IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

ARCHITECTURE OF NEW HIDING TECHNIQUE FOR PROJECTED & COMPRESSED TEXT IN DIGITAL IMAGE

Aditi Soni*, Sujit K. Badodia
* SVITS, Indore, India.
SVITS, Indore, India.

ABSTRACT

The art of information hiding has received lots of attention in the recent years as security of information has become a big concern in this internet epoch. As sharing of sensitive information through a common communication channel has become unavoidable, Steganography is the science and art of hiding information. Steganography means hiding a secret message (the embedded message) within a file (source cover) in such a way that an observer will not be able to detect the presence of contents of the hidden message. In this paper, proposed data hiding method that utilizes Projection of the letters, then compression of that letters with spread spectrum image Steganography technique. Experimental results show that the proposed method can bury a large amount of secret data while keeping very high security, as when the message is decrypted.

KEYWORDS: Steganography, Projection, Compression, Data hiding, Angle, Cover, Stego.

INTRODUCTION

Steganography or Stego is often referred to in the IT community, which means, "covered writing" and it is derived from the Greek language. It is defined by Markus Kahn as follows, "Steganography is the science and art of communicating in a way which hides the existence of the message. In Cryptography, the enemy is allowed and able to detect, intercept and modify messages without being able to offend certain security premises guaranteed by a cryptosystem, the main aim of Steganography is to conceal messages inside other messages in a way that does not permit any enemy to even detect that there is a something fishy in message".

In a digital world, Steganography and Cryptography are both intended to secure information from the parties to which we don’t want to share the information. Steganography can be used in a different types of data formats in the digital world of nowadays. The most well-liked data formats used are .bmp, .doc, .gif, .jpeg, .mp3, .txt and .wav. Used because of their fame on the Internet, ease of use of the steganographic tools that use these data formats and also due to the ease by which redundant or noisy data can be removed from them and replaced with a hidden message.

Steganography can be used to conceal important data inside another file so that the parties intended to get the message knows the presence of secret message. The general model of data hiding can be described in Fig 1. The embedded data is the message that one wants to send in secret.

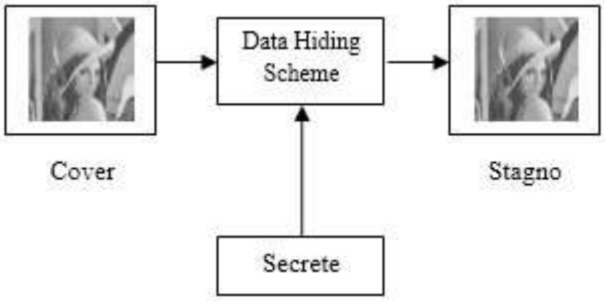

Fig 1. Data Hiding Scheme

New Technique is introduced here, which is the combination of two techniques. First is Permutation Straddling and second is Matrix Encoding. The straddling mechanism shuffles all coefficients using a permutation first. Then, embeds into the permuted sequence. And then Matrix Encoding is done.

PROBLEM DEFINITION

There are many steganography techniques which are capable of hiding data within an image. Different methods were used for Hiding data. All the methods are used to increase the security. The most widely used technique to hide data is the usage of the LSB. The existing techniques are generally based on LSB (Least Significant Bit) where LSBs of the cover file are directly changed with message bits.

Ki-Hyun Jung et. al proposed the semi-reversible data hiding method based on interpolation and LSB substitution. Initially, Interpolation methods are used to scale up and down the cover image before hiding secret data in it for a better capacity and quality. Secondly, the LSB substitution method is used to bury secret data. The most common Steganography techniques that used are least significant bit (LSB) substitution and pixel-value differencing (PVD). LSB substitution replaces the least significant bit with a secret bit stream. LSB matching is either added or subtracted randomly from the pixel value of the cover data when the embedding bit does not match. The interpolation is a method of constructing new data points within the range of a different set of known data points in the mathematical field of numerical analysis. In the interpolation method, the size of the image is changed so that the hackers easily guess that something is fishy in that image. And the LSB technique is the common technique so that Robustness against statistical attacks and Robustness against image manipulation may destroy the hidden message. It is required for Steganography algorithms to be robust against malicious changes to the image.

LITERATURE REVIEW

- In Reference [1], **Ki-Hyun Jung et. al [2014]** this proposed the semi-reversible data hiding method based on interpolation and then LSB substitution. The interpolation method has been preprocessed before hiding secret data for aiming the higher capacity and good quality. Then, the LSB substitution method was applied for burying secret data. The cover image with the scaled down size and secret data could be extracted from the stego-image and any extra information is also not used. The experimental results showed that the average PSNR was 43.94 dB and the capacity was 393,216 bits when k=3. In the case of k=4, we demonstrated that the PSNR and capacity were 37.54 dB and 589,824 bits, respectively.
- In Reference [2], **Mehdi Hussain et.al. [2013]** gave an overview of different Steganography techniques and its major types and classification of Steganography which have been proposed in the literature during last few years. We have critical analyzed different intended techniques which show that visual quality of the image is degraded when hidden data increased from desired limit using LSB based methods.
- In Reference [3], **Atallah M. et. al. [2012]** proposes a new Steganography technique which was presented, implemented and analyzed. The proposed method hides the secret message based on searching about the matching bits between the secret messages and image pixels values. The proposed method was compared with the LSB benchmarking method for hiding the secret message which hide the secret message directly in the least two significant bits of the image pixels.
- In Reference [4], **Mamta Juneja et. al. [2014]** proposed technique achieves the goal of an implementation of new steganography approach for images which integrates three new techniques a) Hybrid feature (line/edge/boundary/circle) detector technique integrating Canny and Enhanced Hough modify for bifurcating an image into edge and smooth areas b) Two Component based LSB Substitution Technique for hiding encrypted messages in edges of images c) Adaptive LSB substitution technique for hiding messages to smooth areas.
- In Reference [6], **Chan CK et. Al. [2004]** proposed a data hiding scheme by simple LSB substitution. By applying an optimal pixel tuning process to the stego-image obtained by the simple LSB substitution method, the image quality of the stego-image can be seriously improved with low extra computational complexity.
- In Reference [7], Ming-Ni WuMin-Hui Lin proposed the LSB substitution and genetic algorithm (GA) to build up two different optimal substitution strategies: one is the worldwide optimal substitution strategy and the otherone is the local optimal substitution strategy. The experimental results confirm that our methods can provide superior image quality than the simple LSB and Wang et al.'s method do while provide large hiding capacity.

METHODOLOGY

A data hiding method that utilizes Projection of the letters, then compression of text and then data hiding using permutation straddling and Matrix Encoing is proposed. The projection part is done by rotating the letters one by one by 85°. Contrasting stream media, image files only provide a partial steganographic capacity. In most of the cases, an embedded message does not require the full Space. That's why, a part of the file left as unused. Fig. 3 shows, that the changes focus on the starting portion of the file, and the unused part resides on the end. To prevent attacks, the embedding function should use the carrier medium as usual as possible. The embedding density should be the same everywhere.

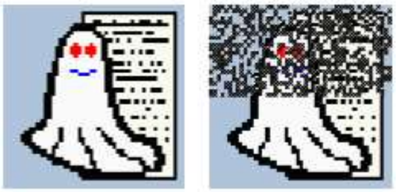

Fig. 3. Continuous embedding concentrates changes

First we use Permutative Straddling. In this, some well-known steganographic algorithms stretch out the message over the whole carrier medium. The straddling mechanism shuffles all coefficients using a permutation first. Then, embeds into the permuted sequence. The contraction does not change the number of coefficients (only their values). The permutation depends on a key derived from a password. It delivers the steganographically changed coefficients in its original sequence to the Huffman coder. With the correct key, the receiver is able to repeat the permutation. Fig. 4 shows the homogeneously distributed changes over the whole image.

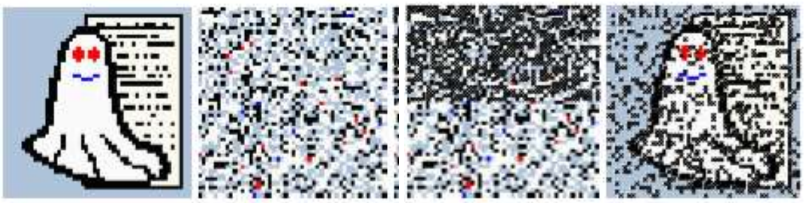

Fig. 4. Permutative embedding scatters the changes

And then Matrix Encoding is done. Furthermore, the original image is not needed to pull out the hidden message. The proposed receiver need only possess a key in order to reveal the secret message. The existence of the hidden information is virtually untraceable by human or computer analysis.

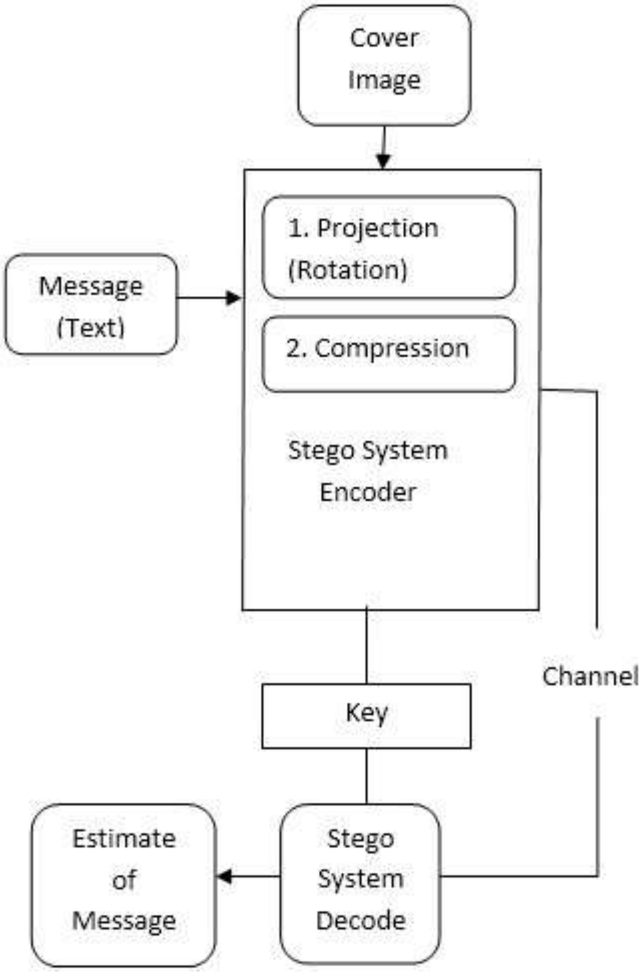

Fig 5 Block Diagram of Proposed System

Fig 5 shows that the sender initiate the message as text for appending on the cover image then it processed with the help of the projection which means that it will be rotated by 850 so that letters are tilted. It will helpful for our method and after this compression will be done. This data uploaded or merge with the cover image and that image not distorted in any manner. Send it to the receiver with the secure channel and at the end of the receiver key used for the decryption of the data and successfully receive the data.

CONCLUSION

In this paper, planned data hiding method that utilizes Projection of the letters, then compression of that letters and then Hiding the data with Permutation Straddling and Matrix Encoding. Also give an overview of different types of Steganography techniques, classification of Steganography which have been proposed in the journalism in last few years. Experimental results show that the proposed method can implant a huge amount of secret data while keeping very high security, as when the message is decrypted. Resistant to statistical attacks

REFERENCES

[1] Ki-Hyun Jung , Kee-Young Yoo “Steganographic method based on interpolation and LSB substitution of digital images” Springer Science+Business Media New York 2014 DOI 10.1007/s11042-013-1832-y.

[2] Mehdi Hussain and Mureed Hussain (2013) A survey of Image Steganography Techniques. International Journal of Advanced Science and Technology Vol. 54.

[3] Atallah M. Al-Shatnawi A New Method in Image Steganography with Improved Image Quality. Applied Mathematical Sciences, Vol. 6, 2012, no. 79, 3907 – 391

[4] Mamta. Juneja, and Parvinder S. Sandhu An Analysis of LSB Image SteganographyTechniques in Spatial Domain International Journal of Computer Science and Electronics Engineering (IJCSEE) Volume 1, Issue 2 (2013) ISSN 2320–401X (Print)

[5] Stefan Katzenbeiser & Fabien A.P.Petitcolas(1999), Information Hiding Techniques for Steganography and Digital Watermarking, Artech House, Computer Security series, Boston, London.

[6] Chan CK, Cheng LM (2004) Hiding data in images by simple LSB substitution. Pattern Recogn 37:469–474

[7] Ming-Ni WuMin-Hui Lin (2007), A LSB Substitution Oriented Image Hiding Strategy Using Genetic Algorithms

[8] Chang CC, Lin MH, Hu YC (2002) A fast and secure image hiding scheme based on LSB substitution. Int J Pattern Recog 16(4):399–416.

[9] Johnson, Neil F., "Steganography", 2000, URL: http://www.jjtc.com/stegdoc/index2.html

[10] Huang LC, Tseng LY, Hwang MS (2013) A reversible data hiding method by histogram shifting in high quality medical images. J Syst Software 86:716–727

[11] Johnson NF & Jajodia S (1998) Exploring steganography: seeing the unseen. Comput Pract 26–34

[12] Jung KH, Yoo KY (2009) Data hiding method using image interpolation. Comput Standards Interfaces 31: 465–470

[13] Jung KH & Yoo KY (2013) Data hiding using edge detector for scalable images. Multimedia Tools and Appl doi:10.1007/s11042-012-1293-84

[14] Lee CF, Huang YL (2012) An efficient image interpolation increasing payload in reversible data hiding. Expert Syst Appl 39:6712–6719