Image Steganography using Dynamic LSB with Blowfish Algorithm

Aishwary Kulshreshta[#1] , Ankur Goyal[*2]
*M.Tech Scholar[#1], Assistant Professor[*2]*
YIT, Jaipur, India

***Abstract*—** The past few years have seen an increasing interest in using images as cover media for Steganography communication. The basic structure of Steganography is made up of three components: cover image, message, and the key. The carrier can be a digital image; it is the object that will carry the hidden message. A key is used to decode/decipher/discover the hidden message. This can be anything from a password, a pattern, a black-code etc. In this paper we propose a new form of Steganography, Which deals with disadvantages of Simple LSB substitution and as well as symmetric cryptography algorithm called Blowfish algorithm.

***Keywords*—** Steganography, Blowfish, Dynamic LSB, Canny Edge Detection

I. INTRODUCTION

The art of sending & displaying the hidden information especially in public needs more attention. There are many different methods have been proposed so far for hiding information in different cover media. In this paper a method for hiding of information on the text form in image as a cover media proposed. A Symmetric key cryptography along with dynamic LSB technique is used here for hiding the secret information. In the present era, communication through computer network requires more security.

Attacks may affect the quality of the data. There are n numbers of approaches available Cryptography is the art and science of achieving security by encoding message to make them non-readable. Means it is used to protect the user data .Cryptography involves two basic functions that are encryption and decryption. Encryption is the process of transforming plain data into the cipher text. Whereas decryption is just opposite process of encryption process in which we retrieve the original plain text from cipher text. Steganography is a technique to hide information from the observer to establish an invisible communication.
This Steganography system consists of a cover media into which the secret information is embedded. The embedding process produces a stego medium by replacing the information with data from hidden message. To hide hidden information, Steganography gives a large opportunity in such a way that someone can't know the presence of the hidden message and thus they can't access the original message.
Steganography is an area in which many studies and intensive research have been carried out. There are several different methods and algorithms of hiding data in different types of files.

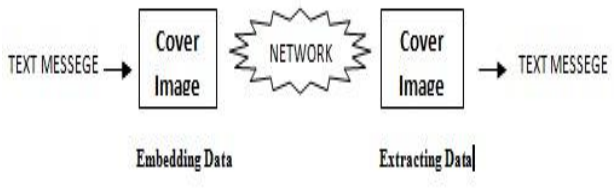


Figure: 1: Structure of Steganography System

The main goal of this method is to hide information on the cover image and send it to the receiver by extracting using the same methods.
There are contemporarily few effectual methods in applying Image Steganography: LSB Substitution, Blocking, and Palette Modification [2]. LSB (Least Significant Bit) Substitution is the process of modifying the least significant bit of the pixels of the cover image. Blocking works by breaking up an image into modules and using Discrete Cosine Transforms (DCT). Each module is broken into 64 bit DCT coefficients that approximate luminance and color of the values of which are modified for hiding messages. Palette Modification replaces the colors which are unused within an image's color palette with colors that represent the hidden message [2]. LSB Substitution allots itself to become a very powerful Image Steganography method with little limitations.

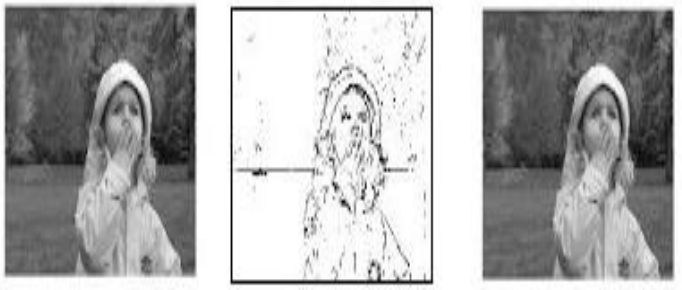
II. THE PROPOSED SCHEME

We specially emphasize on two most effective algorithm blowfish to encrypt the message and dynamic LSB for hiding message into cover image. Blowfish is a symmetric encryption algorithm, meaning that it uses the same secret key to both encrypt and decrypt messages. Blowfish is also a block cipher, meaning that it divides a message up into fixed length blocks during encryption and decryption. The block length for Blowfish is 64 bits; messages that aren't a multiple of eight bytes in size must be padded. The Blowfish algorithm has many advantages. It is suitable and efficient for hardware implementation and no license is required. Blowfish is a fast algorithm and can encrypt data on 32-bit microprocessors at a rate of one byte every 26 clock cycles. The algorithm is compact and can run in less than 5K of memory [3].

The advantages of LSB are its simplicity to embed the bits of the message directly into the LSB plane of

Cover-image and many techniques use these methods. Modulating the LSB does not result in a human-perceptible difference because the amplitude of the change is small. Therefore, to the human eye, the resulting stego-image will look identical to the cover-image. This allows high perceptual transparency of LSB. But the quality of the stego image produced by simple LSB substitution may not be acceptable. It means that the method degrades the image quality and probably attracts unauthorized attention. Once he/she notices the stego image, secret message can be easily extracted by simple LSB analysis.

The proposed scheme solves this Simple LSB problem using dynamic LSB. Dynamic LSB increase the complexity of hidden data as well as preserves the quality of stego image. In the very first step of Dynamic LSB method detects edges of the cover image using canny edge detection algorithm [4]. Cover image now separated into two parts as edges and remaining smooth part. We apply the LSB substitution to the only smooth parts of the image.



(a) (b) (c)

Figure: 2: (a) Cover Image (b) Edge Detection Image (c) Stego Image

In our implementation we first encrypt the message using blowfish algorithm and convert it into cipher text. On the basis of this cipher text we calculate length and divide it into appropriate number of modules. These individual cipher modules then hide into the individual cover image using dynamic LSB method. For dynamic LSB method each cover image is passed over canny edge detection for smooth and edge portions separation.

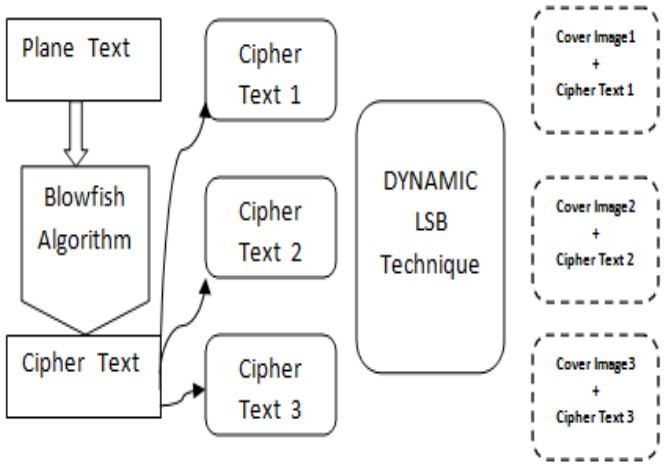


Figure3: Embedding Text into Cover Image

In the figure message embedding process is depicted step by step as plain text is first converted into cipher text using blowfish algorithm. This cipher text is divided into number of blocks according to the length of the original message. Individual cipher text block using dynamic LSB technique embedded into different cover images. Finally the stego image will send to the network and extracted on the receiver side using extraction process.

For the extraction of the message on the receiver side individual cipher text will extracted from stego image using Dynamic LSB extraction process.

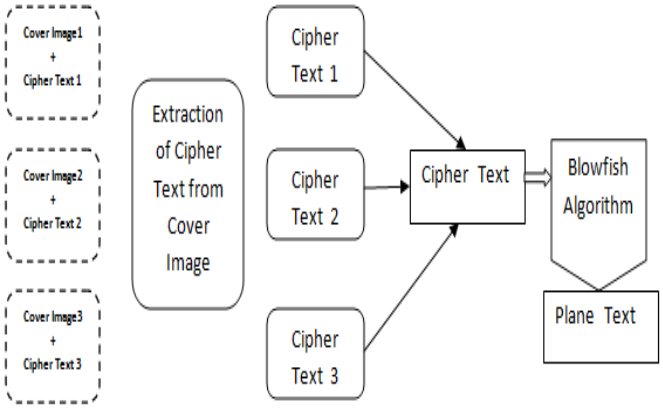


Figure: 4: Extraction of Text from Cover Image

These individuals extracted cipher text then reconstructed in a single cipher text and finally decrypted using Blowfish decryption at the receiver side.

III. Related Work

There are many methods exists for image Steganography such as Fibonacci data hiding technique, DCT Algorithm ,Data hiding using Prime numbers , etc. Dynamic Pattern based Image Steganography technique (DPIS) was discussed in a paper [5]. The idea behind our technique is that dominant cool or significant color in a pixel should not suffer from data embedding while the insignificant color channel can be used for data embedding.

P.Thiyagarajan, Aghila, Venkatesan proposed dynamic pattern based image Steganography technique has been introduced. This technique addresses key important issues like dynamicity in data embedding and indicator sequence and thus making it difficult to hack by steganalyst [5].

Shreelekshmi R, M Wilscy and M Wilscy proposed a transformation method for cover images for increasing the reliability of LSB replacement Steganography in spatial domain [6]. After the proposed transformation the images show very high embedding ratio irrespective of the amount of hidden data. The transformation increases the false alarm rate to 100% and decreases the accuracy of prediction. The length estimation is highly inaccurate especially with small amount of embedding. Thus the transformation proposed increases the reliability of LSB Steganography. The steganalysis results can be made more inaccurate in combination with dynamic compensation method proposed by Luo et. al. Both methods together can detect stego images as cover images and cover images as stego images. Stego images with low amount of hidden data can be detected as cover images or as stego images with very large amount of hidden data. These two methods in combination with random LSB Steganography can thus defeat the most accurate steganalysis methods in the literature thereby increasing the security of LSB replacement Steganography.

Mohammad Tanvir Parevez et.al [7] uses the concept lower color value of a channel has less effect on the color of a pixel than the higher value therefore more data bits can be embedded in the lower color channel. The Number of bits embedded in each channel depends on partition schema which is static throughout the embedding process. Among the R, G and B channel any channel is chosen as Indicator channel and it can be made random. Indicator channel sequence rotates in circular way through the embedding process.

The above listed techniques suffer from the following limitations: Data are embedded sequentially in all pixels, Data are embedded using static partition, schema or same number of bits in the channel, Fails to detect whether the stego image has been modified by the intruder.

IV. Experimental Result

Grayscale images are tested in different formats with same and different input messages using proposed scheme. The dataset we use to test our proposed technique includes 300 randomly picked images. Some of the images in the testing datasets were color images that we converted to gray scale using MATLAB. All the images tested over proposed system and get corrected result of 91%. With this testing process we conclude that the system accuracy is increased as compared with previous work. We have tested proposed system on different size length message and different image format.

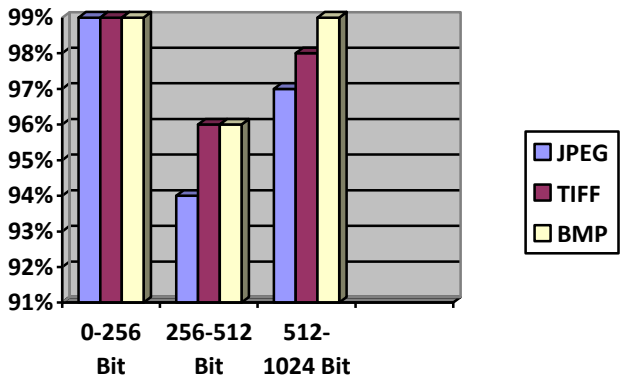


Figure: 5: Graph showing Result in different Format and Size

V. Conclusion

As Steganography becomes more widely used in computing, there are issues that need to be resolved. There are a wide variety of different techniques with their own advantages and disadvantages. Many currently used techniques are not robust enough to prevent detection and removal of embedded data. The use of benchmarking to evaluate techniques should become more common and a more standard definition of robustness is required to help overcome this.

Acknowledgment

First author is a RTU Research Fellow and the work presented here was done while M Tech Research at YIT College, Jaipur. The Co-Author is an Assistant Professor at YIT Jaipur and He is consistently guided me to work in this work. The author is grateful to Mr. Rakesh sharma and Mr. Vivek K Verma at RCEW Jaipur for conversations and suggestions.

References

[1] O. Kurtuldu and N. Arica, "A new steganography method using image layers," in *Computer and Information Sciences, 2008. ISCIS '08. 23rd International Symposium on*, 2008, pp. 1-4.

[2] Kesslet, Gary C. An Overview of Steganography for the Computer Forensics Examiner, Burlington, 2004

[3] Noohul Basheer Zain Ali, and James M Noras "OPTIMAL DATAPATH DESIGN FOR A CRYPTOGRAPHIC PROCESSOR: THE BLOWFISH ALGORITHM"

Malaysian Journal of Computer Science, Vol. 14 No. 1, June 2001.

[4] Canny J., "A Computational Approach to Edge Detection", *IEEE Transactions on pattern analysis and machine intelligence*, vol. 8, pp. 679-698, 1986.

[5] Dynamic Pattern Based Image Steganography, P.Thiyagarajan, G.Aghila, V.Prasanna Venkatesan, JOURNAL OF COMPUTING, VOLUME 2, ISSUE 8, AUGUST 2010, ISSN 2151-9617

[6] Steganography An Art of Hiding Data Shashikala Channalli et al International Journal on Computer Science and Engineering Vol.1(3), 2009, 137-141

[7] Mohammad Tanvir Parvez, Adnan Abdul-Aziz Gutub, "RGB Intensity Based Variable-Bits Image Steganography," apscc, pp.1322-1327, 2008 IEEE Asia-Pacific Services Computing Conference, 2008

[8] Provos N, Honeyman P, Hide And Seek: An Introduction To Steganography, IEEE Security & Privacy Magazine 1 (2008) pp. 32-44