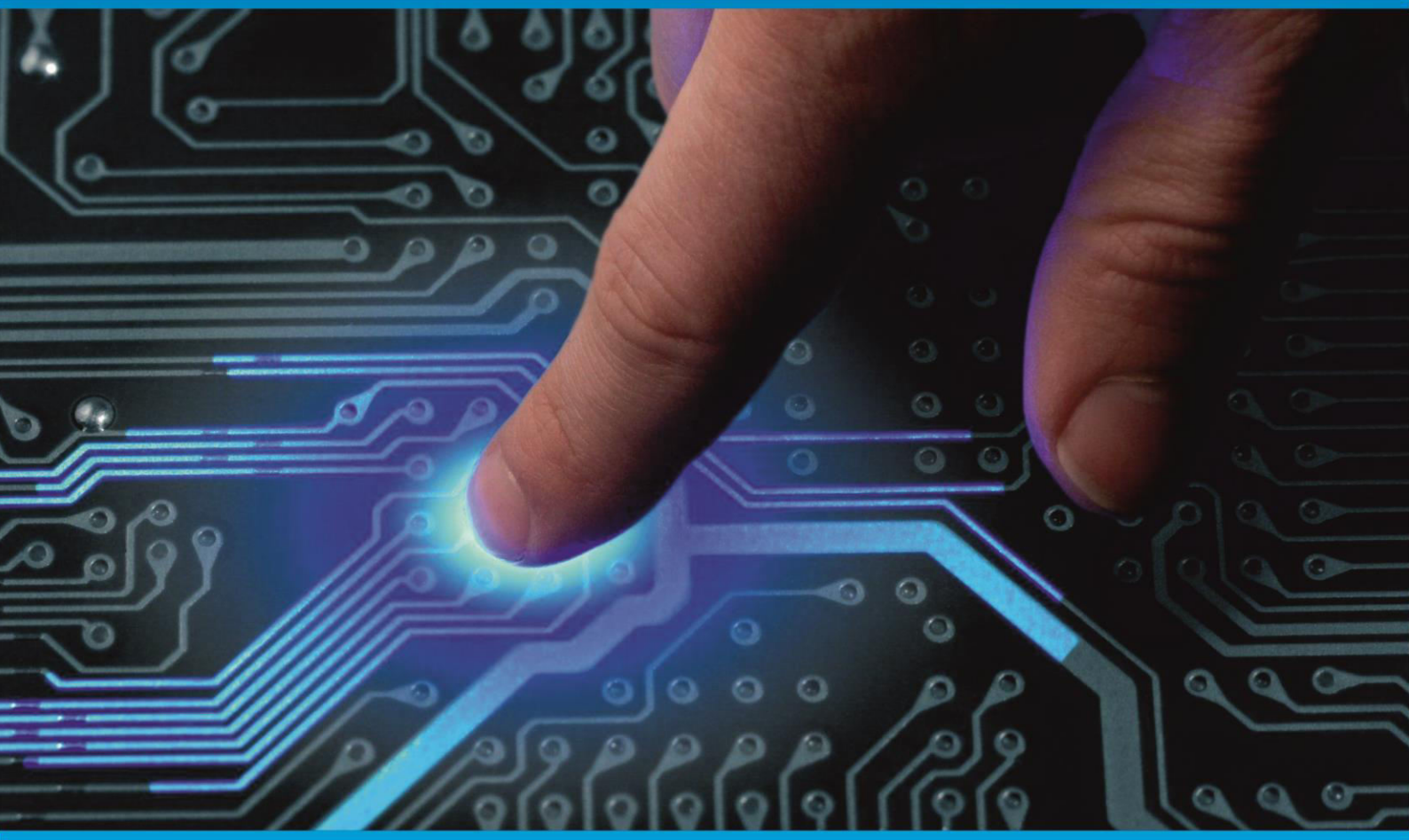
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 9, Issue 3, March 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.488

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 3, March 2021 ||

| DOI: 10.15680/IJIRCCE.2021. 0903135|

Application Based on Image Steganography using Least Significant Bit Method

Agalya R[1], Varshaa S[2], Varshanthini R[3], Senthil P[4]

U.G. Student, Department of IT, S.A. Engineering College, Chennai, India[1,2,3]

Assistant Professor, Department of IT, S.A. Engineering College, Chennai, India[4]

ABSTRACT : Steganography is the art of concealing the fact that contact is taking place by encasing data in other data. There are numerous carrier file formats that can be used, but digital images are the most common due to their prevalence on the internet. Various applications may necessitate complete invisibility of the secret information. Steganography conceals the encoded message inside the host data and delivers it in an imperceptible manner that is to be accurately transmitted to a recipient. The host dataset has been purposefully corrupted, but in a covert manner that is designed to be invisible to an information analysis. This project intends to give an application that hides any files in an image file by converting it into BMP file using Least Significant Bit Method**.**

KEYWORDS : Steganography, Stego-image, Least Significant Bit Method, Cover image, Visual distortion, Data security**.**

I. INTRODUCTION

The practice of concealing a message within another message or a physical object is known as Steganography. It is the practice of concealing secret data inside a non-secret file or message to prevent detection; the secret data is then retrieved at its destination. Steganography can be used in conjunction with encryption to conceal or protect data. Image Steganography is the method of concealing data inside an image file. The image chosen for this reason is referred to as the cover – image and the image obtained after steganography is referred to as the stego - image.

II. RELATED WORKS

1. LSB Steganography: A New Approach to Data Hiding
Author : G. Prashanti and K. Sandhyarani

2015: G. Prashanti and K. Sandhyarani [1] conducted a survey on recent LSB-based image steganography achievements. The authors of this survey explore how to improve steganography results such as robustness, embedding capability, and un-detectability of hidden information. Two new methods are also suggested in conjunction with this survey. The first method involves embedding data or hidden messages into the cover image, while the second method involves embedding a secret grey scale image into another grey scale image. These methods employ a four-state table to generate pseudo-random numbers**.**

2. An Improved Inverted LSB Image Steganography
Author : N. Akhtar et al.

2014: N. Akhtar et al. [2] in present and implement the improved version of traditional LSB image steganography technique. Their work enhances the standard of stego image using bit inversion method. They propose and implement two techniques for bit inversion. These both techniques resolves around bit inversion techniques during which LSBs of pixels of carrier image are inverted only and as long as they arise with specific pattern of pixel's bits. This results in lesser modification in pixels is compared to traditional LSB method. For correct retrieval of secret message, inverted bits got to be embedded somewhere within the stego image. The PSNR value of the stego image has improved as a result of the experiments, and thus the stego image quality has improved.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 3, March 2021 ||

| DOI: 10.15680/IJIRCCE.2021. 0903135|

3. A Novel approach for Edge Adaptive Steganography on LSB insertion technique
Author : P. U. Deshmukh et al.
2014: P. U. Deshmukh et al. [3] also present the edge adaptive steganography based on LSB substitution. They use an adaptive scheme and the difference between two adjacent pixels of the carrier image to embed secret information in sharp (edges) regions of the carrier image. Their method outperforms other LSB and pixel difference-based techniques while maintaining stego image quality.

4. Image Steganography Using an Improved Least Significant Bit Algorithm
Author : S. Gupta et al.
2012: S. Gupta et al. [4] proposes an enhanced LSB algorithm for image steganography. Only the blue portion of the RGB color space is used to encode hidden information in this proposed work. In their technique first M×N size cover image is selected. After selection of cover image only blue component is used for embedding secret information. They also make use of pixel filters to access the best regions to embed information in cover image to obtain best possible rate. Experiments show that this technique reduces cover image distortion, and that the stego image has very good visible quality, and that changes in the cover image are not harmful to the human visual system (HVS). Because only blue components are used to embed the secret information, the colour leap is reduced in this method.

5. A Replacement Approach for LSB Based Image Steganography using Secret Key
Author : S. M. M. Karim et al.
2011: S. M. M. Karim et al. [5] proposed a replacement approach that gives excellent security to secret data. They use LSB approach with secret key. This secret key's will not hide the sensitive information and this information is stored on different LSB bits of image. This steganography technique use RGB true colour images for embedding process. This system embeds the key information inside in LSB of the duvet image and secret key's will not encrypt the key information to avoid unauthorized access. Depending upon the key used, secret information is randomly stored on different location of LSBs of canopy image which make this technique more robust and make difficult for attacker to extract the hidden secret information. Experimental results represent that this method generates good PSNR value and supply greater security to hidden information than traditional LSB based steganographic method.

6. Adaptive LSB Replacement as a High-Capacity Image Data Hiding Scheme
Author : H. Yang et al.
2009: H. Yang et al. [6] presented a new adaptive LSB based method for image steganography. For improved stego image quality, it employs the pixel adjustment technique. This adaptive LSB substitution leads to high hidden capacity. LSB based image steganography method is proposed to hide the info common bit pattern is employed. According to the message and therefore the pattern bits LSB's of pixels are modified. This method has low hidden capacity.

III. IMAGE STEGANOGRAPHY

In our project we propose a new approach to hide any type of data file behind an image using Least Significant Bit method. In this method the least significant bit pixels of the cover image is adjusted to store data. This varies according to the number of bits in an image. The Least Significant Bit method works well with BMP images because the compression is lossless. In our application we can hide any files including text, image, audio, video and archive files behind an image using Least Significant Bit Method.

To overcome the drawbacks of existing system we use an approach called Least Significant Bit method. Using this method we increases the capacity of the application up to 1MB in cover image so that we can avoid visual distortion that appears when we hide an information more than the capacity of the cover image. In other way we can also hide files more than the achieved capacity by compressing it as .zip or .rar files within 1MB.

The Inscribe or Encryption module deals with the process of hiding the secret data into the cover image. The sender should be able to hide the secret message in an image file without causing visible changes to the image. The secret data is hidden in an image using the Least Significant Bit (LSB) technique. The embedding process in the LSB technique consists of the sequential substitution of each least significant bit of the image pixel with the bit values of the secret message to be hidden. This module requires any image and message and gives only one image file in destination.

The Efface or Decryption module deals with the extraction of the secret data from the encrypted image. We can remove the least significant bits from the image to get the hidden information using the LSB technique as the embedding algorithm. This module requires an encrypted image and selected save path to extract the secret data from the encrypted image.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 3, March 2021 ||

| DOI: 10.15680/IJIRCCE.2021. 0903135|

IV. EXPERIMENTAL RESULTS

Figure shows the results of hiding information into an image by using Least Significant Bit algorithm. Figure (a) shows the outlook of user interface used to encrypt and decrypt the data file into an image.

fig (a)

Figure (b) shows a data file successfully concealed into an image after applying the Least Significant Bit algorithm.

fig (b)

Figure (c) shows the original data file successfully extracted from the encrypted image.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 3, March 2021 ||

| DOI: 10.15680/IJIRCCE.2021. 0903135|

fig (c)

IV. CONCLUSION

This paper demonstrates about the image steganography using Least Significant Bit method. This method helps to hide information by adjusting the least significant bits of an image pixel to store data. It increases the storage capacity and can hide any files like image, text, audio, video. It helps to communicate in a completely undetectable manner. Also it is expected furthermore for future enhances.

REFERENCES

1. G. Prashanti, K. Sandhyarani, "A New Approach for Data Hiding with LSB Steganography", Emerging ICT for Bridging the Future - Proceedings of the 49th Annual Convention of the Computer Society of India CSI, Springer 2015, pp. 423- 430.
2. N.Akhtar, S.Khan and P. Johri, "An Improved Inverted LSB Image Steganography", IEEE International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT), Feb. 2014, pp. 749- 755.
3. P.U. Deshmukh and T.M. Pattewar, "A Novel Approach for Edge Adaptive Steganography on LSB Insertion Technique" IEEE International Conference on Information Communication and Embedded Systems (ICICES), Feb. 2014, pp. 1-5.
4. S. Gupta, G. Gujral and N. Aggarwal, "Enhanced Least Significant Bit Algorithm for Image Steganography", International Journal of Computational Engineering & Management, July 2012, pp. 40- 42.
5. S. M. M. Karim, M. S. Rahman, and M. I. Hossain, "A New Approach for LSB Based Image Steganography using Secret Key", Proceedings of 14th IEEE International Conference on Computer and Information Technology, Dec. 2011, pp. 286-29.
6. H. Yang, X. Sun and G. Sun, "A High-Capacity Image Data Hiding Scheme Using Adaptive LSB Substitution", Journal of Radio Engineering, Vol. 18, No. 4, pp. 509-516, 2009.
Saher Manaseer, Asmaa Aljawawdeh, Dua Alsoudi, "A New Image Steganography Depending on Reference & LSB", International Journal of Applied Engineering Research ISSN 0973-4562 volume12,Number9(2017)pp.1950-1955. link:https://www.researchgate.net/publication/317057236_A_New_Image_Steganography_Depending_on_Reference_LSB.
8. Shailendra Gupta, Ankur Goyal, Bharat Bhusan, " Information Hiding Using Least Significant Bit Steganography and Cryptography", I. J. Modern Education and Computer Science, Vol. 6, Pages No. 27- 34, 2012.
9. Shilpa Gupta, Geeta Gujral, Neha Aggarwal, "Enhanced Least Significant Bit algorithm For Image Steganography ", IJCEM International Journal of Computational Engineering & Management, Vol. 15 Issue 4, July 2013 ISSN (Online): 2230-7893.

INNO SPACE

SJIF Scientific Journal Impact Factor

Impact Factor:
7.488

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details