International Journal of Engineering Research and General Science Volume 3, Issue 5, September-October, 2015
ISSN 2091-2730

Architecture For Hiding Projected & Compressed Text In Digital Image Using Spread Spectrum Technique

Aditi Soni, Sujit K. Badodia

SVITS, Indore, India, aditisoni519@gmail.com, +917879633219

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.

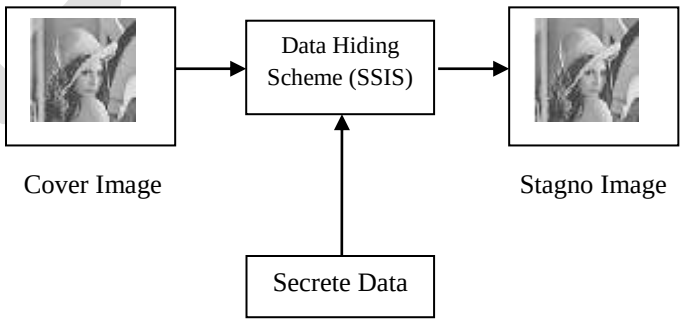

Fig 1. Data Hiding Scheme

CLASSIFICATION OF STEGANOGRAPHY METHODS

Steganography methods can be divided mainly into six categories.

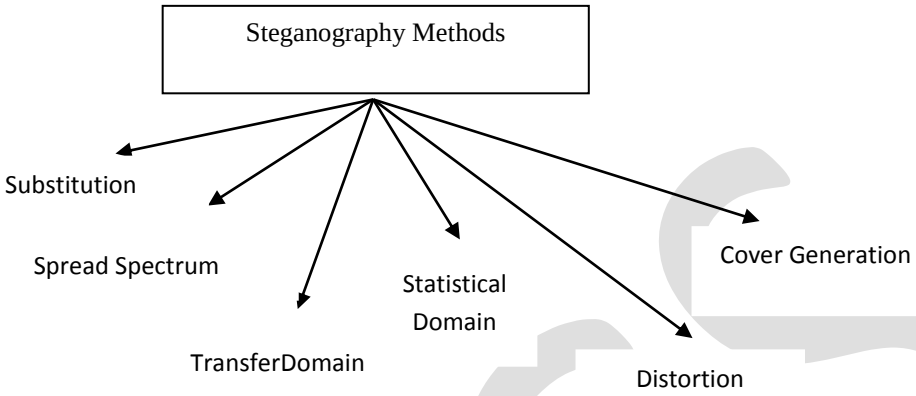

Fig 2 Classification of Steganography Methods

- Substitution methods substitute unneeded parts of a cover with a secret message (spatial domain).
- Transform domain techniques implant secret information in a transform space of the signal (frequency domain)
- Spread spectrum techniques takes the ideas from spread spectrum communication.
- Statistical methods encode information by varying several statistical properties of a Cover and utilize hypothesis testing in the withdrawal process.
- Distortion techniques stock up information by signal distortion and determine the deviation from the original cover in the decoding step.
- Cover generation methods encode information in the way a cover for secret communication is created.

The Spread Spectrum Image Steganography (SSIS) of the present discovery is a data hiding/secret communication steganographic system which uses digital imagery as a cover signal. The method on which we are doing survey i.e. Spread spectrum, it provides the ability to hide a significant abundance of information bits within digital images while avoiding detection by an observer. The message is recovered with lowest error probability due the use of error control coding. Spread spectrum image Steganography consignment is, at a minimum, an order of magnitude greater than of existing watermarking techniques. Furthermore, the original image is not necessary to extract the concealed message. The proposed receiver need only possess a key in order to reveal the secret message. The existence of the hidden information is virtually undetectable by human or computer analysis. At last, SSIS provides resiliency to transmission noise, like which found in a wireless environment and low levels of compression.

PROBLEM DEFINITION

There are many steganography techniques which are capable of hiding data within an image. These steganography techniques can be classified into two categories based on their algorithms: (1) spatial domain based techniques; (2) transform domain based techniques. 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. And many of them embedding techniques can be changed or shows indication of modification of image by careful analysis of the statistical properties of noise or perceptually analysis.
- ☑ 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. It achieves the target of 50% hiding capacity and Imperceptibility(PSNR value) with minimum MSE(mean square error)while hiding more data on edges than smooth areas as edges being high in contrast, color, density, frequency and other noise disturbances can tolerate more changes in their pixel values than 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. The worst case mean-square-error between the stego-image and the cover-image is derived.
- ☑ 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 spread spectrum technique is proposed. The projection part is done by rotating the letters one by one by 85°. Then compression part can be done so that large amount of data can be hiding. Then at last Spread Spectrum Image Steganography (SSIS) is used. Spread spectrum

image Steganography payload is, at a minimum, an order of magnitude greater than of existing watermarking techniques. Furthermore, the original image is not needed to extract the hidden message. The proposed receiver need only possess a key in order to disclose the secret message. The existence of the hidden information is virtually untraceable by human or computer analysis. at last, SSIS provides resiliency to transmission noise, like which found in a wireless environment and low levels of compression

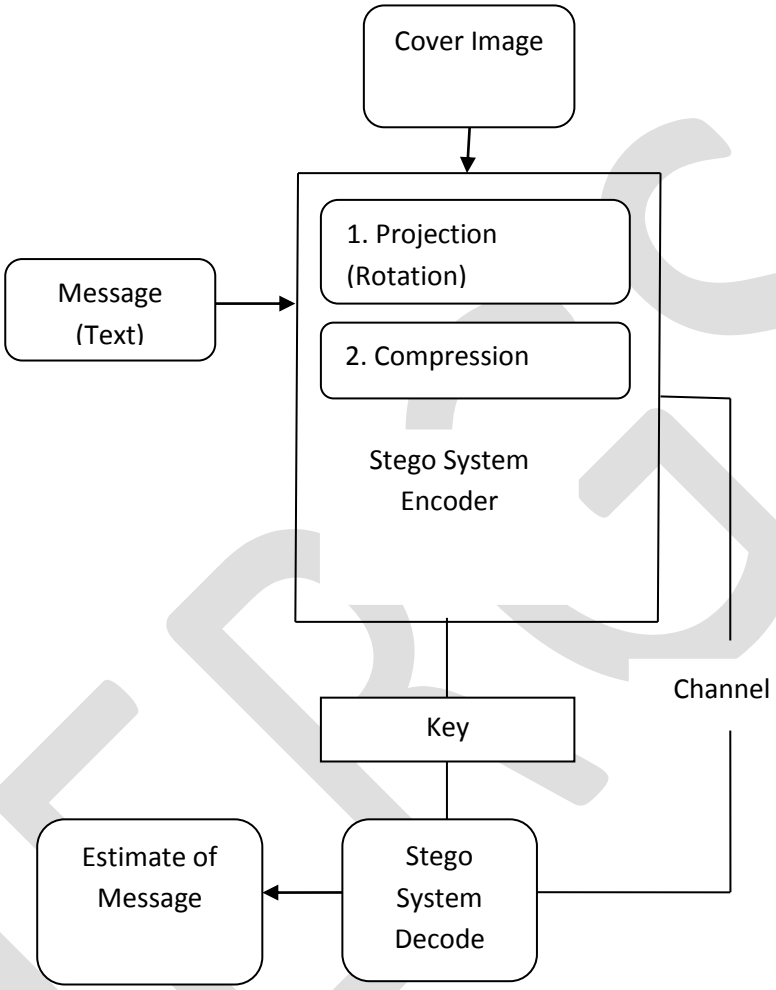

Fig 3 Block Diagram of Proposed System

Fig 3 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 85^0 so that letters are tilted and meaning of the letters are change. 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 spread spectrum image Steganography technique. 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.

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

[15] Lee YP, Lee JC, Chen WK, Chang KC, Su IJ, Chang CP (2012) High-payload image hiding with quality recovery using tri-way pixel-value differencing. Information Sciences 191:214–225

[16] Lehmann TM, Gonner C, Spitzer K (1999) Survey: interpolation methods in medical image processing. IEEE Trans Med Imaging 18(11):1049–1075

[17] Mielikainen J (2006) LSB matching revisited. IEEE Signal Processing Letters 13:285–287

[18] Ni Z, Shi YQ, Ansari N, Su W (2006) Reversible data hiding. Circ Syst for Video Technol IEE 16:354–362 Swanson M, Kobayashi M, Tewfik A (1998) Multimedia data embedding and watermarking technologies. Proc IEEE 86(6):1064–1087