An advanced approach for Image Steganography Method

Yogesh Kumar Sharma[1], Amit Mishra[2] Amit Sharma[3]

SBCET , Jaipur , India

Abstract — *Due to the unprecedented growth of network bandwidth, the Internet has become a quite popular channel for transmitting various data, such as, audio, video, image and text, in digital form. In this paper, we present a novel steganographic method that can be used to increase reliability of transmitted secret data in network. The core concept of proposed method is the use of cryptography with steganography technique. Lots of contents of the secret data are represented by cover image, which enhance invisibility and robustness. A mass of experiments demonstrate that our method has high hiding capacity, good imperceptibility, and certain robustness to some common attacks. These advantages assure the effectiveness of network transmission.*

Keywords — *Steganography, TwoFish, Adaptive LSB using Active Canny Edge Detection and open contours*

I. INTRODUCTION

The classic steganographic technique can be implemented using simple LSB insertion method. But in present era of communication where a secure communication over a channel is a great matter of concern. In case of simple LSB substitution, the presence of a hidden message in the cover medium can be identified very easily. So, lot of other approach have emerged for the taking care of the issue. Now each approach has certain merits and demerits After extensive analysis 'Active Canny edge detection with open active contour Models method'[2] turned out to be best approach in terms of implementation, security and performance.

In the proposed, Active Canny Edge Detection steganographic technique, weak edge are extracted out of the carrier-image[1]. The pixel value of weak

Edges is then replaced by the secret data. More secret bits are embedded in the weak edge area as the change in weak edges is hard to be discovered by human eyes. Moreover, the embedded secret data can be retrieved completely from the Stego-image in impeccable manner

With proposed technique the hidden message is inserted randomly in different bits of the cover medium, not necessarily in the least significant bits. Another problem is there when we use cryptographic methods to encrypt the data for providing more security. Different symmetric and asymmetric algorithms like DES, AES, Serpent, RC4, TwoFish[1], and RSA etc. are used for encrypting the data for providing higher level of security [4]. But each and every algorithm has some merits and demerits in terms of performance, time etc. TwoFish algorithm was proposed by Bruce Schneier in 1998 as an open source and unpatented algorithm which provides highly secured and performs better in terms of time[1]. As we have discussed earlier that in present context security is an important concern, so the combination of steganography and cryptography techniques are used to provide better security against different attacks. These combination techniques are used in present as well as it will be used in future for providing a secure communication over a channel.

The purpose of this research is to provide a full proof secure system for secured communication over the channel. We have combined various methods with each other to provide a higher level of security. We have used the combination of cryptography and steganography techniques. In cryptography, we have used TwoFish algorithm and in the steganography methods we have used 'Active Canny edge detection with open active contour Models method'[2] with an advancement of canny edge detection method. By this edge detection method the cover image can be separated in smooth parts and edge parts. We are only substituting the hidden message into the smooth part of the image so that attacker can't recognize the cover image.

II. RELATED WORK

Work done in the field of Steganography is either focused on Steganography techniques themselves or on their application to real life scenarios. Most of the research done earlier in this area proposes images, audios, and videos as cover media. Here the imperceptibility of hidden data is commonly achieved by exploiting the weaknesses of human auditory and visual systems, using the techniques for example, changing the least significant bits of the pixels of a cover image to embed information.

Lenti J et al. [6] discusses various steganography techniques for hiding data inside images. They cover least significant bit insertion and transform domain based steganography with special emphasis on the

comparison between RSA and elliptic curve based digital signatures. *Shirali et al.* [7] develop over the commonly used LSB (Least Significant Bit) replacement technique by randomizing the distribution of data by first dividing the image into small blocks and then selecting pixels from the block based on a password for LSB (Least Significant Bit) insertion. The method requires the image to be loaded in a block wise manner and requires extra memory space for keeping note of the selected pixels in a block. In [8] *Shirali et al.* uses the technique discussed in [7] is applied for hiding information in MMS (Multimedia Messaging Service). The carrier medium in [8] consists of text and image, steganography is applied in these components to accomplish the purpose.

A cover selection technique for hiding a secret image in a cover image was first introduced in [9]. This approach operates based on carrier texture similarity and substitutes some blocks of a carrier image with identical secret image blocks; then, block location indices of secret image are stored in the cover image. In this method, the blocks of the secret image are compared with the blocks of a set of cover images and the image with most similar blocks to those of the secret image is introduced as the best candidate to carry the secret image. An improvement on this method is proposed in [10] that uses statistical features of image blocks and their neighborhoods. Using block surrounding information prevents appearance of virtual edges in
surronding of the replaced blocks. In [8], the cover selection problem was studied by investigating three scenarios in which the embedder has either no knowledge, partial knowledge, or complete knowledge of steganalysis methods. In addition, some measures for cover selection were introduced in [8]. Cardinality of changeable DCT coefficients, JPEG quality factor, number of modifications in a cover image, and Mean Square Error (MSE) obtained from cover-stego image pairs are some of the proposed measures.

III. PROPOSED WORK

The main aim of the research is to make the data communication over channels secure and to protect the hidden data from the attackers. To achieve the aim of the research, we have included other objectives:

- Apply Two algorithm for encrypting the input message.
- Apply ‘Active Canny edge detection with open active contour Models method’ method to split the cover image into smooth and edge portions.
- Modify the simple LSB method into Active Canny edge detection LSB method using smooth and edge portion separation of the cover image.

These different combinations have been applied to provide different levels of security to achieve the secure communication and as well as the research objectives.

There are basically two major techniques implemented in this work. The first step is the encryption that is being used for converting the plain text (secret message) into the cipher text. The second step is the steganographic algorithm that is being used for embedding the text into the image. So we have two algorithms, namely, TwoFish Algorithm for encryption and adaptive LSB using ‘‘Active Canny edge detection with open active contour Models method’ [2] for image steganography.Cryptography and steganography has been used in conjunction to enhance embedding capacity of a steganographic channel by pre-processing the secret data and applying encryption technique over it to make it more robust against Steganalysis. As for encrypting the message a strongest and fastest technique TwoFish is used. In below fig1 displays message embedding process after encryption of the plain text (Text Message) into cipher text.

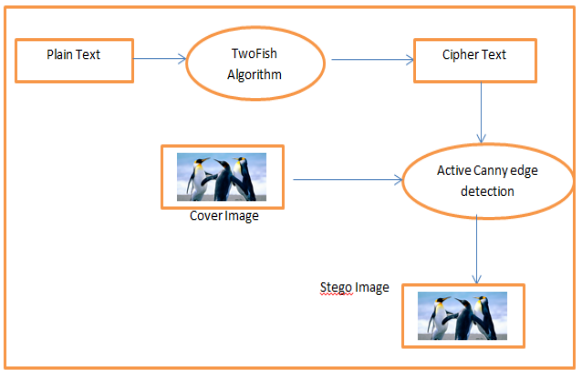

Fig. 1: Steganography message embedding process

below fig2, displays a message retrieval/ extraction process in which adaptive LSB is used for cipher text extraction and then the decryption of cipher text using TwoFish algorithm.

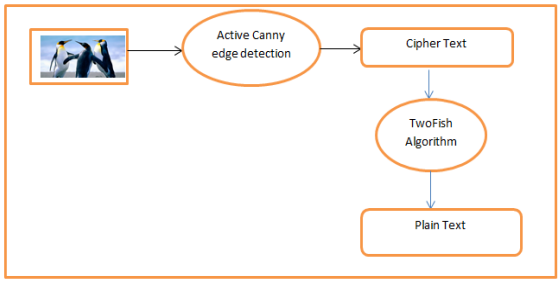

Fig. 2: Steganography message extracting process

In the first phase we convert plain text into cipher text by using TwoFish encryption. There are few strong reasons for selecting TwoFish for encryption as follows:

•Security: TwoFish has security Factor of more than 2.76[1]

Fast: TwoFish encrypts data in a 32-bit microprocessor at a rate of 12 clock cycles per byte.

• Simple: The simple structure of TwoFish is easy to implement and thus further eases the task of determining the strength of the algorithm.

• Variable Security: The key length is a variable and not a constant. The Maximum key length can be 256-bits. This fact allows a tradeoff between higher speed and higher security.

• TwoFish is not patented, thus it is widely used encryption algorithm.

• It is more secure than AES(**Rijndael**)[1].

• TwoFish is easy to implement. The working algorithm of TwoFish includes only 16 passages which involve very simple operations and some 32-bit XOR links.

Generally, steganography for non-compressed images typically happens in the spatial domain. Data is generally hidden in images by modifying the least significant bit (LSB) of a Image pixel value. This introduces a very small change in the color of the pixel that is not noticeable to the human eye. By ripping the LSB values in a bitmap we can embed a binary message that can be retrieved at a later point. In the compressed JPEG image, pixel values can't be altered in the spatial domain because the JPEG compression algorithm is lossy in nature. This means that should we try embedding data on the LSB of pixel values we may not get the same pixel value after decompression. Due to this problem steganography needs to take place in a different manner than in non-compressed bitmap images. By using advanced approach in our project to separate the edge part of the image we are extracting the smooth portions only to embed the message bits. For this we use 'Active Canny edge detection with open active contour Models method' to remove the edge part from cover image.

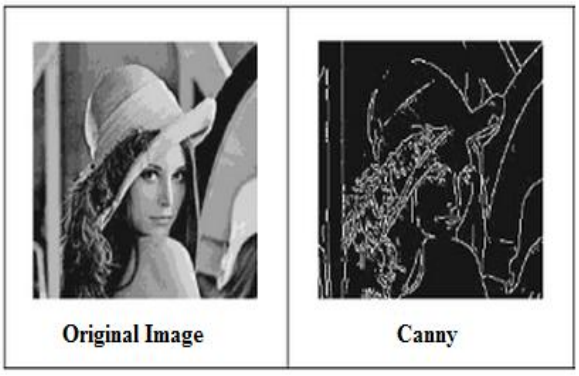

Fig. 3: Active Canny Edge detection

After separating the smooth portion of the cover image we need to convert each character of the plain text into its corresponding ASCII equivalent. ASCII value is being converted into its binary equivalent. As for instance, the conversion of "HELLO" is done as below.

Table 1 ASCII value and corresponding binary value

H	E	L	L	O
72	69	76	76	79
01001000	01000101	01001100	01001100	01001111

So each character of the text file are converted into its binary equivalent using the aforementioned technique. Also Masking can be done before replacing it in the pixels of the image. The *Masking Technique* is shown in the below example. In this technique the each byte of the text file's binary equivalent is binary ANDed with the binary equivalent of 254. Then the bits are hidden with the image pixels. This masking process will provide additional security.

For "H" binary value: 01001000

Mask (255) : 11111111

01001000

The system also ensures that the length of the secret message is below the maximum embedding potential of the first image.

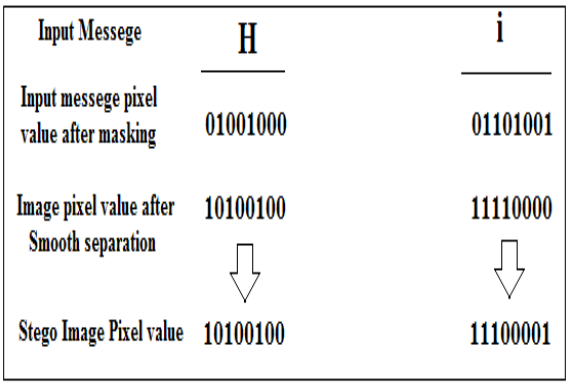

Fig. 4: Adaptive LSB Technique – Illustration

The Adaptive LSB using active canny edge technique can also be briefly explained with the help of bits. In above Figure 4 the LSB technique is explained with the help of binary values. As shown in the figure the last bits of the pixels are replaced with the bits of the cipher text. So the eventual image will be look exactly as the original image.

the Adaptive LSB using active canny does not cause distortion in a human perceptible difference because the amplitude of the change is small. Therefore, for human eye, the final stego-image will look exactly to the cover-image. This allows high perceptual transparency of Adaptive LSB.

IV. CONCLUSIONS

In this paper, an Adaptive LSB using active canny pattern based image steganography technique has been introduced. This technique resolves key issues like adaptiveness in data embedding. TwoFish algorithm for cryptography. both of these in combination give appropriate results. Proposed technique give very high embedding capacity with low noise and distortions and all this have been proved by experimental results.

REFERENCES

[1] The Twofish Team's Final Comments on AES SelectionBruce Schneier. John Kelseyy Doug WhitingzDavid Wagnerx Chris Hall{ Niels FergusonkTadayoshi Kohno.. Mike StayyyMay 15, 2000

[2] Active Canny: Edge Detection and Recovery with Open Active Contour Models Muhammet Bastan, S. Saqib Bukhari, Thomas M. Breuel *IET Image Processing*

[3] EFFICIENT IMAGE CONTOUR DETECTION USING EDGE PRIORJiangping Wang1, Changhu Wang2, and Thomas Huang1
1Beckman Institute, University of Illinois at Urbana-Champaign, USA 2Microsoft Research Asia, Beijing, China{jwang63,huang}@ifp.uiuc.edu, chw@microsoft.com

[4] Ghazanfari, K.; Ghaemmaghami, S.; KhosraviS.R."LSB^{++}: An improvement to LSB^{+} steganography TENCON 2011 - IEEE Region 10 Conference Pp. 364 – 368, 2011.

[5] P. Kruus, C "A survey of steganography image files." Advanced Security Research Journal.[On line], 5(1), pp. 41-52. 2011.

[6] Lenti J.: Steganographic Methods. Periodica Polytechnica Ser. El. Eng. 44(3-4), 249-258 2000.

[7] Shirali Shahreza, M.: An Improved Method for Steganography on Mobile Phone. In: Sandberg, I.W. (ed.) Proceedings of the 9th WSEAS International Conference on Systems. ICS 2005, World Scientific and Engineering Academy and Society (WSEAS 2005.

[8] Shirali Shahreza, M.: Steganography in MMS. In: Proceedings of the 1 1th IEEE International Multitopic Conference, Lahore. Pakistan. December 28-30, 2007.

[9] Dhanashri, D., Patil Babaso, S., Patil Shubhangi, H.: Mms Steganography For Smartphone Devices. In: Proceeding of 2nd International Conference on Computer Engineering and Technology, Jodhpur, India, November 13-14, vol. 4, pp. V4-513—V4-516, 2010.

[10] Kermani, Z.Z., Jamzad, M.: A Robust Steganography Algorithm Based on Texture Similarity Using Gabor Filter. In: IEEE Symposium on Signal processing and Information Technology, pp. 578-582, 2005.

[11] Sajedi, M.: Cover Selection Steganography Method Based on Similarity of Image Blocks. In: IEEE CIT, Sydney, Australia 2008.

[12] Kharrazi, M., Sencar, H., Memon, N.: Cover Selection for Steganographic Embedding. In: ICIP. pp. 117-121, 2006.