LSB steganography presently known, focusing on the case when grayscale Bitmaps are used as cover images.

[11]et al present that a newest steganographic attack that can losing audio steganography algorithms while keep an admissible audio deformation level. The attacking method is depend on a define transform known as discrete spring transform. Alike to the time scale alteration, the spring transformation disables the synchronization of the hidden information. Also, the defined manner has few benefits over the traditional time scale alteration, therefore the steganography technique that can resist to the time scale modification still can be defeated by the define technique [15].

[12]A robust image steganography process depends on redundant discrete wavelet transforms has been define. Steganography is the approach of hiding one intermediate of conversation like textual content, audio and photograph inside a different. The define steganography algorithm exploits blind recovery method. We have tested the define way on dissimilar payload and cover images. Simulated outcomes are examined exploiting PSNR and BER.

[13] Personal picture is hiding into two more than one domains like DWT and IWT. The secret image and cover image co-efficient values are embedded thru 512*512 exploiting fusion process methods. The applied several groupings of IWT and DWT on images and achieved a good quality stego images.

[14] A digital image is examined and depend on this study an LSB depend steganographic algorithm is planned. Using this algorithm software is developed and its performance is compared with various other steganographic tools available on the internet.

[15] A newest Steganography method implemented and analyzed and exists. The define manner hides the secret message depend on searching about the identical bits amid the secret messages and image pixels values. The define technique is equated with the LSB benchmarking way. It is implemented to covertly de the confidential message "I will come to see you on the first of June" on two Bmp images, with size (24 x 502 x 333) and (24 x 646 x 165) respectively.

[16] The rapid development of data transmit thru internet has create it simple to transmit the info faster and accurate to the target, but in sequence to transfer the data securely to the receiver without any alterations, there are several methods like steganography. The idea of steganography exploiting “LSB METHOD” is introduced.

[17] A newest transform domain image stenographic method DWTDM is existing where confidential data is embedded in adjacent DWT coefficient changes. The dynamic range of the DWT dissimilarity considered while extraction of data that outcomes an robust and efficient stenographic method that can avoid many image attacks and completely well for both uncompressed and compressed domain.

[18] In the confidential info are encrypted exploiting encrypted information and RSA algorithm is embedded in the LSBs of randomly selected pixels. The end user has given the choice of inputting one to maximum three messages. These strategies also explain an extracts the encrypted expertise at the receiving finish and decryption of it to get original info and aid to obtain better capability and protection to misgiving.

[19] The Hash based LSB procedure for steganography in that place of LSB for hiding the text messages is made up our minds based on hash function. Hash function search the position of LSB of all RGB pixel's .Then the Hash LSB technique uses the values provided by hash function to hide the data.

[20] Genetic Algorithm in this technique, it will translate text message into binary type. Then that binary message is encrypted. After that it will convert encrypted message in numeric form. After that it will divide this numeric form by single digits. And it is going to get dividend, quotient and reminder and deviser. Presently a few pictures are as cover to cover these records. It also calculates LSB of each pixels of each image. This LSB is replaced thru the bit of encrypted message one by one.

[21] This article projected a better LSB based Steganography method for images reporting improved data security for thrashing covert information in pictures. In this item we shows enhanced steganalysis techniques, depend on the mainly trustworthy detectors of thinly-spread LSB steganography currently known, focusing on the situation when grayscale Bitmaps are exploited as cover images

VII. COMPARISON TABLE OF STEGANOGRAPHY TECHNIQUES

Domain	**Algorithm**	**Invisibility**	**Capacity**	**Robustness**	**Security**	**Complexity**
spatial	LSB	High	1-3bpp	Low	Low	Low
	PIT	Medium	>1bpp	Low	High #	Low
	OPAP	Medium	1bpp	Low	High	Medium
	Shabnam samima et al [23]	Very High	2bpp [23]	High	High	Medium
	Ratnakirti roy et al [26]	Very high	NA*	High	High	Medium
transform	Jsteg	Medium	<1 bpnc	Medium	High	Medium
	Outguess	High	0.4 bpnc	Medium	High	High
	F5	Very High	0.8 bpnc	Medium	High	High
	Po-Yueh Chen et al [14]	Medium	<1 bpnc	High	High	Medium
	Tanmay Bhattacharya et al [21]	High	<1 pbnc (3 secret images per cover image)	Medium	High	Medium
	Swapnali zagade et al. [24]	High	<1 bpnc	High	High	Medium

#.Till capacity <3 bpp. *. Capacity varies on the degree of mapping it cannot be calculated in bpp. Bpp-bit per pixel bpnc-bit per non-zero coefficient.

VIII. CONCLUSION

Even though only few of the main image steganography process were discussed in this paper, researcher can observe that their current a big choice of approaches or methods to hiding confidential info in images. All these techniques try to satisfy three most vital elements of steganographic design i.e. capacity, undetectability, and robustness. Spatial domain LSB techniques have a high payload capacity, but they frequently fail to prevent the statistical attacks. So they are detected easily. Especially when the hidden message is minor, the promising methods like DCT and adaptive steganography and DWT are not prone to attacks. They change the coefficients in transform domain, resulting in the minimum image distortion. Experiments on DCT coefficients introduced liberal of promises outcomes and diverted researchers‟ attention towards JPEG images.

Message embedding in the DWT domain reveals the constructive results and it outperforms the DCT embedding. For all these benefits, DCT and DWT are superior choices.

REFERENCES

[1] Parmar Ajit Kumar Maganbhai1 , Prof. Krishna Chouhan, “A Study and literature Review on Image Steganography”. (IJCSIT) 2015

[2] Yamuna Dasar , Preethi. P, “A Secure Image Steganography Based on RSA Algorithm and Random Pixel Selection Technique”.IJRETM 2015

[3] Hemang A. Prajapati & Dr. Nehal G. Chitaliya “Secured and Robust Dual Image Steganography: A Survey” International Journal of Innovative Research in Computer and Communication Engineering Issue 1, January 2015

[4] Jasleen Kour & Deepankar Verma “Steganography Techniques –A Review Paper” worldwide paper of Emerging Research in Management &Technology ISSN: 2278-9359 (Volume-3, Issue-5).

[5] Hui Tian, Jie Qin, Yongfeng Huang, Yonghong Chen, Tian Wang, Jin Liu, Yiqiao Cai “Optimal matrix embedding for Voice-over-IP steganography” College of Computer Science and Technology, National Huaqiao University, Xiamen 361021, China

[6] Divyanshu Triapthi , Yash Kumar Singh , Rohit Singh, “A Review on Digital Image Steganography with its Techniques and Model” IJSART 2016

[7] Palak R Patel, Yask Pate,” Survey on Different Methods of Image Steganography” IJIRCCE,2014

[8] Md. Rashedul Islam, Ayasha Siddiqa, Md. Palash Uddin, Ashis Kumar Mandal and Md. Delowar Hossain,” An Efficient Filtering Based Approach Improving LSB Image Steganography using Status Bit along with AES Cryptography”, 3rd INTERNATIONAL CONFERENCE ON INFORMATICS, ELECTRONICS & VISION 2014 IEEE

[9] Zohreh Fouroozesh and Jihad Al jam,” Image Steganography based on LSBMR using Sobel Edge Detection”, 2014 IEEE, pp: 141- 145.

[10] Manu Devi and Nidhi Sharma,” Improved Detection of Least Significant Bit SteganographyAlgorithms in Color and Gray Scale Images”, Proceedings of 2014 RAECS UIET Panjab University Chandigarh, 06 – 08 March, 2014 IEEE.

[11] Qilin Qi, Aaron Sharp, Dongming Peng, Yaoqing Yang and Hamid Sharif,” An Active Audio Steganography Attacking Method using Discrete Spring Transform”, 2013 IEEE 24th International Symposium on Personal, Indoor and Mobile Radio Communications: Services, Applications and Business Track, 2013 IEEE, pp: 3456-3460.

[12] Siddharth Singh and Tanveer J. Siddiqui,” Robust Image Steganography Technique Based on Redundant Discrete Wavelet Transform” ©2012 IEEE

[13] Prabakaran G, Dr. Bhavani R,” Dual Wavelet Transform in Color Image

[14] Steganography Method” International Conference on Electronics and Communication System ICECS, 2014

[15] Kaustubh Choudhary,” Image Steganography and Global Terrorism” Global Security Studies, Fall 2012

[16] Atallah M. Al-Shatnawi,” A New Method in Image Steganography with Improved Image Quality”,2012

[17] Rahul Joshi1, Lokesh Gagnani2 , Salony Pandey3 “Image Steganography With LSB” (IJARCET), 2013

[18] Souvik Bhattacharyya, Gautam Sanyal,” A Robust Image Steganography using DWT Difference Modulation (DWTDM)” © 2012 MECS

[19] Yamuna Dasar, Preethi. P, “ A Secure Image Steganography Based on RSA Algorithm and Random Pixel Selection Technique”. IJRETM-2015

[20] Anil Kumar, Rohini Sharma, “A Secure Image Steganography Based on RSA Algorithm and Hash-LSB Technique”. International Journal of Computational Science & Software Engineering, Volume 3, 2013.

[21] Chital R. Gaidhani, Vedashree M.Deshpande and Vrushali N.Bora, “Image Steganography for Message Hiding Using Genetic Algorithm”, 30 March 2014.

[22] Manu Devi, Nidhi Sharma, “Improved Detection of Least Significant Bit SteganographyAlgorithms in Color and

Gray Scale Images”. 978-1-4799-2291-8/14/$31.00 ©2014 IEEE

[23] Pooja Rai, Sandeep Gurung, M.K. Ghose, “Analysis of Image Steganography Techniques: A Survey”. International Journal of Computer Applications (0975 – 8887)2015