Asian Journal of Electrical Sciences
ISSN: 2249-6297 (P) Vol.6 No.2, 2017, pp.25-29

DOI: https://doi.org/10.51983/ajes-2017.6.2.1999

Random Scan Approach for Image Steganography

Sahil Gupta[1] and Kamal Deep Garg[2]
[1]Department of Physics, Baba Farid Group of Intuition, Bathinda, Punjab, India
[2]Department of Computer Science and Engineering,
Chitkara University, Rajpura, Punjab, India
Email: sahil.gupta311@gmail.com

(Received 13 June 2017; Revised 5 July 2017; Accepted 7 August 2017; Available online 16 August 2017)

***Abstract* – Steganography is the art of hiding information in a cover media. The cover and secret data can take many forms such as text, audio, images and videos. In this paper, secret data in the form of (image) is hidden into the cover image. To achieve perceptual invisibility and Robustness, Random Scan approach is used. Before embedding data in cover media, an encryption technique is applied on secret data. Experimental results confirm the PSNR superiority of proposed algorithm.**
***Keywords*: Data security, image steganography, Mean Square Error (MSE), Peak Signal to Noise Ratio(PSNR), EXOR**

I. INTRODUCTION

In today's world, communication via digital media has become more favorable as data is easily available in digital format. However, data security is the most prominent factor for communication on the internet. Numerous approaches have been developed for the security of data during transmission on the internet such as cryptography watermarking and steganography.

Cryptography: It scrambles the secret messages and the data becomes meaningless to eavesdroppers. But data is completely changed so there is an intuition for the attackers of the existence of communication. So this technique is not very much effective alone.

Watermarking: It is used for protection of copyright data as it must be robust against any type of intentional attack that tries to remove or change the data.

Steganography: It is the art of hiding information in such a way that it hides the existence of communication. The origin of word steganography comes from the Greek language where stego means cover and graphia means writing. So (literally meaning *covered writing*)[1]. This technique is used from a long time for secure communication and the first attempt takes place in Greece (440 BC) where King Darius of Susa shaved the head of his slave and then the message was written on his head. They waited until hair came back. Then slave was sent to another place, where his head was shaved again to read the secret message. The second event also took place in Greece when Herodotus says that soldier Demeratus needed to send a message to Sparta. So he used the technique of hiding messages within the wax tablet. He wrote messages on wood and covered it with wax that bore an innocent covering message [2].

Comparison between cryptography, watermarking and steganography are tabulated in table 1[3,4].

TABLE 1 COMPARISON BETWEEN CRYPTOGRAPHY, WATERMARKING, AND STEGANOGRAPHY

Criteria	Cryptography	Watermarking	Steganography
Secret key	Necessary	Optional	Optional
Cover data	Text or image	Digital image/audio	Any media
Security	Medium	High	Very high
Capacity	High	Low	Very high
Visibility	Yes	May or may not be	Never

Out of these, steganography is getting popularity due to high security, high payload capacity, perceptual transparency, robustness and temper resistance.

Figure 1 shows the embedding of secret message in the cover object and its extraction from stego object. This model consists of following elements: cover object (which hides the secret message), secret message, an Encryption Algorithm and Embedding algorithm. The output is in the form of stego object. Later on, the original secret message is extracted from it using extraction algorithm [4].

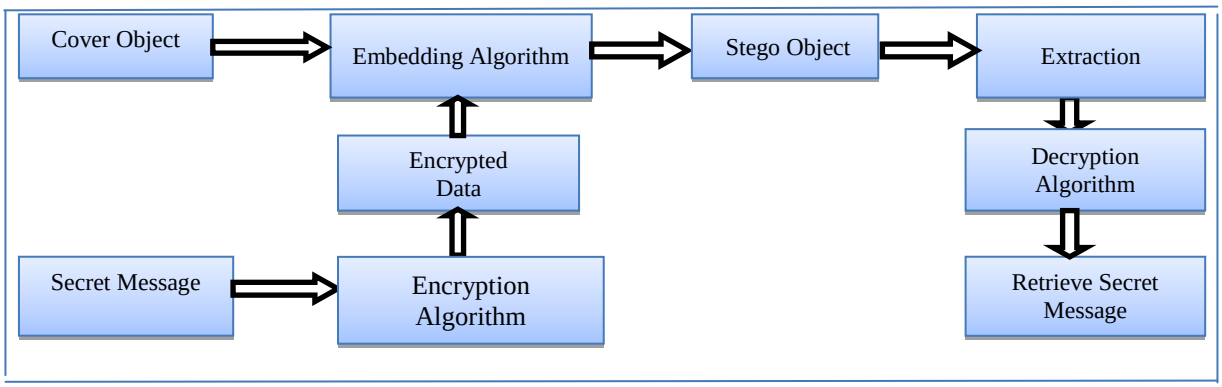


Fig.1 Steganography Model

II. LITERATURE SURVEY

In 2013, Wafaa Hasan Alwan, proposed modified or dynamic based LSB technique for hiding data in the video [5]**.** In this technique, the most significant pixel of hidden image was stored in the least significant pixel of the cover video. The experimental results showed that value of PSNR and MSE varies from 25.33 to 31.16 (dB) and 11.35 to 20.26 respectively. To extend the size of data storage, 3-layer approach was proposed by Jain et al. in 2015. [6]. The advantage of this method was that detection of hidden data was very hard, so security and capacity both got improved. The concept of dual steganography which was a combination of steganography and cryptography is given by Selvigrija et al. in (2015) [7]. Their experimental results indicate the high-level security of dual to secret videos. Bhautmage *et.al* [8] presented a new technique for data embedding and extraction for AVI (audio video interleave) videos in which instead of changing the LSB of the cover file, the LSB and LSB+3 bits are changed in alternate bytes of the cover file.

III. EXPERIMENTAL SET UP

To embed secret data (image) in the cover image, Random Scan technique is implemented here. The experimental set up of this process is shown in figure 2.

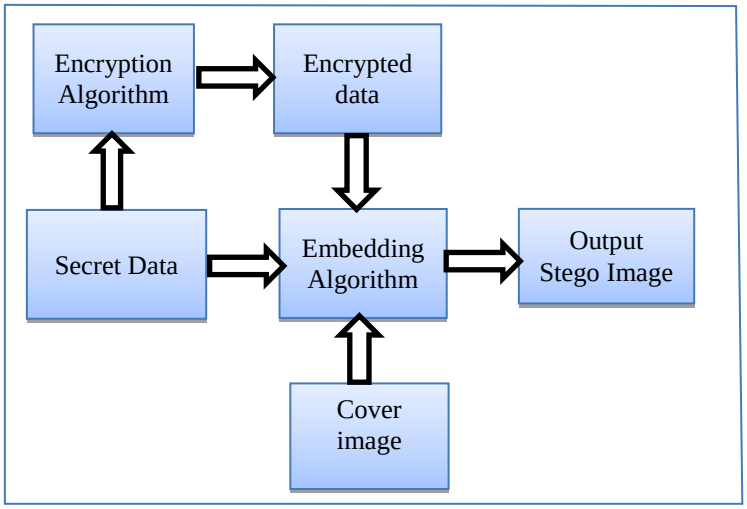


*Fig.*2 Experimental set up of image Steganography

Secret data: The secret data can be in any form like text, audio and image. In the proposed algorithm, the image is taken as secret data. Firstly secret image is read out using "imread" Matlab command and get information about the pixel present in it.

Encryption Algorithm: To enhance security, all pixels present in secret data are encrypted using 1's complement and encrypted pixels are available.

Cover Image: The cover media can be in any form like test, audio, image and video. In the present work, the image is taken as cover media.

Embedding Algorithm: Before embedding the secret data, each 8-bit pixels of encrypted data is split into 4 new pixels of 8 bit each using AND operation. Then each of this 4 pixels has 2 bit of encrypted data and all other bits are made zero. After that data is embedded in the cover image using Random Scan technique.

Random scan technique- Here, data is hidden at (1 to 4) LSB position randomly taking any 2 positions at a time and EXOR operation is used to embed the secret data.

Stego image: After embedding the encrypted data in the cover image, stego image is generated.

The data embedding and pixel variation in Random scan technique are illustrated by taking an example:

Example:

1. Secret data pixel value: 10100010
2. Encrypted pixel value: 01011101
3. Cover image Pixels value
4. Stego image pixel Values by Random Scan Technique.

TABLE II COVER IMAGE PIXEL VALUE

Cover data of Ist Row	00101011	10100001	10010100	01010001

TABLE III STEGO IMAGE PIXEL VALUE AFTER RANDOM SCAN TECHNIQUE

Cover data of ist Row	00101011	10100001	10010100	01010001
Encrypted data shifted to any ist four LSB position taking two at a time	00000100	00000011	00000100	00000001
Data Embedding using EXOR	00101111	10100010	10010000	01010000

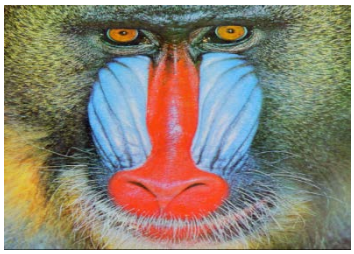
IV. RESULTS AND DISCUSSION

For testing the proposed method, several simulations were performed to evaluate the performance in term of PSNR, MSE and correlation factor. PSNR describe the quality of the stego image compared with the cover image. MSE indicates dissimilarity between Cover image and Stego image and correlation factor measure of extent and direction of a linear combination of two random variables [9]. A set of 5 test images namely (Lina, Babbon, Peppers, Barbara and Tiffany) were used as a cover image and one test image (Elephant) was used as a secret image. Taking one of test image as a cover image and an encrypted version of the secret image is embedded using Random scan algorithm.

The whole work is performed on MATLAB 2013. The input cover and output stego images are shown in figure 5.

(a) Cover image Lena

(b) Stego image Lena



(a) Cover image Babbon

(b) Stego image Babbon

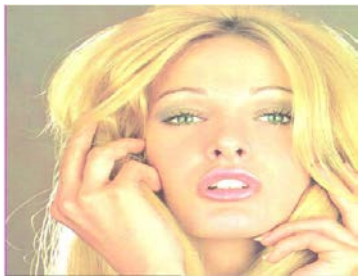
(a) Cover image Peppers

(b) stego image Pepper

(a) Cover image Barbara

(b) Stego image Barbaar

(a) Cover image Tiffany



(b) Stego image Tiffany

Fig.3 Input and Output (a) Cover image (b) stego image

According to the invisibility benchmark, minimum PSNR value of 30 dB is adopted as a quality requirement of stego image [10]. Our experimental results are promising as can be concluded from table 4 that PSNR value lie between (45.48- 46.01), the MSE value lies between (1.62-1.83) and correlation factor is .999. Therefore the proposed method is showing the high value of PSNR, the low value of MSE and correlation factor is approximately close to 1.

TABLE IV EXPERIMENTAL RESULTS OF PROPOSED METHOD FOR DIFFERENT TEST IMAGES

Test image	**Size**	**Format**	**Proposed method**		
			PSNR	**MSE**	**Correlation**
Lena	512*512	Png	46.00	1.632	.999
Babbon	512*512	Png	45.82	1.70	.999
Peppers	512*512	Png	45.58	1.79	.999
Barbara	720*576	Bmp	46.01	1.62	.999
Tiffany	512*512	Bmp	45.48	1.83	.999
Average			45.8	1.70	.999

For the sake of comparative evaluation of proposed method, we have compared the algorithm with other algorithm [11,12,13,14] as shown in table 5 and figure 4. It is cleared from results that proposed method achieved a high value of PSNR and low value of MSE.

TABLE V COMPARISON OF PSNR VALUE OF PROPOSED METHOD WITH OTHER METHODS

Method	PSNR (dB)				
	Lena	Babbon	Tiffany	Barbara	Average
Luo et al.'s [11]	38.80	33.33	38.88	37.45	37.11
Lin [12]	37.70	36.55	37.99	n/a	37.41
Chan et al.'s [13]	37.23	39.09	41.31	37.31	38.73
Lee et al.'s [14]	32.17	30.02	35.09	31.32	32.15
Proposed method	46.00	45.82	45.48	46.01	45.82

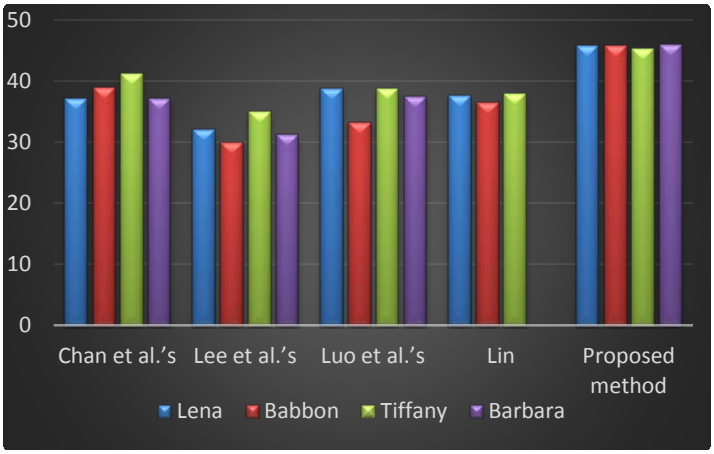


Fig.4 Comparison of PSNR value of proposed method with other methods

V. CONCLUSION

In this paper, secret data is hidden randomly at its 4 LSB position of the cover image. To enhance the security, an encryption technique is also applied before embedding. The proposed method maintains the stego image quality with an average PSNR value of 45.8 dB and MSE value of 1.70. Higher the PSNR and lower the MSE value, better is the steganography algorithm. So the proposed method fulfills both criteria of PSNR and MSE. In Future, more emphasis will be given on frequency domain, dual steganography and visual cryptography due to better PSNR and MSE value as compared to the spatial domain.

REFERENCES

[1] Bassam Jamil mohd, Saed Abed and Thaier Al-hayajneh, Sahel Alouneh, "FPGA Hardware of the LSB Steganography Method", *Computer, Information and Telecommunication Systems (CITS)*, 2012.

[2] K.S.Jenifer, G. Yogaraj and K. Rajalakshmi, 2014, "Approach for Video Steganography to embed Images," *International Journal of Computer Science and Information Technologies*, Vol. 5, No.1, 319-322, 2014.

[3] Mennatalla m. sadek, Amal S. Khalifa and Mostafa G.M.Mostafa, "Video Steganography: A Compressive Review", Multimed Tools Appl, 2014.

[4] Bharti Chandel and Shaily Jain, "Video Staganography: A Survey", *IOSR Journal of Computer Engineering*, Vol. 18, No.1, 2016, pp. 11-17.

[5] Wafaa Hasan Alwan, "Dynamic Least Significant Bit technique for Video Steganography", *Journal of Kerbala university*, Vol.11, No.4, , pp. 7-16, 2013.

[6] Neha Jain and Sudhir Goswami, "An Improved Steganography Technique of LSB Substitution Method", *International Journal of Engineering and Computer Science*, Vol.4, No.1, pp. 9912-9915, 2015.

[7] Selvigrija and E. Ramya, "Dual Steganography for Hiding Video in Video", *International Journal for Trends in Engineering and technology*, Vol.3, No.3, pp. 74-79, 2015.

[8] Pritish Bhautmage, Amutha Jeya Kumar and Ashish Dahatonde, "Advanced Video Steganography Algorithm," *International Journal of Engineering Research*, Vol.3, No.1, pp. 1641-1644, 2013.

[9] S.Uma Maheswari and D.Jude Hemanth, "Frequency domain QR code based Image Steganography using Fresnlet Transform", *International Journal of electronics and Communications*, Vol. 69, pp 539-544, 2015.

[10] Abbas Cheddad, Joan Condell, Kevin Curran and Paul Mc Kevitt, "Skin Tone Based Steganography in Video Files exploiting the YCBCR Colour Space," *International Conference on Multimedia and Expo*, 2008, pp 905-908.

[11] Luo W, Huang F and Huang J. "Edge adaptive image steganography based on LSB matching revisited", *IEEE Trans Inform Forensics Secure*, Vol.5, No.2, pp. 201–214, 2010.

[12] Lin YK, "High capacity reversible data hiding scheme based up on discrete cosine transformation" *Journal of System and Software*, pp. 2395–2404, 2012.

[13] Chan YK, Chen WT, Yu SS, Ho YA, Tsai CS and Chu YP, "A HDWT-based reversible *data hiding method", Journal of System and Software*, pp. 411–21, 2009,

[14] Lee CF, Chen HL and Tso HK, " Embedding capacity raising in reversible data hiding based on prediction of difference expansion", *Journal of System and Software*, , pp.1864–1872, 2010.