IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 12, Issue 2, February 2023

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.118

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.118| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 2, February 2023 ||

| DOI:10.15680/IJIRSET.2023.1202084 |

A Survey on Information Hiding Within ImageUsing Image Steganography Technique

V.C.Sanap[1], Yashraj Pillay[2], Premraj Rupnar[3], Rohit Pithani[4], Vardhan Raisoni[5]

Lecturer, Dept. of Computer Engineering, A.I.S.S.M.S. Polytechnic Pune, Maharashtra, India[1]

Student, Dept. of Computer Engineering, A.I.S.S.M.S. Polytechnic Pune, Maharashtra, India[2,3,4,5]

ABSTRACT: The prompt development of data transfer through internet made it easier to send the data accurate and faster to the destination. One of the most prime factors of information technology and communication has been the security of the information. The process of hiding the information in other information without change is known as Steganography. For security Cause the concept of Steganography is being used. Steganography is art and science of concealed communication. Image steganography refers to hiding information i.e. content, images or audio files in another image or video files. Steganography is the method through which extant of the message can be kept secret. Attacks, misuse or unofficial access of information is of great study today which makes the protection of documents through digital media is a priority problem. Digital images are universally used in order to store the information. For hiding secret information in images, there exists a large variety of techniques.. The proposed method hides the secret message based on searching about the identical bits between the secret messages and image pixels values

KEYWORDS: Steganography, least significant bit, secret information, Carrier File, Decryption, Encryption, digital image, image steganography.

I. INTRODUCTION

Steganography refers to the art of covert communications. The message is embedded among another object referred to as a cover Work, by tweaking its properties. It become additional necessary as additional folks be part of the computer network revolution. Steganography is that the art of concealing information in ways in which prevents the detection of hidden message. A completely unique methodology is projected to produce additional security for the key information with the mixture of compression and encoding methodology. It needs less memory house and quick transmission rate as a result of compression technique is applied. We have a tendency to review the various security and knowledge concealing techniques that sqaure measure accustomed implement a steganography like LSB, ISB and MLSB etc. Image steganography is performed for images and also the regarding the knowledge is additionally decrypted to retrieve the message image. Steganography is that the science that involves communication secret knowledge in associate in nursing applicable trasmission carrier.

It's been propelled to the forefront of current security techniques by the exceptional growth in process power, the rise in security awareness by, e.g., people, groups, agencies, government and through intellectual pursuit. With procedure on the opposite hand, different, distinctive marks sqaure measure embedded in distinct copies of the carrier object that sqaure measure equipped to totally different customers. This allows the belongings of owner to spot customers who break their licensing agreement by supplying the property to third parties. This paper describes the LSB algorithmic program used for image steganography to parenthetically the safety potential of steganography for business and private use.

The most popular medium used is image files owing to their high capability and simple convenience over the internet. At the sender's aspect, the image used for embedding the secret message is called cover image, and therefore the secret information that has to be protected is known as a message. As shortly as information are embedded using some appropriate embedding algorithm, then it is called stego image. This stego image is transferred to the receiver, and he extracts out the key message using extraction formula. Another information hiding technique, cryptography is aditionally used for secure transmission of messages over the web, however steganography is changing into a lot of in style owing to its benefits over cryptography. Cryptography hides the precise which means of message from the third party whereas steganography hides the terribly existence of the message itself.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.118| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 2, February 2023 ||

| DOI:10.15680/IJIRSET.2023.1202084 |

Adaptive steganography utilizes image options and content information to enhance the embedding process. For example, less detectable artifacts is also introduced into the cover image by the embedding technique. In some cases these artifacts square measure detected with problem by steganalysis methods thanks to trivial changes introduced in image statistics. No matter how, the artifacts may be visually perceptible to the human eye. Therefore, sensory activity undetectability is incredibly important in steganography. This suggests that applying a steganography technique to an image should not leave any visually perceptible phenomena. To support this idea and improve hardiness of watermarking methods, perceptual models, like Watson's visual model, were proposed to describe the human sensory system. The strategies which use the human visual model in steganography square measure mentioned within the next section.

II. RELATED WORK

The concept of image inpainting was first introduced by Bertamio et al. [1]. The method was inspired by the real inpainting process of artists. The image smoothness information interpolated by the image Laplacian is propagated along the isophotes directions, which are estimated by the gradient of image rotated by 90 degrees. Exemplar Based method proposed by Criminisi et al. [2] used a best exemplar patch to propagate target patch including missing pixels. This technique uses an approach which combine structure propagation with texture synthesis and hence produced very good results. In [3], the authors decompose the image into sum of two functions and then reconstruct each function separately with structure and texture filling-in algorithms. Morphological technique is used to extract text from the images presented in [4]. In [5], the inpainting technique is combined with the techniques of finding text in images and a simple algorithm that links them. The technique is insensitive to noise, skew and text orientation. The authors in [6] have applied the CCL (connected component labelling) to detect the text and fast marching algorithm is used for Inpainting.
The work in this paper is divided in two stages. 1) Text- Detection 2) Inpainting. Text detection is done by applying morphological open-close and close-open filters and combines the images. Thereafter, gradient is applied to detect the edges followed by thresholding and morphological dilation, erosion operation. Then, connected component labelling is performed to label each object separately. Finally, the set of selection criteria is applied to filter out non text regions. After text detection, text inpainting is accomplished by using exemplar based Inpainting algorithm.

III. METHODOLOGY

Least Significant Bit Technique :-
Least significant bit (LSB) insertion may be a common, straightforward approach to embedding data in a cover image. The lsb bit in different words, the 8th bit of some or all of the bytes within an image is modified to a bit of the key message. Once employing a 24-bit image, a bit of each of the red, green and blue colour components are often used, since they're each represented by a computer memory unit(byte). In different words, one will store 3 bits in each pixel. An 800 × 600 pixel image, will so store total quality of 1,440,000 bits or 180,000 bytes of embedded information. Within the LSB technique of Message concealing, the least significant bit was replaced by the message bit of the key message. We tend to evaluated the technique victimization gray scale images of size 64*64 whitin which each pixel value was portrayed with 8 bit illustration.

For Example –

Lets take an example whereby once the number 300 (representation in binary: 100101100) implemented into the least significant bits of this part of the Cover image. If we have a tendency to overlay these nine bits over the LSB of the nine bytes higher than, we have a tendency to get the subsequent (where bits in bold have been changed)

10010101 00001100 11001000

10010111 00001110 11001011
10011111 00010000 11001010

After embedding the message into the cover image, the stego image are going to be obtained, and so this stego image was remodeled with the DWT transformation technique so any hacker can't realize wherever the message was

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.118| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 2, February 2023 ||

| DOI:10.15680/IJIRSET.2023.1202084 |

embedded. At the receiver finish the inverse DWT is applied, when steganography the initial image and message are going to be obtained. Secrete information will be hide in image method is termed LSB steganography method whereas retrieving secret information from stego image is termed LSB steganography process that is shown in figure.

Encryption :

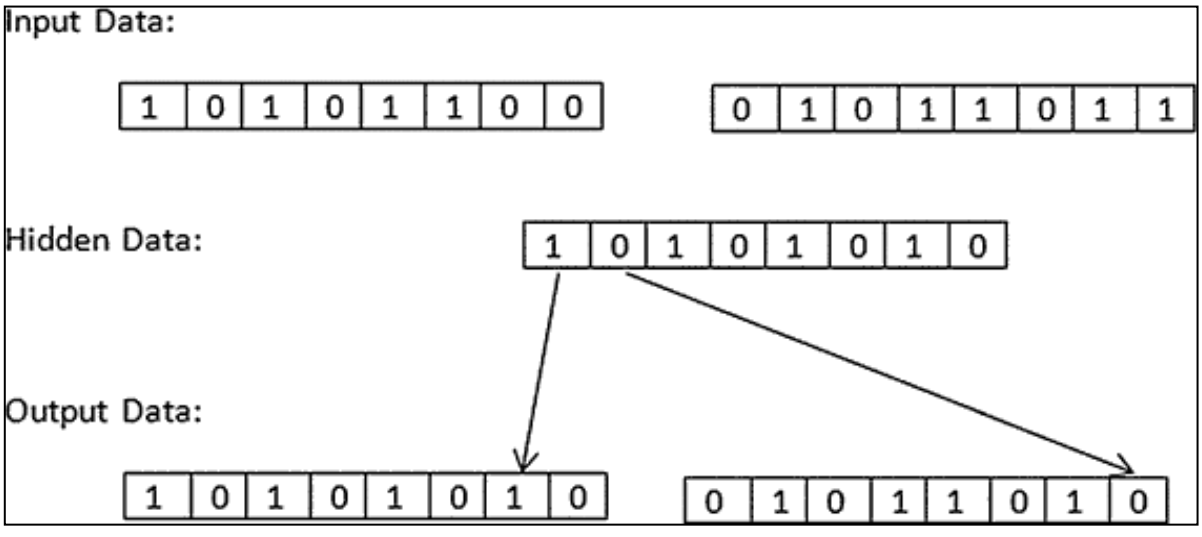
An image portrayed as associate in nursing N*M (in case of greyscale images) or N*M*3 (in case of color images) matrix in memory, with every entry representing the intensity value of a element. In image steganography, a message is embedded into an image by fixing the values of some pixels, that area unit chosen by an encryption algorithm. The recipient of the image should remember of the constant algorithm in order to realize which pixels he or she should choose to extract the message. Detection of the message at intervals the cover image is done by the method of steganalysis. This could done through comparison with the cover image, bar chart(histogram) plotting, or noise detection. Whereas efforts area unit being invested with developing new algorithms with a bigger degree of immunity against such attacks, efforts are also being devoted towards up existing algorithms for steganalysis, to sight the exchange of secret data between terrorists or criminal components.

Decryption :

Decryption could be a method that transforms encrypted data into its original format. The process of encryption transforms data from its original format — known as plaintext — into an indecipherable format
— known as ciphertext — whereas it is being shared or transmitted. To do this, parties to a individual conversation use an encryption theme, known as an algorithmic rule, and therefore the keys to encode and decode messages. Encrypted messages known as ciphertext, as algorithms are also known as ciphers. Message recipients rewrite the data back to its original, clear format.

III. EXPERIMENTAL RESULTS

As shown in [A], The Least Significant Bit (LSB) [93] method is the easiest way to embed secret information. By replacing the minimum weighting value of a sampled speech signal with binary bits of secret information data, the secret information can be hidden in the speech.



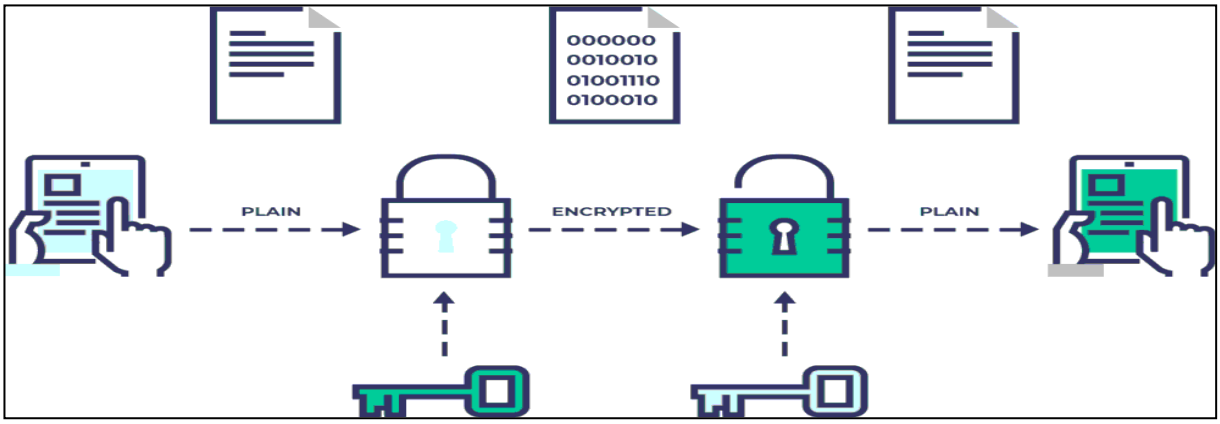
[A]Fig. Leastsignificant bit

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.118| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 2, February 2023 ||

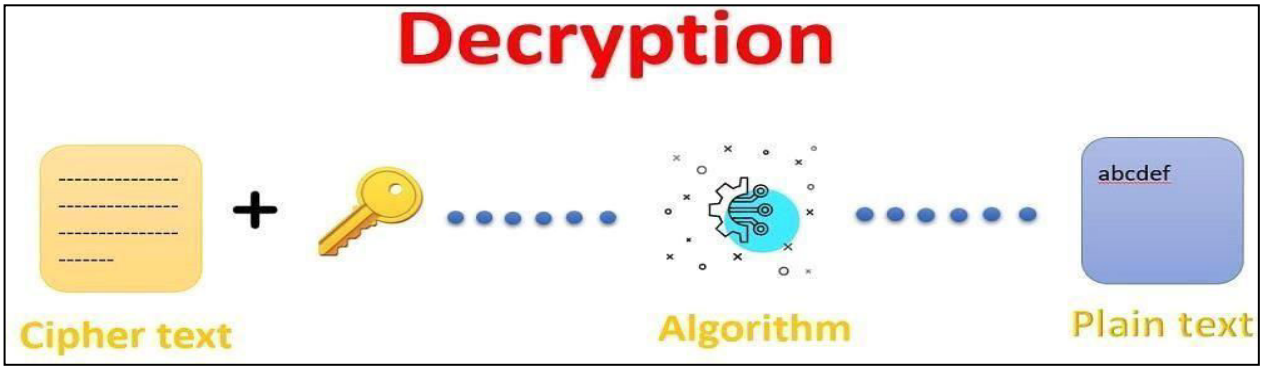
| DOI:10.15680/IJIRSET.2023.1202084 |

As shown in [B], Sender picture is hidden in the carrier picture. In this technique, sender image pixel value has to convert in binary form, and then, this binary value hides in LSB of carrier image pixel bytes. Using this technique, the secret image is hidden in the cover picture and protects the secret picture or hidden picture



[B]Fig. EncryptionMethod

As shown in [C], The recipient of decryption receives a prompt or window in which a password can be entered to access the encrypted data. For decryption, the system extracts and converts the garbled data and transforms it into words and images that are easily understandable not only by a reader but also by a system.



[C]Fig. Decryption Method

IV. CONCLUSION

A stego-key has been applied to the system throughout embedment of the message into the cover image. This steganography application software package provided for the aim to a way to use any variety of image formats to activity any variety of files within their. The master work of this application is in supporting any variety of images without need to convert to bitmap, and lower limitation on file size to cover, due to

victimisation most memory space in images to cover the file. The application creates a stego image during which the private knowledge is embedded within the cover file image.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.118| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 2, February 2023 ||

| DOI:10.15680/IJIRSET.2023.1202084 |

REFERENCES

1. Dr. Ekta Walia, Navdeep and Payal Jain. ***"An analysis of LSB & DCT based Steganography."*** GlobalJournal ofComputer Science and Technology, April 2010.
2. D. Sellars. "***An introduction to steganography.***
3. Internet:http://www.cs.uct.ac.za/courses/CS400W/papers99/stego.html [Jul., 2011].
4. H. Farid. ***"Detecting Hidden Messages Using Higher-Order Statistical Models"***, Proceedings of theInternationalConference on Image Processing, Rochester, NY, USA, 2002.
5. Balajee, J. "***MATLAB CODING's – PART II."*** researchviews.blogspot.com. N.p., 21 Nov. 2012.Web. 12 Dec.2015.
6. Atul Kahate," ***Cryptography & Network Security",*** Tata McGraw-Hill Education, 2003.
7. J. Fridrich, ***"Feature-based steganalysis for jpeg images and its implications for future design of steganographicschemes",*** Proc. of the 6th Information Hiding Workshop, Springer, vol. 3200 , pp. 67-81,2004.
8. R. Bohm and A. Westfeld. ***"Breaking cauchy model-based JPEG steganography with first orderstatistics."*** InProc. of ESORICS'2004, 2004. pp. 125-140.
9. Shikha, and Vidhu Kiran Dutt. "***International Journal of Advanced Research in Computer Science andSoftwareEngineering."*** Http://www.ijarcsse.com/. N.p., Sept. 2014. Web.
10. R. Gonzales, R. Woods, and S. Eddins. ***"Digital Image Processing Using MATLAB",*** PublishingHouse ofElectronics Industry, ISBN: 7-5053-9876-8, 2004.
11. D.C. Lou, J.L. Liu, H.K. Tso, Evolution of information –hiding technology, in H. Nemati (Ed.), Premier Reference Source–***Information Security and Ethics: Concepts, Methodologies, Tools and Applications,*** New York: Information Science Reference, 2008, pp. 438-450.
12. M. Juneja and P.S. Sandhu. ***"Designing of robust image steganography technique based on LSB insertion and encryption."*** IEEE International Conference on Advances in Recent Technologies in Communication and Computing, 2009, pp. 302-305.
13. K. B. Raja, Kiran Kumar. K, Satish Kumar. N, Lashmi. M. S, Preeti. H, Venugopal. K. R. and Lalit. M.Patnaik ***"Genetic algorithm based steganography using wavelets,"*** International Conference on Information System Security Vol. 4812, pp, 51-63. 2007.

INNO SPACE
SJIF Scientific Journal Impact Factor
Impact Factor: 8.118

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

Scan to save the contact details