Research Journal of Information Technology

ISSN 1815-7432

Academic Journals Inc.

www.academicjournals.com

Research Journal of Information Technology 5 (2): 209-217, 2013
ISSN 1815-7432 / DOI: 10.3923/rjit.2013.209.217

Concealed to Protect and Protect to Conceal: A Conserved Stego Image

[1]Rengarajan Amirtharajan, [2]R. Anushiadevi, [2]V. Meena, [2]V. Kalpana and [1]J.B.B. Rayappan

[1]Department of Electrical and Computer Engineering, School of Electrical and Electronics Engineering, SASTRA University, India

[2]Department of Computer Science and Engineering, School of Computing, SASTRA University, India

Corresponding Author: Rengarajan Amirtharajan, Department of ECE, School of Electrical and Electronics Engineering, SASTRA University, India

ABSTRACT

In the ubiquitous computing world, data are accessed by everyone at any time anywhere. People want to perform their business and personal tasks on-line. A person always wants to be on communication for banking, shopping and learning. The attractive and faster access on line facilities have to concern the secrecy of the messages exchanged over the communication media. Besides the communicating parties, there is a chance for the intruder to access the secret data. Data should be secured such that no malicious user knows the presence of the secret data. Everybody in this universe needs a secret communication world. To satisfy the need of all the Internet users, information hiding technology has developed. The most powerful weapon to hide a secret message is steganography, which is older than cryptography. This study presents one more algorithm involving three easily implementable but complex procedures to increase the security during transmission of secret data. The routines are key value based k-bit embedding, embedding in line with Fibonacci series and by Shannon-Fano encoding, respectively. Each method follows an ideal procedure to encapsulate more secret information at the same time meeting other requirements for an idyllic transmission. The performance of this study is evaluated by means of MSE and PSNR and the results are tabled.

Key words: Information hiding, steganography, Fibonacci series, Shannon-Fano encoding

INTRODUCTION

Steganography appeared before cryptography. In the 5th century BC, King Darius used steganography for his communication. He used their political prisoners as cover medium and tattooed the secret message onto the shaven scalp of the prisoner. It becomes stego after hair grows. Wax tablets, invisible inks and microdots were also used for Steganography (Kahn, 1983). While Cryptography protects the contents of a message (Schneier, 2007), Steganography holds responsibility for defending information and communicating bodies (Stefan and Fabin, 2000; Bender *et al*., 1996, 2000). Traits of Steganography and that of Watermarking are almost alike. One of the main differences between these two techniques needs to be highlighted (Hmood *et al*., 2010a, b; Cheddad *et al*., 2010; Zaidan *et al*., 2010).

Digital watermarking ascertains no exclusion of or unchangeable watermark despite the fact of being bluntly evident (Stefan and Fabin, 2000). But Steganography, conversely, zooms in on

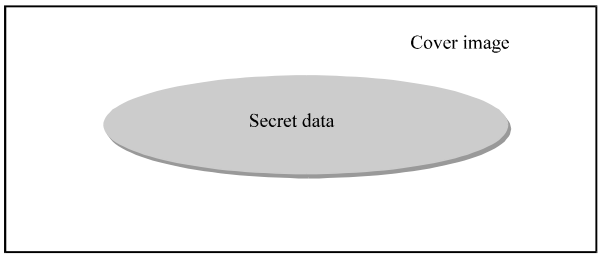

Fig. 1: Embedding process

masquerading secret information (Amirtharajan and Rayappan, 2012a-d). But it falls short if the secret content is exposed by the interloper (Padmaa *et al*., 2011; Qin *et al*., 2010). The advancements in computer technology today have improved the electronic media such as text (Shirali-Shahreza and Shirali-Shahreza, 2008; Al-Azawi and Fadhil, 2010), image (Chan and Cheng, 2004; Thanikaiselvan *et al*., 2011; Rajagopalan *et al*., 2012; Janakiraman *et al*., 2012a, b), audio (Zhu *et al*., 2011) and video (Al-Frajat *et al*., 2010) used for the steganographic communication (Zanganeh and Ibrahim, 2011; Luo *et al*., 2008; Thenmozhi *et al*., 2012).

Image Steganography uses image as cover object by hiding the relevant information in the cover image so that avoiding the information to be exposed to an intruder (Stefan and Fabin, 2000; Amirtharajan and Rayappan, 2012a-d). Digital images are used as cover-images in steganography because of their higher propagation and higher degree of redundancy in steganography because of their higher propagation and higher degree of redundancy. Steganography possesses two vital imputes, namely, payload and sensitivity. Steganography utilizes human insight as human wits are not taught to search for records having veiled information. Therefore, steganography conceals data from hackers. Payload is the amount of the secret information a cover image has (Amirtharajan and Rayappan, 2012a-d).

At the transmitter end, the secret message is embedded into the cover image as shown in Fig. 1. At the receiver end, the stego image is extracted to get the original secret message. Fundamental principle of Steganography is to maneuver the cover file's pixels and their corresponding values in succession, thus turning it to a code which is helpful in rebuilding the message while retrieving. This study tries to study the performances of 3 such suggested methods from Amirtharajan *et al*. (2012).

PROPOSED METHODOLOGY

In this study, three different embedding techniques such as k-bit embedding with a key, embedding based on Fibonacci series, embedding secret text encoded by Shannon-Fano encoding technique are implemented for information hiding. The MSE and PSNR for the above three methods have been calculated and tabulated. The pros and cons of the methods are also discussed in this study. Block diagram of this proposed technique is shown in Fig. 2.

Algorithm for k bit embedding with a key

1. Convert the secret text into binary form and name it as secret binary.
2. Convert the key value into binary form and name it as key binary.
3. For each pixel in cover image do the following
   - Loop(I = 1 to I = 4)
     - If (Ith LSB of key binary = 1) embed secret binary bit in Ith LSB of cover pixel
4. Store the resulting image as stego image.

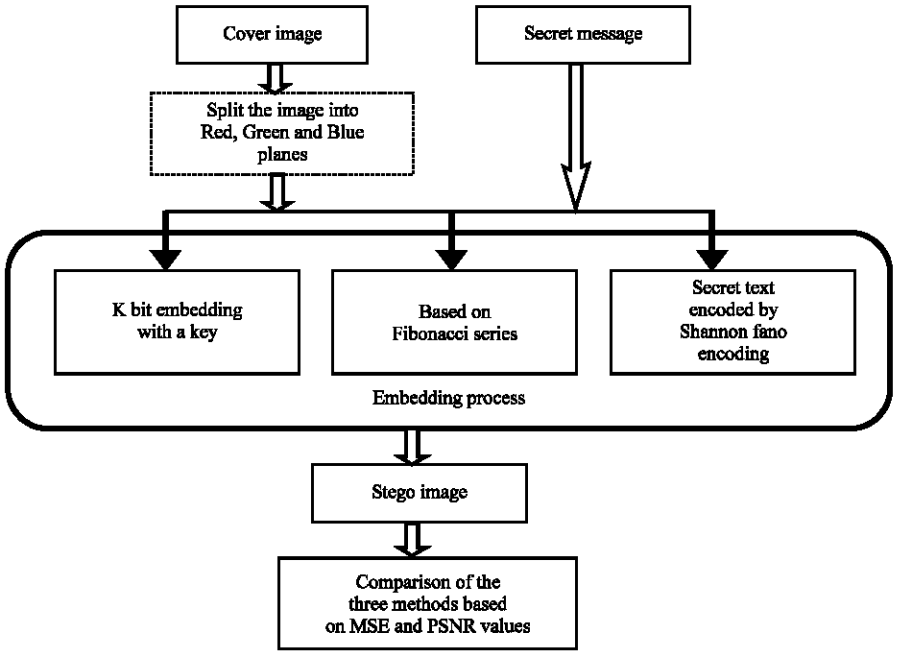

Fig. 2: Block diagram of proposed technique

Figure 3 represents the flow chart for k-bit embedding with a key.

Algorithm for embedding based on Fibonacci series

Input: Cover image, Message.

Output: Stego image

1. Split the cover image into Red, Green and Blue planes.
2. Generate the Fibonacci series up to the total number of pixels.
3. For each row in the image,
   - If row number matches with the Fibonacci series
     - For each column in the current row call k-bit embedding in all planes of the current pixel.
   - Go to the next row.
4. Store the resultant image as the stego-image

Figure 4 gives the flow chart for embedding based on Fibonacci series.

Algorithm for embedding secret text encoded by Shannon fano encoding technique

Input: Cover image, Message.

Output: Stego image

Split the cover image into Red, Green and Blue planes

1. Convert the secret image into Shannon-Fano encoding format
2. For each pixel in the cover-image,
   - Call k-bit embedding in all planes of current pixel.
3. Store the resultant image as stego image.

Figure 5 represents the Flow chart for embedding secret text encoded by Shannon-Fano encoding technique.

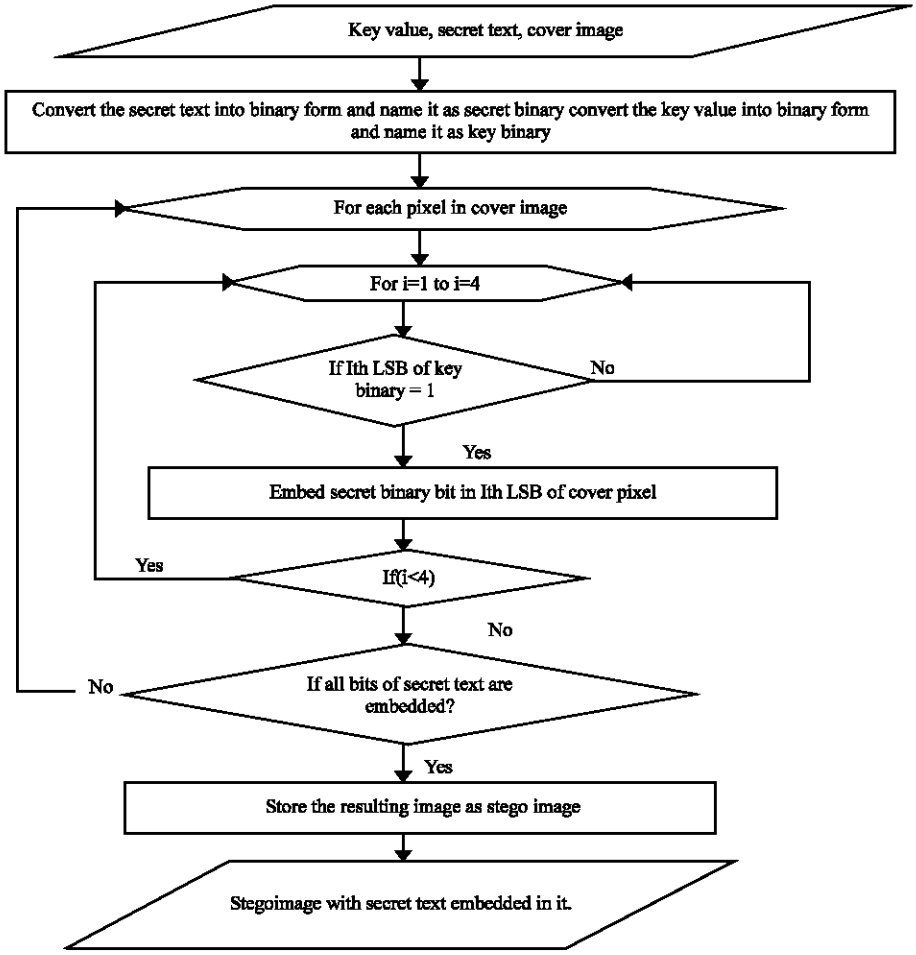

Fig. 3: Flow chart for k-bit embedding with a key

RESULTS AND DISCUSSION

To evaluate the performance of the implemented methods several experiments have been conducted, two image quality metrics are analysed are as follows. The MSE and PSNR values calculated for the proposed techniques are shown in the Table 1.

MSE: Mean square error this measures the signal to noise ratio. It is calculated from finding difference of intensities between cover image and stego image:

$$MSE = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}(X_{i,j} - Y_{i,j})^2$$

Where:

M = No. of rows in the image
N = No. of columns in the image
$X_{i,j}$, $Y_{i,j}$ = Pixel intensity of the stego imagecover image

PSNR: Peak signal to noise ratio is calculated by finding the ratio between the maximum intensity and the distortion in the image after embedding:

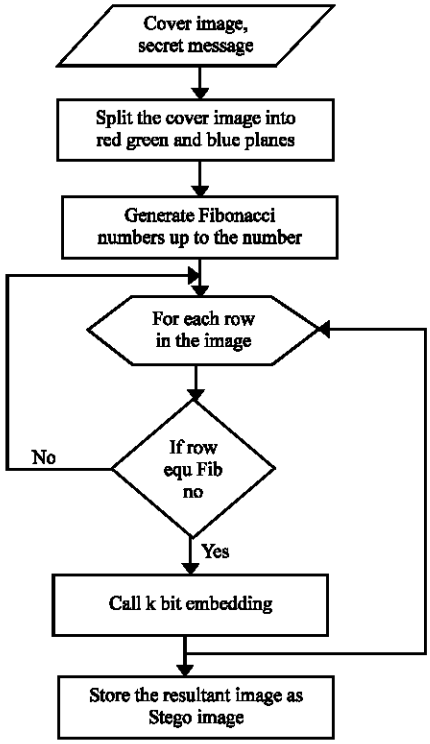

Fig. 4: Flow chart for embedding based on Fibonacci series

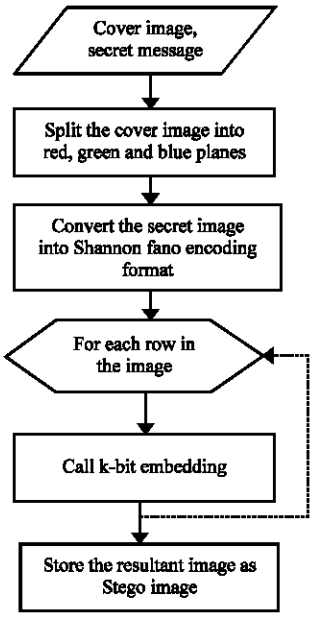

Fig. 5: Flow chart for embedding secret text encoded by Shannon-Fano encoding technique

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

where, I_{max} is maximum intensity of the image.

As given in the table, rose image (cover image) of dimension 250×250 having the size of about 1.09 KB is taken for the execution of all the three methods. The MSE and PSNR values for individual plane for all the three methods are charted. For Fibonacci and Shanon Fano methods, the red plane has higher PSNR than blue and green. If judged against these two, the latter bids added imperceptibility than the former. It escapes human suspicion. Needless to mention here is the fact that in the first method entrenching takes place for chosen pixels only whereas in the second one, it is done for the entire pixels. In the K-bit embedding proposal, embedding is done by shifting the key values ranging from 2 to 14, whose MSE values face ups and downs in all the planes. As it is vivid, key value 2 tenders high imperceptibility of 58 dB than the rest which designates that it is fairly a high quality image.

The original covers and their resultant stego are given in Fig. 6a, b, 7a, b and 8a, b, respectively for three methods. They have high degree of similarity which makes their

Table 1: Comparison table of three methods

				MSE			PSNR		
Algorithm name	Pay load size	Cover image	Embedding type	Red	Green	Blue	Red	Green	Blue
Fibonacci	1.09 KB	250×250	K Bit in all planes (RGB order)for selected pixels	0.06163	0.062352	0.0644	60.2327	60.1822	60.04
Shanon Fano	1.09 KB	250×250	K bit in all planes (RGB order)for all pixels	0.03921	0.039584	0.0401	62.1961	62.1556	62.09
K bit embedding with key value	1.09 KB	250×250	Key value = 2	0.09945	0.097536	0.0968	58.1544	58.2391	58.26
			Key value = 4	0.40190	0.039010	0.3886	52.0890	52.2185	52.23
			Key value = 5	0.23083	0.213700	0.2199	54.4970	54.8308	54.70
			Key value = 6	0.27987	0.257856	0.2512	53.6612	54.0170	54.13
			Key value = 8	1.62300	1.509376	1.60460	46.0275	46.3428	46.07
			Key value = 9	0.91025	0.835488	0.88353	48.5391	48.9114	48.66
			Key value = 10	0.98028	0.892224	0.93190	48.2172	48.6262	48.43
			Key value = 11	0.67192	0.590288	0.63328	49.8576	50.4201	50.11
			Key value = 12	1.23238	1.012480	1.08211	47.2233	48.0769	47.78
			Key value = 13	0.87704	0.705488	0.77036	48.7006	49.5459	49.26
			Key value = 14	0.94003	0.746560	0.81529	48.3993	49.4001	49.01

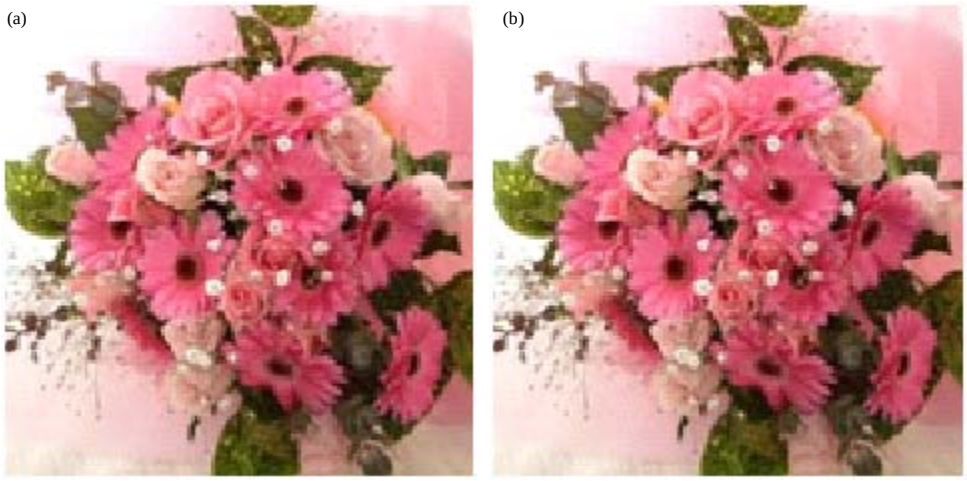

Fig. 6(a-b): Results for k-bit embedding for key value = 14 (a) Cover image and (b) Stego image

Fig.7(a-b): Results for embedding based on Fibonacci series, (a) Cover image and (b) Stego image

Fig. 8(a-b): Results for embedding secret text encoded by Shannon-Fano encoding technique, (a) Cover image and (b) Stego image

characterization pretty hard. The fact of identification of secret data remains quite difficult. As a final point, this construct is capable of accomplishing soaring rate of capability, refuge and stoutness.

CONCLUSION

This study, rooted in K-bit embedding, Fibonacci series and Shannon-Fano encoding method projects a data masking algorithm apt for elevated privacy, capacity. By defining the strictures of selection or amount of pixels and key values, data is implanted adaptively as said by the algorithm. In this fashion, it circumvents huge deformation and can push in extra surreptitious data. This upshot offers the leeway of safe and sound conduction of desired information through computer.

Tentative results prove that this anticipated scheme validates the conclusion and without doubt surpasses the former plots. Hence, this method is a viable means for covert communication.

REFERENCES

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. Inform. 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. Inform. 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. Inform. Technol., 4: 124-139.

Amirtharajan, R., J. Qin and J.B.B. Rayappan, 2012. Random image steganography and steganalysis: Present status and future directions. Inform. 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.

Bender, W., W. Butera, D. Gruhl, R. Hwang, F.J. Paiz and S. Pogreb, 2000. Applications for data hiding. IBM Syst. J., 39: 547-568.

Chan, C.K. and L.M. Cheng, 2004. Hiding data in images by simple LSB substitution. J. Pattern Recognit. Soc., 37: 469-474.

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.

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. Inform. 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. Inform. Technol. J., 11: 9-19.

Kahn, D., 1983. The Codebreakers: The Story of Secret Writing. Macmillan, New York.

Luo, G., X. Sun and L. Xiang, 2008. Multi-blogs steganographic algorithm based on directed hamiltonian path selection. Inform. Technol. J., 7: 450-457.

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

Qin, J., X. Xiang and M.X. Wang, 2010. A review on detection of LSB matching steganography. Inform. 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.

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

Shirali-Shahreza, M. and S. Shirali-Shahreza, 2008. High capacity persian/arabic text steganography. J. Applied Sci., 8: 4173-4179.

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 Inform. 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. Inform. Technol., 4: 31-46.

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. Inform. Technol. J., 10: 1285-1294.

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