Securing Cipher Information using Edge Based Adaptive Pixel Pair Matching

Shanmugam .E† and T.K.Thivakaran††,

Department of Computer Science & Engineering,
Sri Venateshwara College of Enginnering,
Sriperumbadur, TamilNadu,India.

Summary
Securing the information from other persons is always difficult one when you are connected in an open network. In order to send some confidential information you must protect it from the attackers. Cryptography and Steganography plays vital role in securing information from others. Cryptography is the art of secret writing and Steganography is the art of hiding information. When combining these two mechanisms the advantages on security will increase. Hence the proposed method will encrypt the data with crypto module using Blowfish algorithm and then embed the encrypted data into the cover image with stego module using Edge based Adaptive Pixel Pair Matching (EAPPM) method. With the proposed method in this paper a double layered security for the confidentiality of the information hidden in the stego file is ensured. i.e., even though the attackers able to retrieve the hidden information from the stego file they will get only the encrypted message, which needs more time to crack the encryption scheme. The experimental results show the proposed method is hiding the information in fair manner compared against normal Adaptive Pixel Pair Matching (APPM) method.

Key words:
Adaptive Pixel Pair Matching (APPM), Blowfish, Edge based Adaptive Pixel Pair Matching (EAPPM).

1. Introduction

Data communication over the internet can be made secure and private by using two security mechanisms namely, cryptography and steganography. Typically cryptography based communication have four steps: encrypting, sending, receiving and decrypting. Sender encrypts the data and the sends it to the receiver. Whereas the receiver receives the encrypted data which has to be decrypted in order to read the original message. Since a cryptographic algorithm can be easily cracked by the attackers using average computation power, a parallel research field named Steganography had been developed which tries to hide data in a cover medium. This paper presents the idea of combining both cryptography and steganography mechanisms, which will increase the overall security of a communication through a open channel.

In such a combined system, it becomes even harder to get the secret data due to the complexity in the process of extracting the encrypted data from stego file and then deciphering it. But developing such a system increases the time complexity of the algorithm. In order to reduce the time complexity, the combined system uses a symmetric key encryption (Blowfish) algorithm [14] [11] in cryptography module. Since symmetric key encryption algorithm [14] [11] [13] takes small amount of computation time and taking only a small amount of the system assets to perform encryption and decryption against asymmetric key encryption. To increase the security in steganography, the stego module perform edge detection on the cover image file then performs the Adaptive Pixel Pair Matching (APPM) method to hide the encrypted data into the cover file.

This paper is organized as follows: Section II will give an overview of the works related to this proposed system. The proposed system is divided into two modules: Crypto module and Stego module. These modules are briefly discussed in Section III. Section IV will give the experimental results and analysis of Edge based Adaptive Pixel Pair Matching along with normal Adaptive Pixel Pair Matching method. Section V will walk through the conclusion of the paper.

2. Related Works

The security of Steganography method depends on the following aspects: detection of the data present in the stego file, and removal of those data from the stgo file. Once a method gives difficulty to those aspects then the method is consider to be secure one, but it is not easy to satisfy. Least-significant bit (LSB) is the most widely used Steganography method as it is easy to implement but the detection of data and extraction of the data from the stego file can be easily done. Hence the problem with LSB method is that the data can be easily detected and extracted from the stego file using simple steganalysis method.

A Pixel Pair Matching (PPM) [6] approach for steganography had been proposed, which is improvement of LSB matching; this method uses two pixels as an embedding unit while LSB uses single pixel value. Chao

Manuscript received June 5, 2014
Manuscript revised June 20, 2014

et.al [12] proposed a diamond encoding (DE) method which enhance the payload of exploiting modification direction (EMD) [18] method. Hong and Chen [17] proposed Adaptive Pixel Pair Matching (APPM) method based on the concept of PPM. Suppose a data to be hiding in a pixel value, first calculate the modular distance for that pixel then find neighbourhood pixel according to the calculated modular distance. Once the neighbourhood pixel is calculated, it will be replaced by the original pixel value.

3. Proposed Work

Steganography methods are used to hide the existence of secret data in a cover file. The confidentiality of the hidden information is an important aspect that is to be considered. To ensure confidentiality of a secret data, in this paper a new approach of embedding encrypted data into an image cover file has been proposed. As Blowfish [14] [11] is the best performing algorithm compared with all other most widely used symmetric key algorithms.The proposed method first encrypts the data using Blowfish encryption algorithm. It also has an advantage that Blowfish is very harder crack because it uses the key length values varying from 32 bits to 448 bits. The next step is to embed the encrypted data into an image cover file using EAPPM method. Figure 1 gives overview of the proposed system.

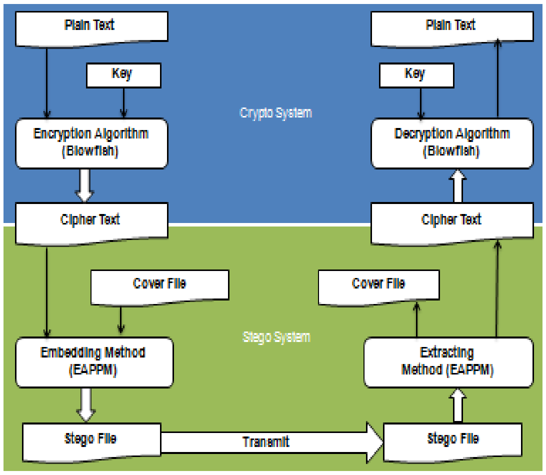


Figure 1. Proposed system block diagram

3.1 Blowfish Encryption Algorithm

Blowfish [13] [15] is a 64-bit block cipher with

a variable-length key. Key expansion and data encryption are the two parts of Blowfish algorithm. The key expansion step converts 448 bit key into 4168 bytes. It uses a Single P-array that has size of 18 and four S-boxes that have size of 256.

The overall process of data encryption consists of six steps as shown in Figure 2. Data encryption has a simple function which is iterated 16 times. In each round a 32 bit subkey is XOR-ed with leftmost 32 bits of plaintext and the result is then passed to the F function of Blowfish.

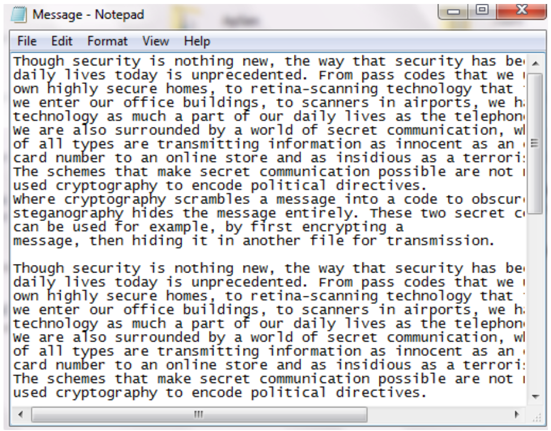
```
1. Divide X into two 32-bit halves: XL, XR
2. For i = 1 to 16
       XL = XL ⊕ Pi
       XR=F(XL) ⊕ XR
       Swap XL and XR
3. Swap XL and XR (Undo the last swap )
4. XR=XR ⊕ P17
5. XL = XL ⊕ P18
6. Concatenate XL and XR
```

Figure 2. Description of Blowfish

This result becomes rightmost 32 bits for the next round and the output of F function is XOR-ed with the original rightmost 32 (XR) bits of plaintext becomes leftmost 32 (XL) bits for the next round function and proceeds. The Function F follows:

F(XL) = {{S1[a] + S2[b] mod 232} • S3[c]} + S4[d] mod 232

Where, S1, S2, S3 and S4 are S-boxes 1, 2, 3 and 4 respectively.



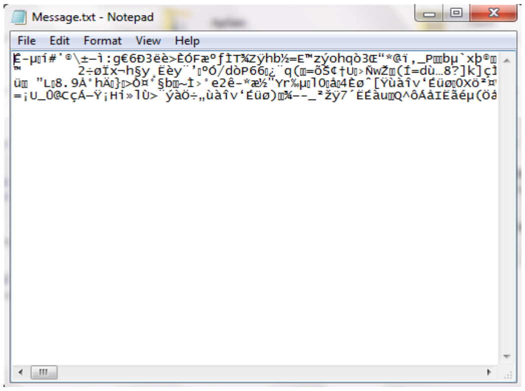
```
Though security is nothing new, the way that security has be
daily lives today is unprecedented. From pass codes that we
own highly secure homes, to retina-scanning technology that
we enter our office buildings, to scanners in airports, we h
technology as much a part of our daily lives as the telephon
We are also surrounded by a world of secret communication, w
of all types are transmitting information as innocent as an
card number to an online store and as insidious as a terrori
The schemes that make secret communication possible are not
used cryptography to encode political directives.
Where cryptography scrambles a message into a code to obscur
steganography hides the message entirely. These two secret c
can be used for example, by first encrypting a
message, then hiding it in another file for transmission.

Though security is nothing new, the way that security has be
daily lives today is unprecedented. From pass codes that we
own highly secure homes, to retina-scanning technology that
we enter our office buildings, to scanners in airports, we h
technology as much a part of our daily lives as the telephon
We are also surrounded by a world of secret communication, w
of all types are transmitting information as innocent as an
card number to an online store and as insidious as a terrori
The schemes that make secret communication possible are not
used cryptography to encode political directives.
```

Figure 3a. Snippet of Text file

Figures 3a and 3b are snippet of text file before and after encrypting the data by Blowfish encryption algorithm.

3.2 Edge based Adaptive Pixel Pair Matching (EAPPM)

Normal human visual system notifies the alteration in soft areas of an image rather than sharp areas in that. In order to find sharp areas of an image an edge detection mechanism is used. There are many edge detection methods like Canny, Fuzzy, Sobel and Laplacian filters [1] which are commonly used and these sharp edges are used to hide the data using steganography method which gives good results than the normal steganography method. For this reason the proposed method embed the data in sharp areas.



```
Ê-µ▯í#'®\±–ì:g€6Ð3ëè>ÈÓFæºƒÌT%Zÿhb½=E™zýohqò3Œ"*@ï,_P▯▯bµ`xþ®▯
™        2÷øÏx¬h§y¸Ëèy¨'▯ºÓ/dòP66▯¿¨q(▯=õŠ¢†U▯›ÑwŽ▯(Í=dù…8?]k]çÌ
ü▯ "L▯8.9Å°hÄ▯}▯>Ò¤˚§b▯~Ì›˚e2ê–*æ½"Yr‰µ▯l0▯å▯4Èø^[Ÿùàîv'ÉüøØXö²¤
=¡U_Û@CçÁ–Ÿ¡Hi»lÙ>¨ýàÖ÷„ùàîv'Éüø)▯¾––_²žÿ7´ËÉàu▯Q^ôÁåIËãéµ(Öå
```

Figure 3b. Snippet of Crypt file

Figure 4.1a

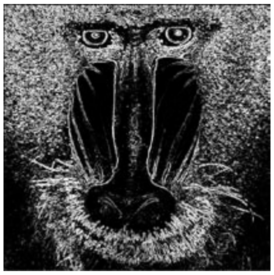


Figure 4.1b

Figure 4.2a

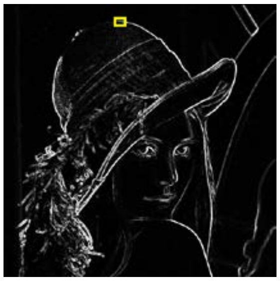


Figure 4.2b

Sobel edge detection method is chosen for detecting the sharp areas in the proposed method. Figure 4.1a and 4.2a is the couple of sample images taken as input to the Sobel operator and the outcome of edge based images are 4.1b and 4.2b. From the outcome of images the sharp areas of the original image are recorded.

Select a pixel from the recorded sharp areas to embed data in that. Suppose a pixel (x, y) is selected to embed the data digit (ma) then calculate the modular distance by md by using formula 2 and 3. The next step is to find the neighbourhood pixel (x+x(md), y+y(md)) of (x, y) based on figure 5. Once the neighbourhood pixel is calculated, it is replaced by the original pixel (x,y).

$$md = ma\text{-}f(x,y) \bmod 16 \qquad (2)$$

$$f(x,y) = (x+6*y) \bmod 16 \qquad (3)$$

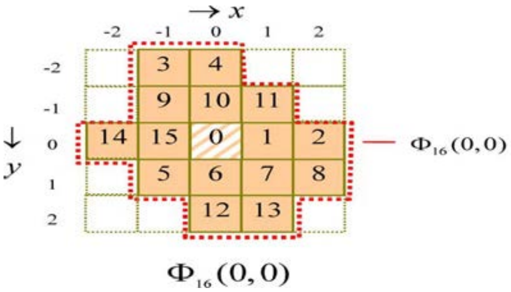


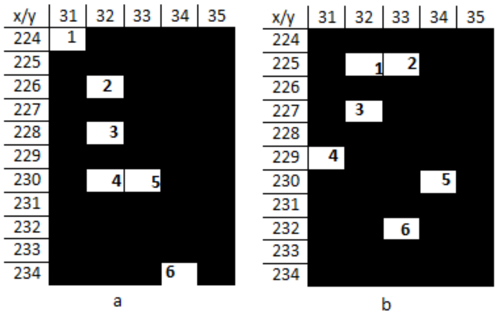
Figure 5. Finding Neighbourhood Pixel

In order to extract the data from a stego file, initially the stego file is given to the Sobel operator to find the sharp areas in the image and those pixel values are recorded. Suppose a pixel (x',y') is selected to extract the data from it, calculate f(x',y') by using the formula 3. The result will give the embedded data digit in it.

4. Experimental setup and Results

The proposed technique has been applied on a set of 10 sample text files with various sizes (ranges from 250 bytes to 4000 bytes) over a set of 50 sample cover images. A data file as in figure 3a is taken for the experimental process, the crypt file figure 3b of the taken data file is generated by using the Blowfish encryption algorithm. In order to embed the encrypted data file in the cover images 4.1a and 4.2a, the data is converted into Hexastring format.

The pixel ranges starting from {(30,210),(31,209),..} are the outcome of sobel operator of image lena (Figure 4.2a the pixel ranges are highlighted in a binary image of lena is shown in Figure 4.2b. Now the Hexastring values are converted into bit values then use the EAPPM method to embed the data.



x/y	31	32	33	34	35
224	1				
225					
226		2			
227					
228		3			
229					
230		4	5		
231					
232					
233					
234				6	

a

x/y	31	32	33	34	35
224					
225		1	2		
226					
227		3			
228					
229	4				
230				5	
231					
232			6		
233					
234					

b

Figure 7a. sample window before embedding.
Figure 7b. sample window after embedding.

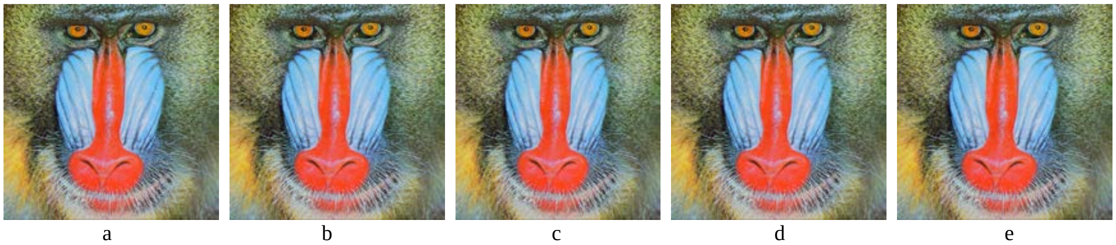


Figure 6.1 a. Original image, b.APPM Stego image for text , c. APPM Stego image for crypt text, d. Edge based APPM Stego image for text, e. Edge based APPM Stego image for crypt text.

Figure 6.2 a. Original image, b.APPM Stego image for text , c. APPM Stego image for crypt text, d. Edge based APPM Stego image for text, e. Edge based APPM Stego image for crypt text.

Table 1 Pixel values of Sample window before and after embedding

Pixel Number	**Hexa decimal values of Data Bit**	**Original Pixel Values**	**RGB Values of Original Pixels**	**Neighbourhood Pixel Values**	**RGB Values of Neighbourhood Pixels**	
					Before Embedding	**After Embedding**
1	6	31,224	101,52,45	32,225	85,39,41	101,52,45
2	7	32,226	78,37,43	33,225	81,37,38	78,37,43
3	2	32,228	96,38,37	32,227	82,35,41	96,38,37
4	D	32,230	83,35,33	31,229	90,39,35	83,35,33
5	6	33,230	77,36,34	34,230	74,39,37	77,36,34
6	1	34,234	71,40,37	33,232	65,29,29	71,40,37

A 5x11 window which is marked with yellow color rectangle in the binary edge image show in figure 4.2b is taken as example. This zoomed view of the window is shown in figure 7a. The text file shown in figure 3a has to be embedded in the cover image shown in figure 4.2a. Consider the edge pixel value (31,224) from the figure 7a, if 6 is the data bit to be hidden in the selected pixel (31,224) the corresponding neighborhood pixel is calculated by using the equations 2 and 3 as follow:

$$\begin{aligned} Md &= 6 - f(31,224) \bmod 16 \\ &= 6 - [(31+6*224) \bmod 16] \bmod 16 \\ &= 6 - [0 \bmod 16] \bmod 16 \\ md &= 6 \end{aligned}$$

So the corresponding neighborhood pixel is (32,225) calculated by using the figure 5. Similarly the neighborhood pixels are calculated for all other edge pixels. The original pixels are replaced by the neighborhood pixels. After embedding all the content of the data file the sample window is as shown in figure 7b. The original values of edge pixels present in the sample window and the calculated neighborhood pixel values before and after embedding is tabulated in table 1.

For the purpose of analysis of the proposed system the process is also subjected to APPM method over a text file and crypt file. The obtained stego images from both APPM and EAPPM embedding process are subjected to image quality analysis. The image quality measures used for analysis are Structural content (SC), Normalized cross correlation (NCC), Peak Signal to Noise Ratio (PSNR), mean Square Error (MSE).

Structural content is a measure of structural quality of an image if it value is placed at one, it means that image is of better quality. If value is too large then it is a poor quality image. Normalized cross correlation is a measure of how much similar the given images are. If it value tends to one then it said that both are very much similar. Highest PSNR value and lowest MSE value represents a better quality image. Figure 6.1 and 6.2 show a sample of two images which have been used for analysis.

Table 2. Comparison of image quality parameters for normal text

Method/ Parameter	APPM		EAPPM	
	Image1	Image2	Image1	Image2
Structural Content	1.0000	1.0001	1.0000	1.0001
Normalized Cross Correlation	1.0000	1.0000	1.0000	1.0000
Peak Signal to Noise Ratio	57.7449	57.8443	60.3148	60.3025
Mean Square Error	0.1190	0.1274	0.0605	0.0606

Table 3. Comparison of image quality parameters for Crypt text

Method/ Parameter	APPM		EAPPM	
	Image1	Image2	Image1	Image2
Structural Content	1.0001	1.0002	1.0001	1.0002
Normalized Cross Correlation	0.9994	0.9993	0.9999	0.9999
Peak Signal to Noise Ratio	55.6083	55.9320	58.6556	58.6759
Mean Square Error	0.1496	0.1518	0.0883	0.0882

Experimental results for two sample images are recorded and show in table 2, 3 and 4. Table 2 is a comparison of image quality parameters of stego images which are obtained after embedding the text file and table 3 gives a comparison of those parameters of stego images obtained after embedding a crypto file. From the table 2 it is seen that the value of SC is nearly one and NCC value is also one and hence we can say that the images are similar to the original after embedding the text. The stego image obtained after edge based APPM method have highest PSNR value and lowest MSE value which shows that EAPPM have better performance in terms of image quality. Similarly from table 3 it can be said that edge based APPM method is best.

Table 4 shows a comparison of image quality measures of stego files obtained using EAPPM over a text file and crypt file. From table 4 it is seen that SC value and NCC value of a text file are nearly one which seems to be better than a crypt file. Similarly the value of PSNR is high and MSE is low for a text file. This results show that EAPPM is better over a text file than a crypt file.

Table 4 Comparison of image quality parameters for EAPPM

File/ Parameter	Text File		Crypt File	
	Image1	Image2	Image1	Image2
Structural Content	1.0000	1.0001	1.0001	1.0002
Normalized Cross Correlation	1.0000	1.0000	0.9999	0.9999
Peak Signal to Noise Ratio	60.3148	60.3025	58.6556	58.6759
Mean Square Error	0.0605	0.0606	0.0883	0.0882

5. Conclusion

The experimental results show that edge based APPM is better than normal APPM method. EAPPM gives better performance for a text file over the crypt file in terms of image quality. Compared to image quality, the confidentiality of the secret data is the most important aspect in an open channel communication. In terms of security EAPPM over a crypt file is highly secure than EAPPM over a normal text file. Hence it is concluded that EAPPM over a crypt file can be considered as the best steganography method which ensures high confidentiality to the embedded secret data.

References

[1] Anastasia Ioannidou, Spyros T. Halkidis, George Stephanides “A novel technique for image steganography based on a high payload method and edge detection”, Expert Systems with Applications 39 (2012) 11517–11524.

[2] Cheng-HsingYang “Inverted pattern approach to improve image quality of information hiding by LSB substitution”, Journal of Pattern Recognition 41 (2008) 2674 – 2683.

[3] Chi-Kwong Chan, L.M. Cheng “Hiding data in images by simple LSB substitution” Journal of Pattern Recognition 37 (2004) 469 – 474.

[4] Eric Cole.”Hiding in Plain Sight: Steganography and the Art of Covert Communication”.

[5] Ingemar J. Cox, Matthew L. Miller, Jeffrey A. Bloom, Jessica Fridrich, and Ton Kalker.”Digital Watermarking and Steganography”, Second Edition 2008.

[6] Jarno Mielikainen “LSB Matching Revisited” IEEE SIGNAL PROCESSING LETTERS, VOL. 13, NO. 5, MAY 2006.

[7] Jianjun Wang ,YitingSun et.al. “An improved section-wise exploiting modification direction method”, Journal of Signal Processing 90 (2010) 2954–2964.

[8] National Bureau of Standards – 3-Data Encryption Standard, FIPS Publication 46, 1977.

[9] National Bureau of Standards – Data Encryption Standard, FIPS Publication 46, 1977.

[10] NIST, "Advanced Encryption Standard Call", NIST, 1997. http://www.nist.gov/aes/

[11] Verma O P, Ritu Agarwal, Dhiraj Dafouti, Shobha Tyagi “Peformance Analysis of Data Encryption Algorithms” Electronics Computer Technology (ICECT), 2011 3rd International Conference.

[12] Ruey-Ming Chao, Hsien-ChuWu, Chih-Chiang Lee, and Yen-Ping Chu “A Novel Image Data Hiding Scheme with Diamond Encoding” ” EURASIP Journal on Information Security Volume 2009.

[13] Schneier B. “Description of a New Variable-length Key 64-Bit Block Cipher (Blowfish).” Fast Software Encryption, Cambridge Security Workshop Proceedings (December 1993), Springer-Verlag, 1994, pp. 191-204. http://www.schneier.com/paper-blowfish-fse.html

[14] Shanmugam.E and Dr.T.K.Thivakaran, “Performance Comparison of AES and Blowfish for Dual Layer Security in an Open Channel”. 3rd Indian Conference on Computational Intelligence (ICCI), April 2013.

[15] Stallings, Cryptography & Network Security - Principles & Practice, Prentice Hall, 3rd Edition 2002.

[16] Stefan Katzenbeisser and Fabien A “Information Hiding Techniques for Steganography and Digital Watermarking”.

[17] Wien Hong and Tung-Shou Chen “A Novel Data Embedding Method Using Adaptive Pixel Pair Matching”, IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 7, NO. 1, FEBRUARY 2012.