ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 1, Issue 8, November 2013

Novel Steganographic method for Encrypted Image as a cover media for Binary image, Text and Audio

Mr. Arjun R. Nichal[1], Mr. Vinod B. Kumbhar[2]

Assistant Professor, Electronics & Telecommunication Department, AITRC, Vita, India[1]

Assistant Professor, Electronics & Telecommunication Department, AITRC, Vita, India[2]

Abstract: Data hiding is an important branch of information security. Imperceptibility and Hiding Capacity are very important aspects for efficient secret communication. In this paper we propose a Steganographic method for encrypted image. In this method our aim is to embed the data like binary image, Text and Audio file in encrypted cover media. This method first encrypts the Cover media with encryption method and after Encryption secrete data can be embedded into the Encrypted cover object by modifying a small proportion of Encrypted data. PSNR (Peak Signal to Noise Ratio), EC (Embedding Capacity) and NBE (Number of Bits Embedded) these three are the quality parameters.

Keywords: Steganography, Encryption, Data hiding, Secrete Communication.

I. INTRODUCTION

Information hiding in digital images has drawn much attention in recent years. Secret message encrypted and embedded in digital cover media. The redundancy of digital media as well as characteristics of human visual system makes it possible to hide secret messages. Two competing aspects are considered while designing information hiding scheme 1) Hiding capacity and 2) Imperceptibility. Hiding capacity means maximum payload. Imperceptibility means keeping undetectable [1].

A least significant bits (LSB) substitution method is widely used for hiding data in digital images. This method widely used because of large capacity and easy implementation. Cryptography was created as a technique for securing the secrecy of communication and many different methods have been developed to encrypt and decrypt data in order to keep the message secret. Unfortunately it is sometimes not enough to keep the contents of a message secret, it may also be necessary to keep the existence of the message secret. The technique used to implement is called steganography. It is the art and science of invisible communication.

The advantage of steganography over cryptography alone is that messages do not attract attention to themselves, to messengers, or to recipients. Steganographic messages are often first encrypted by some traditional means, and then a cover text is modified in some way to contain the encrypted message, resulting in stego text. This is a technique to embed additional message into some distortion-unacceptable cover media, such as military or medical images, with a reversible manner so that the original cover content can be perfectly restored after extraction of the hidden message.

Steganography is the art and science of writing hidden messages in such a way that no one apart from the intended Recipient knows of the existence of the message; this is in contrast to cryptography, where the existence of the message itself is not disguised, but the content is obscured. The advantage of steganography over cryptography alone is that messages do not attract attention to themselves, to messengers, or to recipients.

II. PROPOSED SCHEME

A sketch of the proposed schemes is given in Fig.1. A content owner encrypts the original uncompressed image using an encryption key to produce an encrypted image, and then a data-hider embeds additional data into the encrypted image using a data-hiding key though he does not know the original con-tent. With an encrypted image containing additional data, a receiver may firstly decrypt it using the encryption key, and the decrypted version is similar to the original image. According to the data-hiding key, he can further extract the embedded data and recover the original image from the decrypted version. The detailed procedures are as follows

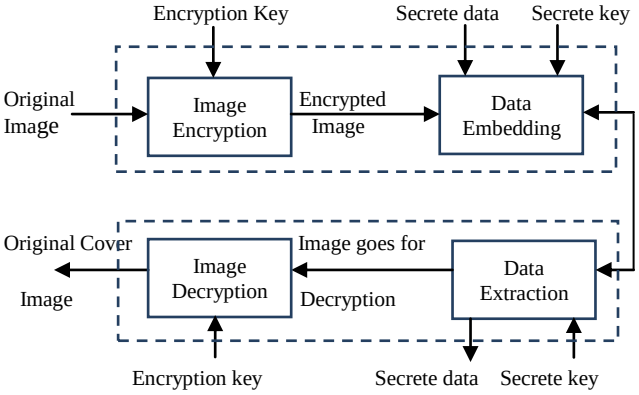


Fig.1 Block Diagram of Proposed Scheme

ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 1, Issue 8, November 2013

A. Image into Image

1. Image Encryption:

In image encryption method first Grayscale Image 512x512 is converted into Binary Image of 512x4096.

1		512
18	10	……
19	99	…….

Fig. 2 Original Grayscale image data (512x512)

1							4096	
0	0	0	1	0	0	1	0	…..
0	0	0	1	0	0	1	1	…..
.								
.								

Fig. 3 Binary Image of (512 x 4096)

Generate key stream of same size of binary image (512x4096)

Apply xoring on converted binary image 512x4096 key streams. We get Cover encrypted Image of 512x4096 size.

Encrypted Image=Binary Image $\oplus$ Key stream

2. Data Embedding:

In Data Embedding process first Generate a key stream which having same size that of secret image.

Encryption of secrete image is carried out using secrete key stream using xoring process.

Encrypted_sec_Img = Sec_img $\oplus$ Secrete Key stream

Each one bit of encrypted secret image is store in 8thbit of the Cover Encrypted image & generates a 512x4096 size of stego image.

One by one bit of encrypted secret image is store in 8thbit place of the Cover Encrypted image & generates a 512x4096 size of stego image.

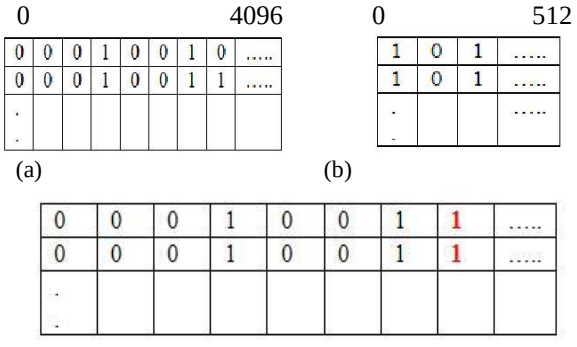


Fig. 4(a) Encrypted Original Image (b) Encrypted Secrete Image (c) Embedded Image

3. Data Extraction:

1) In this step our aim is to extract each 8th bit of embedded image and store it into new matrix having a same rows & columns to that of secret image. After Extracting secrete bits we get our original encrypted cover image back.

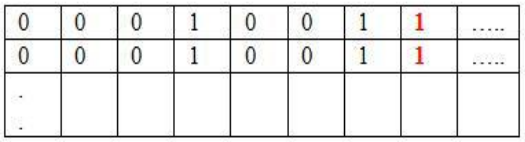


Fig 5. Embedded Image

Fig 6. (a) Recovered Encrypted image (b) Recovered Encrypted Secrete Image

4. Original Secrete Image and Cover Image Recovery:

For Original secrete image we need to xor Matrix of Recovered Encrypted secrete image with secrete key stream that we used at the sender side.

Recovered Sec Img = Recovered Encrypted Secrete img $\oplus$ Secrete Key stream

For Original cover image we need to xor Recovered encrypted image key stream. Then we get Binary Image of size 512x4096.

Binary Image = Recovered Encrypted Image $\oplus$ key stream

Each 8 pixel of Binary Image is converted into Single pixel of Grayscale image then we get Original gray scale cover image.

For Gray pixel

00010010 = 18 similar process for all

B. Text into Image

Basically after converting text into binary number we get one single stream of binary data. Our aim is to embed this data into encrypted cover image. Remaining embedding process is same to that of Image into image steganography.

C. Audio into Image

Audio file is in single stream form. Our need is to embed this audio file into gray scale image. We carried out this process as we did in Image into image steganography.

III. QUALITY PARAMETERS

We have considered various quality parameters such as Peak Signal to Noise Ratio (PSNR), Embedding Capacity (EC) and Number of bits embedded (NBE)

A. Peak Signal to noise ratio (PSNR)

ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 1, Issue 8, November 2013

Peak signal to noise ratio is calculated by using following formula

$$PSNR = 10log_{10}\left(\frac{{MAX_I}^2}{MSE}\right)$$

$$MSE = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j) - K(i,j)]^2$$

Where n is Number of rows in original image.
n is number of columns in original image.
MSE is Mean Square Error.
MAX_I is Maximum pixel value in Original Image.

B. Embedding Capacity (EC)

Embedding Capacity is calculated by using following formula

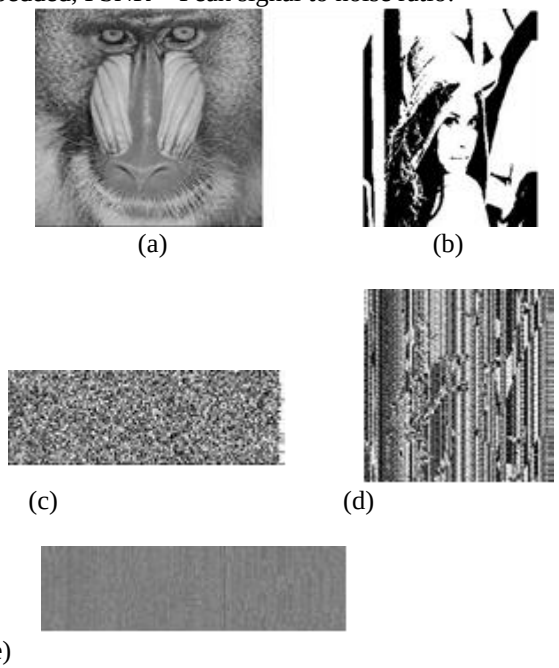
$$EC = \sum_{i=1}^{m}\sum_{j=1}^{n} Cover(i,j)$$

Where m is total number of rows and n is total number of columns. $Cover(i,j)$ is Cover image

IV. EXPERIMENTAL RESULTS AND DISCUSSION

A. Image into Image Method:

Following results are obtained for Baboon Image with the Binary image Lena as a Secrete image. The terms in table are EC = Embedding capacity, NBE = Number of bits embedded, PSNR = Peak signal to noise ratio.



(a) (b) (c) (d) (e)

Fig. 5(a) Original Image (b) Secrete Image (c) Encrypted Original Image (d) Encrypted Secrete Image (e) Stego Image

TABLE I
VARIOUS QUALITY PARAMETERS FOR IMAGE INTO IMAGE

PARAMETRES		
PSNR	**EC**	**NBE**
51.1538	262144	2.09715e+

B. Text into Image Method:

Following results are obtained for barbara Image as a cover image with different size of Text data. The terms in table are EC = Embedding capacity, NBE = Number of bits embedded, PSNR = Peak signal to noise ratio.

(a) (b)

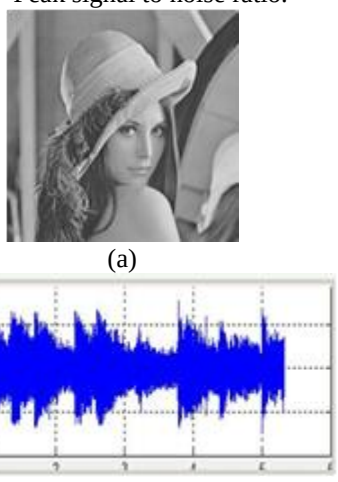
Fig. 6(a) Original Image (b) Stego Image

TABLE II
VARIOUS QUALITY PARAMETERS FOR TEXT INTO IMAGE

Text Size	Parameters		
	PSNR	**NBE**	**EC**
30kb	51.1514	243576	262144
20kb	52.8618	164656	262144
10kb	55.8514	82648	262144

C. Audio into Image:

Following results are obtained for Lena Image as a cover image with the different types of Audio Data. The terms in table are EC = Embedding capacity, NBE = Number of bits embedded, PSNR = Peak signal to noise ratio.

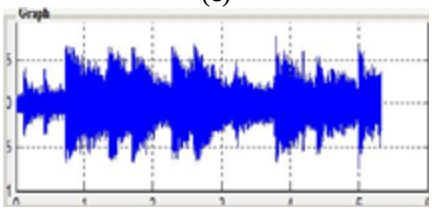


(a) (b)

ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 1, Issue 8, November 2013

(c)



(d)

Fig. 7(a) Original Image (b) Secrete Audio file (c) Stego Image (d) Recovered Audio file

Audio file Size	Parameters		
	PSNR	NBE	EC
104kb	73.7893	53248	262144
320kb	57.7665	81920	262144
504kb	54.2849	258084	262144

V. CONCLUSION

In this work, a novel data hiding scheme for encrypted image with a low computation complexity is proposed, which consists of image encryption, data embedding and data extraction image-recovery phases. The data of original image are entirely encrypted although a data-hider does not know the original content; he can embed additional data into the encrypted image by modifying a part of encrypted data.

With an encrypted image containing embedded data, a receiver may firstly decrypt it using the encryption key, and the decrypted version is similar to the original image. LSB Substitution method is used for embedding purpose. This work gives effective study of simple but strong steganography.

REFERENCES

[1] Xinpeng Zhang "Reversible Data Hiding in Encrypted Image", IEEE SIGNAL PROCESSING LETTERS, VOL. 18, NO. 4, APRIL 2011

[2] J. Tian, "Reversible data embedding using a difference expansion," IEEE Trans. Circuits Syst. Video Technol., vol. 13, no. 8, pp. 890–896, Aug. 2003.

[3] Z.Ni,Y.-Q.Shi,N.Ansari, andW.Su, "Reversibledatahiding,"IEEE Trans. Circuits Syst. Video Technol., vol. 16, no. 3, pp. 354–362, 2006.

[4] M.U.Celik,G.Sharma,A.M.Tekalp,and Saber,"Losslessgen-eralized-LSB data embedding,"IEEE Trans. Image Process.,vol.14, no. 2, pp. 253–266, Feb. 2005

[5] L. Luo, Z. Chen, M. Chen, X. Zeng, and Z. Xiong, "Reversible image watermarking using interpolation technique,"IEEE Trans. Inf. Foren-sics Secur., vol. 5, no. 1, pp. 187–193, 2010.

[6] W. Hong, T.-S. Chen, Y.-P. Chang, and C.-W. Shiu, "A high capacity reversible data hiding scheme using orthogonal projection and predic-tion error modification,"Signal Process., vol. 90, pp. 2911–2922, 2010.

BIOGRAPHIES

Prof.A.R.Nichal received his B.E. degree in Electronics and telecommunication from Shivaji University at Ashta in 2010 and received M.Tech in electronics from Walchand College of engineering, Sangli. His area of interest is Digital Image Processing and embedded system.

Prof.V.B.Kumbhar received his B.E. degree in Electronics from Shivaji University at PVPIT Budhgaom in 2005 and is pursuing M.E in electronics from Shivaji University. His area of interest is Industrial power electronics and Industrial Automation.