Research Journal of Information Technology

ISSN 1815-7432

Academic Journals Inc.

www.academicjournals.com

Research Journal of Information Technology 5 (2): 171-180, 2013
ISSN 1815-7432 / DOI: 10.3923/rjit.2013.171.180

Key Decided Cover for Random Image Steganography

Rengarajan Amirtharajan, V. Mahalakshmi, J. Nandhini, R. Kavitha and J.B.B. Rayappan
Department of Electronics and Communication Engineering, School of Electrical and Electronics Engineering, SASTRA University, Thanjavur, 613 401, India

Corresponding Author: Rengarajan Amirtharajan, Department of Electronics and Communication Engineering, School of Electrical and Electronics Engineering, SASTRA University, Thanjavur, 613 401, India

ABSTRACT

The electronic era of today rely on almost all sorts of online communication to a great extent which indeed and in turn encounters many menaces and malware attacks. The solution in disguise came in the forms of cryptography and steganography. Although, these have a long history, their updated and digital forms, derivatives, is implemented to ensure secure communication. Here proposes a yet another study in steganography which pleases the intention for which it is shaped. The study puts forward three techniques Coding method, Diagonal traversing and Random pixel traversing, respectively. The underlying idea in these methods is that confidential information is embedded in the cover based on the key generated. The performance is evaluated by means of several image metrics. The routine augments the enigmatic effect of the data camouflage, making it intricate for any invader to haul out the clandestine data.

Key words: Steganography, coding method, diagonal traversing method, random pixel traversing method

INTRODUCTION

The modern era digital communication bloomed with the evolution of internet. As it is nothing but the interconnection of computer networks globally, it employs state-of-the-art modern day optical and wireless technologies. This has paved the way for extensive researches in the field of information security to mainly detect and correct datum sabotage (Cheddad *et al*., 2010; Salem *et al*., 2011; Schneier, 2007; Stefan and Fabin, 2000). The first and foremost functions of information security are information protection, control access and administer users. Some threats for the aforementioned include attacks erudition, rapid exposure to weaknesses, disseminated attacks and intricacies of patching. Information security makes certain the veracity, discretion, ease of use and off the record facts. The main goal here is to cater to the quandaries in the administrative, technical and physical fields in secure applications.

Cryptography concept dates back to 2000 BC, through hieroglyphics- an Egyptian practice. In modern world, cryptography has become a combat zone of top computer scientists and mathematicians (Schneier, 2007; Zaidan *et al*., 2010). Because, today, the decisive issue in business, online communication, war etc is the capability to safely hoard and transmit perceptive data. Cryptography is a significant classification of security system. It is characterized by plain text (original text), encryption (encoding), cipher text (modified text), decryption (decoding), key (tool with which plaintext is turned to cipher text). According to the keys used, cryptography can be

classified as public key cryptography and private key cryptography (Rajagopalan *et al*., 2012; Salem *et al*., 2011; Schneier, 2007; Zaidan *et al*., 2010). The two ciphers used in this mechanism are block ciphers and stream ciphers. In former, the operation is done on blocks of ciphers while in the latter operation is done bit by bit. The time taken for encryption and decryption is the disadvantage of cryptography. The effective solution to this problem will be steganography (Al-Azawi and Fadhil, 2010; Al-Frajat *et al*., 2010; Xiang *et al*., 2011; Zanganeh and Ibrahim, 2011; Zhao and Luo, 2012; Zhu *et al*., 2011) and watermarking (Abdulfetah *et al*., 2010; Zeki *et al*., 2011) and its counter attack explained by Qin *et al*. (2010) called steganalysis.

"Steganography"- We can't say that this sounds alien. It has been in use since very ancient times; term coined from Greek and is nothing but secret message in disguise. putting it simple, hidden writing. Now it is used in digitalized version. So, what exactly does it mean? The phenomenon by which one digit file is hidden or embedded in other (Amirtharajan and Rayappan, 2012a-d; Amirtharajan *et al*., 2012; Bender *et al*., 1996; Cheddad *et al*., 2010; Janakiraman *et al*., 2012a, b; Rajagopalan *et al*., 2012; Thenmozhi *et al*., 2012). The files can be text (Al-Azawi and Fadhil, 2010; Xiang *et al*., 2011), video(Al-Frajat *et al*., 2010), audio (Zhu *et al*., 2011) and image (Amirtharajan and Rayappan, 2012a-d; Amirtharajan *et al*., 2012; Gutub, 2010; Hmood *et al*., 2010a, b; Janakiraman *et al*., 2012a; Padmaa *et al*., 2011; Thanikaiselvan *et al*., 2011; Thenmozhi *et al*., 2012; Zanganeh and Ibrahim, 2011). As it does so, it is mainly attributed to images.

The main modules of steganography are:

- Cover image (in which desired message is hidden)
- Secret message/image (confidential information)
- Key (tool used to do embed/retrieve the secret known only to the sender and receiver)
- Finally steganographic algorithm (the procedure or method of Steganography)

So, what is the unique feature of steganography or why it is needed? Of many, important uses are to combat fraud detection, authentication, traitor tracing, copy control, data integrity and many more (Stefan and Fabin, 2000; Zaidan *et al*., 2010). What a stego image should thrive for? The answer will be robustness, capacity and imperceptibility. That is more of secret information should be hidden and the resultant should survive the attacks and hence, of course, should be free of human artifacts (Luo *et al*., 2011; Mohammad *et al*., 2011).

Watermarking is a vital sub discipline of information hiding (Abdulfetah *et al*., 2010; Stefan and Fabin, 2000; Zeki *et al*., 2011). Mostly, it takes audio or image files as carrier and the secret data to be conveyed is termed as watermark. The main intention of watermarking is preservation of copyright and the substantiation is accomplished by cross correlation. The attack on watermarking is done by image processing. The mechanism does not make the grade when the payload (watermark) is swapped or removed. Watermarking is a trait of the cover, i.e., cover is imperative than message. But its choice is constrained. It can be done in Spatial domain (color separation, bit flipping) and Frequency domain (i.e., embedding in high frequencies). Unlike Steganography, here exists 1: many communications but the challenge is that an interloper can't replace or confiscate the message. In watermarking, prominence is laid on avoiding deformation of cover and every method should be as stout as possible.

Aforementioned methods have given an overview about data security through various cover objects and there is a good scope for random image steganography; hence this paper proposes three such methods to improve the randomness and imperceptibility.

PROPOSED METHOD

Method 1: In this method, two keys are used; one for defining the number of secret bits and the other to locate the area to embed. Thus, using the given key code array, text data is embedded in an image and if the code contains binary one the secret data is embedded otherwise no embedding takes place.

Method 2: Here, the text data is entrenched in cover image's pixels in random fashion. Both the size of the secret data and cover image decides the selection of those random pixels.

Method 3: Embedding follows the diagonal traversing style in this routine as in Fig. 1. That is traversing is followed from the leftmost pixel value to the rightmost one of the cover image as per the key. Figure 2 describes the proposed methodology, where the embedding adopts any of the methods 1, 2 or 3.

Coding algorithm: Embedding algorithm:

Inputs: cover image(c), secret data (D), Keys K1, K2.

Outputs: Stego image.

Step 1: Convert D to binary form as in Fig. 3

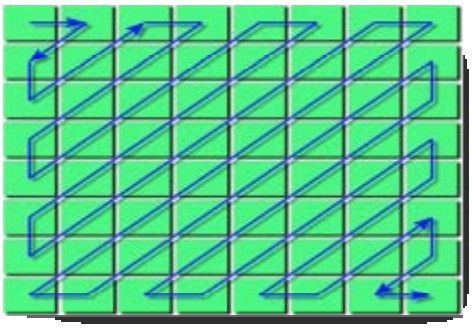

Fig. 1: Embedding in diagonal traversing path

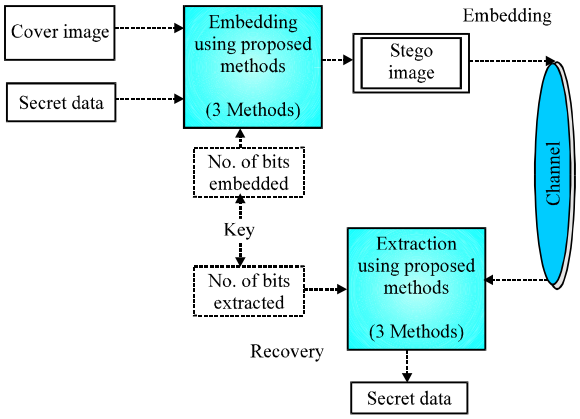

Fig. 2: Block diagram of proposed method

Algorithm Continue:

Step 2: Read the cover image
Step 3: Read the key k1
Step 4: Decide the number of secret bits inserted in each pixel
Step 5: Read the key K2
Step 6: User decides the key code array
Step 7: Based upon the key code array embed the secret data in the cover image
Step 8: If all the secret data is embedded, then store it as Stego image

Random pixel traversing algorithm:

Inputs: cover image(c), secret data (D),Key k.
Outputs: Stego image.
Step 1: Convert the secret data into binary format
Step 2: Obtain the gray cover image
Step 3: Read the key k
Step 4: Decide the no. of secret bits inserted in each pixel
Step 5: m = size of the secret data in terms of bits
Step 6: n = size of the cover image
Step 7: Let check the following condition
If(m<=n)
P = pixels are randomly selected based upon the size of the secret data
Else
P = pixels are randomly selected based upon the size of the cover image
Step 8: Based on the random key embed the secret data in the cover image
Step 9: if all the secret data is embedded, then store it as Stego image

Figure 4 and 5 represents the flowchart for random pixel and diagonal traversing methods, respectively.

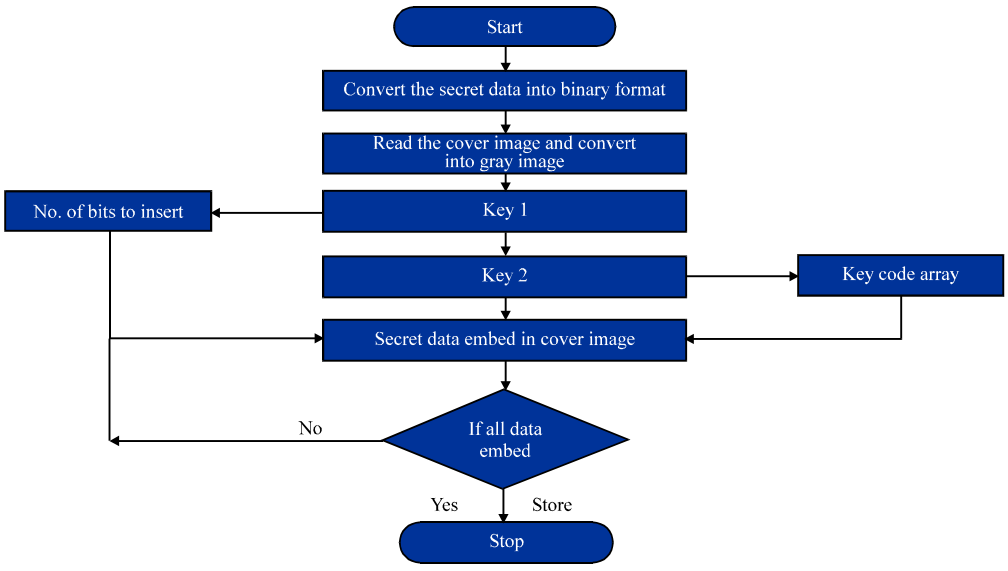

Fig. 3: Flow chart for coding method 1

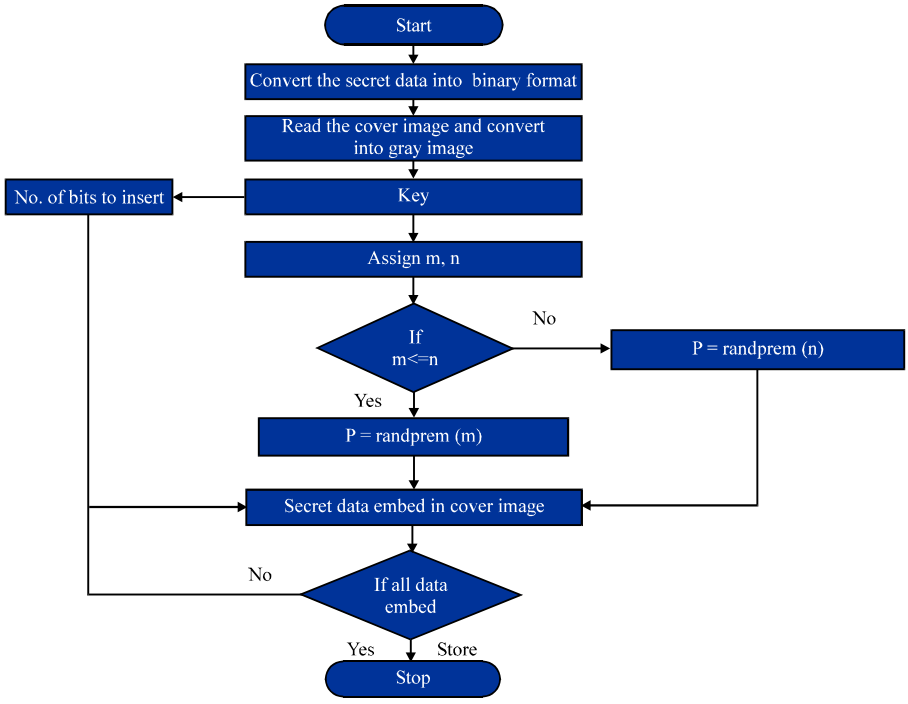

Fig. 4: Flow chart for random pixel traversing method

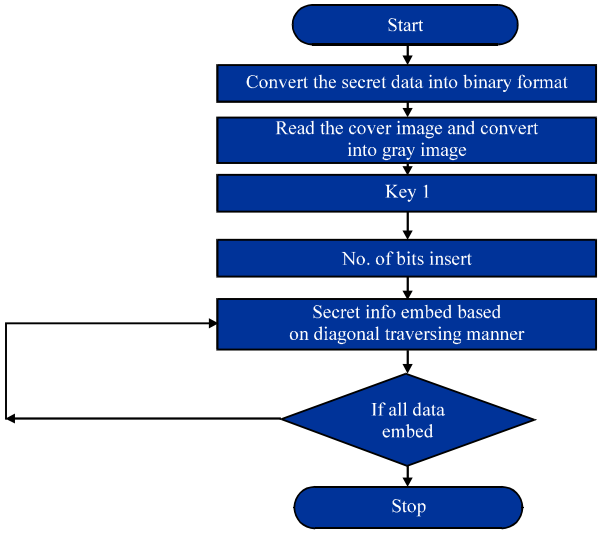

Fig. 5: Flow chart for diagonal traversing method

Diagonal traversing method:

Algorithm:

Inputs: Cover image(c),secret data(D),Key k.

Outputs: Stego image with secret data embedded in it.

Step 1: Convert the secret data into binary format

Algorithm continue:

Step 2: Obtain the color image and convert into gray image

Step 3: Read the key k

Step 4: Decide the no. of secret bits inserted in each pixel

Step 5: Secret information is embedded based on the diagonal traversing manner

Step 6: If all the secret data is embedded, then store it as Stego image

RESULTS AND DISCUSSION

Four gray cover images Lena, Baboon, Gandhi and Temple of size 256×256 pixels is considered for testing the performance all the implemented methods in Matlab. Figure 6a-d are used as cover images are tested for full embedding capacity and the stego images are given in Fig. 7a-d, respectively for coding method 1. The obtained MSE, PSNR, MSSIM, Relative entropy and payload readings of all the stego objects are tabulated in Table 1-3, respectively.

Results of random pixel traversing method: Figure 8a-d are used as cover images are tested for full embedding capacity and the stego images are given in Fig. 9a-d, respectively for Random pixel traversing method.

Table 1: MSE, PSNR, MSSIM and relative entropy values for coding method for K1 = 3 and K2 = 11010

Cover image	MSE	PSNR	MSSIM	Relative entropy	Embedding capacity
Lena256	20.2395	32.0924	0.9043	0.0410	149048
Baboon256	14.8923	33.4247	0.9768	0.0284	138000
Temple256	17.1919	32.8011	0.9277	0.0397	143000
Mahatmagandhi	12.0589	34.3413	0.9341	0.0345	132024

Table 2: MSE, PSNR, MSSIM and relative entropy values for random pixel traversing method: K = 4 and K2 = 11010

Cover image	MSE	PSNR	MSSIM	Relative entropy	Embedding capacity
Lena256	18.5665	32.4671	0.9045	0.2394	205992
Baboon256	16.4291	32.9982	0.9747	0.2235	202304
Temple256	12.6741	34.1252	0.9344	0.2188	194736
Mahatmagandhi	14.5296	33.5318	0.9222	0.2581	199280

Table 3: MSE, PSNR, MSSIM and relative entropy values for diagonal traversing method: K = 4 and K2 = 11010

Cover image	MSE	PSNR	MSSIM	Relative entropy	Embedding capacity
Lena256	18.6745	32.4419	0.9049	0.2505	205992
Baboon256	15.9062	33.1387	0.9786	0.2245	201440
Temple256	12.8615	34.0615	0.9332	0.2277	196264
Mahatmagandhi	15.1929	33.3380	0.9184	0.2623	200808

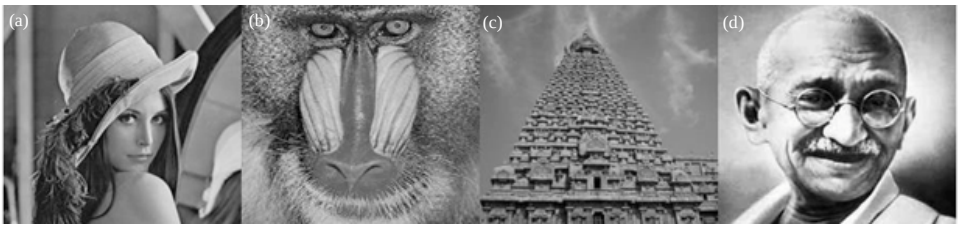

Fig. 6(a-d): Cover image of (a) Lena (b) Baboon (c) Temple and (d) Mahatma Gandhi by using Coding methods

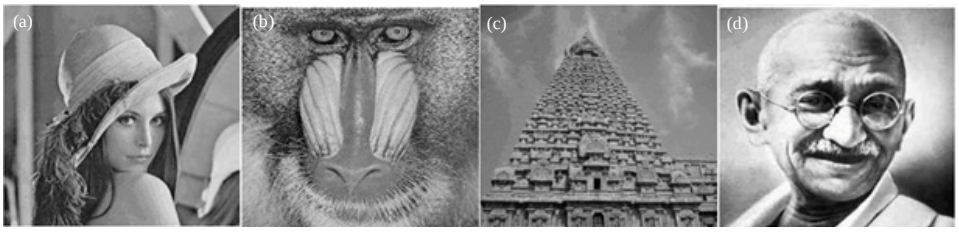

Fig. 7(a-d): Stego image of (a) Lena, (b) Baboon, (c) Temple and (d) Mahatma Gandhi, by using Coding methods

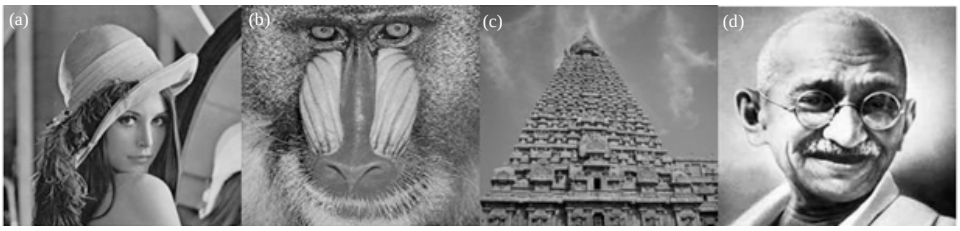

Fig. 8(a-d): Cover image of (a) Lena, (b) Baboon, (c) Temple and (d) Mahatma Gandhi, by using Random pixel traversing methods

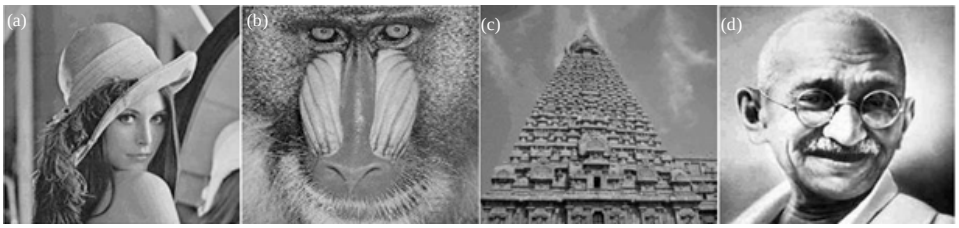

Fig. 9(a-d): Stego image of (a) Lena, (b) Baboon, (c) Temple and (d) Mahatma Gandhi, by using Random pixel traversing methods

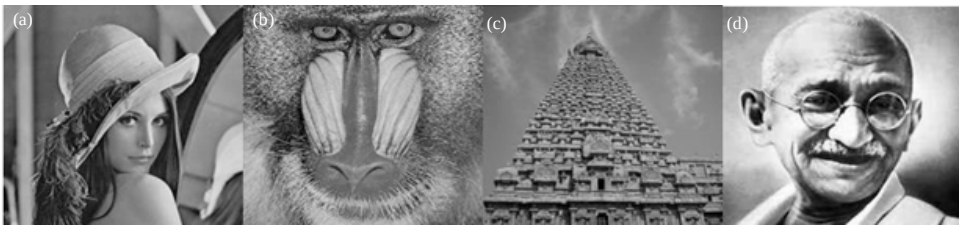

Fig. 10(a-d): Cover image of (a) Lena, (b) Baboon, (c) Temple and (d) Mahatma Gandhi, by using Diagonal traversing method

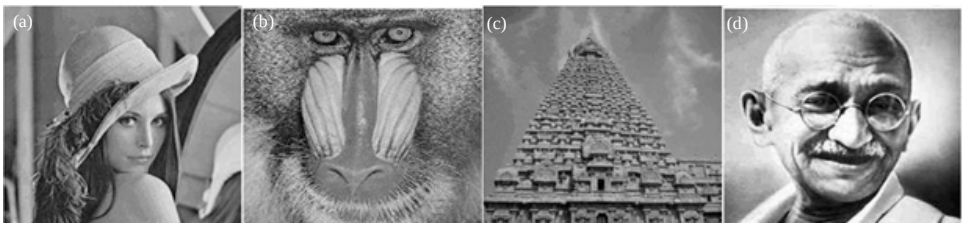

Fig. 11(a-d): Stego image of (a) Lena, (b) Baboon, (c) Temple and (d) Mahatma Gandhi by using Diagonal traversing method

To evaluate the performance of the proposed methods MSE, PSNR, MSSIM, Relative Entropy and capacity of the stego images is calculated using the following formulae. Figure 10a-c and d are used as cover images are tested for full embedding capacity and the stego images are given in Fig. 11a-c and d, respectively for Diagonal traversing method.

Mean square error: The average squared difference between a original image and resultant (stego) image is called Mean Squared Error (MSE). It dampens small variation between the two pixels but reprimands large ones:

$$MSE = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}\left(o_{ij} - s_{ij}\right)^2$$

where, o_{ij} represents the pixels in the original image and s_{ij} represents the pixels of the stego-image.

Peak signal-to-noise ratio: The higher the Peak Signal-to-Noise Ratio (PSNR), the nearer the stego image is to the cover. A higher PSNR value associates to a high quality image:

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

Mean structural similarity index: To interpret the overall image quality we use Mean Structural Similarity Index (MSSIM) which is expressed by:

$$MSSIM\ (O,S) = \frac{1}{M}\sum_{j=1}^{m} SSIM\left(O_j, S_j\right)$$

$$SSIM(X,Y) = \frac{\left(2\mu_O\mu_S + C_1\right)\left(2\sigma_{OS} + C_2\right)}{\left(\mu_O^2 + \mu_S^2 + C_1\right) \geq \left(\sigma_O^2 + \sigma_S^2 + C_2\right)}$$

where, $C_1 = (K_1L)^2$ L = 255.

$$K_1 = 0.01\ C_2 = (K_2L)^2\ L = 255\ K_2 = 0.03$$

$$\mu O = \frac{1}{N}\sum_{i=1}^{N} xi$$

where, μ_O is the estimate of the mean intensity of the cover (N = 255), σ_0 is the standard deviation.

$$\sigma_O = \left(\frac{1}{N-1}\sum_{i=1}^{N}\left(O_i - \mu_i\right)^2\right)^{\frac{1}{2}}$$

$$\sigma_{OS} = \frac{1}{N-1}\sum_{i=1}^{N}\left(O_i - \mu_O\right)\left(S_i - \mu_O\right)$$

Here σ_{OS} is correlation coefficient.

Relative entropy: The parameter that concerns about stego system's security. when P(el), P(e2), ..., P(em) exhibits a particular intensity probabilities. The entropy of an image is expressed by:

$$H(e)=\log_2 (p(ei))$$

If P_c denotes probability distribution of the cover image and p_s denotes probability distribution of the stego image. Then the relative entropy is expressed by:

$$D(p_c \text{II } P_s)=\sum PC \log\left(\frac{P_c}{P_s}\right)$$

CONCLUSION

Steganography is the science of hiding information. Complexity of a stego-image should be higher and it can be improved by embedding the pixel in disorder way; since it requires entropy as a paramount parameter, randomization plays a vital role in steganography. Imperceptibility and embedding capacity are improved with the help of three methods namely random pixel traversing method, diagonal traversing method and coding algorithm. In this paper the observed value of MSE, PSNR, MMSIM, ENTROPY are outstanding than the existing methods and also provides a surpassing security. It offers elevated capacity while retaining a fine stego image eminence. Even if someone looks into the indiscrimination, envisioning for each pixel causes nightmare to the prowler. Thus, this paper offers everything what a steganographic scheme should take.

REFERENCES

Abdulfetah, A.A., X. Sun, H. Yang and N. Mohammad, 2010. Robust adaptive image watermarking using visual models in DWT and DCT domain. Inf. Technol. J., 9: 460-466.

Al-Azawi, A.F. and M.A. Fadhil, 2010. Arabic text steganography using kashida extensions with huffman code. J. Applied Sci., 10: 436-439.

Al-Frajat, A.K., H.A. Jalab, Z.M. Kasirun, A.A. Zaidan and B.B. Zaidan, 2010. Hiding data in video file: An overview. J. Applied Sci., 10: 1644-1649.

Amirtharajan, R. and J.B.B. Rayappan, 2012a. An intelligent chaotic embedding approach to enhance stego-image quality. Inf. Sci., 193: 115-124.

Amirtharajan, R. and J.B.B. Rayappan, 2012b. Brownian motion of binary and gray-binary and gray bits in image for stego. J. Applied Sci., 12: 428-439.

Amirtharajan, R. and J.B.B. Rayappan, 2012c. Inverted pattern in inverted time domain for icon steganography. Inf. Technol. J., 11: 587-595.

Amirtharajan, R. and J.B.B. Rayappan, 2012d. Pixel authorized by pixel to trace with SFC on image to sabotage data mugger: A comparative study on PI stego. Res. J. Inf. Technol., 4: 124-139.

Amirtharajan, R., J. Qin and J.B.B. Rayappan, 2012. Random image steganography and steganalysis: Present status and future directions. Inf. Technol. J., 11: 566-576.

Bender, W., D. Gruhl, N. Morimoto and A. Lu, 1996. Techniques for data hiding. IBM Syst. J., 35: 313-336.

Cheddad, A., J. Condell, K. Curran and P.M. Kevitt, 2010. Digital image steganography: Survey and analysis of current methods. Signal Process., 90: 727-752.

Gutub, A.A.A., 2010. Pixel indicator technique for RGB image steganography. J. Emerg. Technol. Web Intell., 2: 56-64.

Hmood, A.K., B.B. Zaidan, A.A. Zaidan and H.A. Jalab, 2010a. An overview on hiding information technique in images. J. Applied Sci., 10: 2094-2100.

Hmood, A.K., H.A. Jalab, Z.M. Kasirun, B.B. Zaidan and A.A. Zaidan, 2010b. On the capacity and security of steganography approaches: An overview. J. Applied Sci., 10: 1825-1833.

Janakiraman, S., R. Amirtharajan, K. Thenmozhi and J.B.B. Rayappan, 2012a. Firmware for data security: A review. Res. J. Inf. Technol., 4: 61-72.

Janakiraman, S., R. Amirtharajan, K. Thenmozhi and J.B.B. Rayappan, 2012b. Pixel forefinger for gray in color: A layer by layer stego. Inf. Technol. J., 11: 9-19.

Luo, H., Z. Zhao and Z.M. Lu, 2011. Joint secret sharing and data hiding for block truncation coding compressed image transmission. Inf. Technol. J., 10: 681-685.

Mohammad, N., X. Sun and H. Yang, 2011. An excellent Image data hiding algorithm based on BTC. Inf. Technol. J., 10: 1415-1420.

Padmaa, M., Y. Venkataramani and R. Amirtharajan, 2011. Stego on 2n: 1 Platform for users and embedding. Inf. Technol. J., 10: 1896-1907.

Qin, J., X. Xiang and M.X. Wang, 2010. A review on detection of LSB matching steganography. Inf. Technol. J., 9: 1725-1738.

Rajagopalan, S., R. Amirtharajan, H.N. Upadhyay and J.B.B. Rayappan, 2012. Survey and analysis of hardware cryptographic and steganographic systems on FPGA. J. Applied Sci., 12: 201-210.

Salem, Y., M. Abomhara, O.O. Khalifa, A.A. Zaidan and B.B. Zaidan, 2011. A review on multimedia communications cryptography. Res. J. Inf. Technol., 3: 146-152.

Schneier, B., 2007. Applied Cryptography: Protocols, Algorithm and Source Code in C. 2nd Edn., Wiley, India.

Stefan, K. and A. Fabin, 2000. Information Hiding Techniques for Steganography and Digital Watermarking. Artech House, London, UK.

Thanikaiselvan, V., S. Kumar, N. Neelima and R. Amirtharajan, 2011. Data battle on the digital field between horse cavalry and interlopers. J. Theor. Applied Inf. Technol., 29: 85-91.

Thenmozhi, K., P. Praveenkumar, R. Amirtharajan, V. Prithiviraj, R. Varadarajan and J.B.B. Rayappan, 2012. OFDM+CDMA+Stego = Secure communication: A review. Res. J. Inf. Technol., 4: 31-46.

Xiang, L., X. Sun, Y. Liu and H. Yang, 2011. A secure steganographic method via multiple choice questions. Inf. Technol. J., 10: 992-1000.

Zaidan, B.B., A.A. Zaidan, A.K. Al-Frajat and H.A. Jalab, 2010. On the differences between hiding information and cryptography techniques: An overview. J. Applied Sci., 10: 1650-1655.

Zanganeh, O. and S. Ibrahim, 2011. Adaptive image steganography based on optimal embedding and robust against chi-square attack. Inf. Technol. J., 10: 1285-1294.

Zeki, A.M., A.A. Manaf and S.S. Mahmod, 2011. High watermarking capacity based on spatial domain technique. Inf. Technol. J., 10: 1367-1373.

Zhao, Z. and H. Luo, 2012. Reversible data hiding based on Hilbert curve scan and histogram modification. Inf. Technol. J., 11: 209-216.

Zhu, J., R.D. Wang, J. Li and D.Q. Yan, 2011. A huffman coding section-based steganography for AAC audio. Inf. Technol. J., 10: 1983-1988.