Research Journal of Information Technology

ISSN 1815-7432

Academic Journals Inc.

www.academicjournals.com

Research Journal of Information Technology 5 (2): 234-241, 2013
ISSN 1815-7432 / DOI: 10.3923/rjit.2013.234.241

Compressed and Encrypted Secret Hides in Image for Rugged Stego

Rengarajan Amirtharajan, J.H.S. Karthikesh, M. Nirup Reddy, Ch. Sri Harsha Kaushik and J.B.B. Rayappan
School of Electrical and Electronics Engineering, SASTRA University, Thanjavur, 613 401, India

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

ABSTRACT

This study projects a unique means of steganography incorporating two diverse plots for images viz., compression and encryption. Being indispensable for the sake of e-world, where images are numerously involved information security has caught attention of many. In this heterogeneous distributed computing world data are transferred accurately and faster. Many transmission mediums are available to send the data through internet. The main concern of the data transfer is to secure the data without any unauthorized access. To have a secured data transfer steganography and cryptography methods are involved. Cryptography scrambles the data whereas steganography conceals the data transfer. In this proposed method secret text is compressed using Shannon fano method and then encrypted using rail fence cipher followed by ceaser cipher to improve the security. Mean Squared Error (MSE) and Peak Signal-to-Noise Ratio (PSNR) are calculated and analysis is done. K-bit embedding is employed in this study to put the secret out of sight. This study pledges security, embedding capability and imperceptibility possessing high hardiness to security threats.

Key words: Cryptography, information hiding, shannon-fano encoding, image steganography

INTRODUCTION

In the current fashions of the world, everybody transfers data from one to another end in this world through internet. One of the important anxieties of the internet is the security hazard. To prevent the confidential data from malicious user various security methods like cryptography (Salem *et al*., 2011; Schneier, 2007), steganography and watermarking (Abdulfetah *et al*., 2010; Zeki *et al*., 2011) are developed (Stefan and Fabin, 2000; Rajagopalan *et al*., 2012). Cryptography encrypts the covert data thus generates cipher text and then transmits to the destination with unfamiliar key. Steganography goes one step further by disguising it in any communication media (Bender *et al*., 1996) like text (Xiang *et al*., 2011), images (Cheddad *et al*., 2010; Chan and Cheng, 2004; Luo *et al*., 2011; Mohammad *et al*., 2011; Zhao and Luo, 2012), audio (Zhu *et al*., 2011), video (Al-Frajat *et al*., 2010).

The digital Steganography involved a carrier medium "Cover" such as a document, audio (Zhu *et al*., 2011) or an image which supported fractionation. The data to be embedded was the secret message and the medium after the embedment "the stego image" (Amirtharajan and Rayappan, 2012a-d; Amirtharajan *et al*., 2012). The choice of the algorithm is driven by parameters such as Integrity, robustness, capacity and availability (Hmood *et al*., 2010a, b). The

other factor that drives the choice of algorithm is the domain in which the data is encoded i.e. spatial domain (Amirtharajan and Rayappan, 2012a, c; Thanikaiselvan *et al*., 2011) and frequency domain (Amirtharajan and Rayappan, 2012d).

In this day and age Steganography finds its applications in diverse fields (Janakiraman *et al*., 2012a, b; Thenmozhi *et al*., 2012). To quote few, in photography, aperture size, shuttle speed and other settings may be embedded in the picture itself for future references without degrading the fidelity of the image (Cheddad *et al*., 2010). Another scenario is the case in which a person would want to keep a file containing private information unknown to anyone (Stefan and Fabin, 2000). This technique can also be used to embed patient information within the medical imagery. Despite these many friendly applications, steganography may be outrageously used in spying and evil plots by terrorists. Consequently, it has gained a great deal of attention from political and academic institutes (Amirtharajan and Rayappan, 2012a, d; Amirtharajan *et al*., 2012).

Steganography owns a number of benefits for instance; only experts can study and analyze the digital files, abundance of images and patterns for use etc. One of the main boons is it stands all sorts of digital files which are very common in commercial and non-commercial ventures. Thus researches are rapidly increasing in this enchanting domain making it so vast to unearth new concepts and methodologies of diverse origin and its counter attack called steganalysis (Qin *et al*., 2010).

This study is a valuable means of image steganography wherein both cryptographic and steganographic security is guaranteed. This plot takes image compression and encryption as backbone and the result (preprocessed image) submits itself to steganography all the way through K-bit embedding. Thus, this combo offers additional security to images-with-secret being transferred.

LITERATURE REVIEW

Information hiding techniques are classified as irreversible (Amirtharajan and Rayappan, 2012a, d; Amirtharajan *et al*., 2012) and reversible methods (Zhao and Luo, 2012). In irreversible data hiding receiver can get only the surreptitious message from its stego output (Zanganeh and Ibrahim, 2011). But in the second method receiver can revive both the cover and secret information without any distortion. Irreversible data hiding method offers remarkable hiding competence and visual quality but recovery of cover image is not possible. Reversible methodologies find application in communicating sore information for instance of medicinal and military origin. The execution of two-sided entrenching algorithm is appraised via the extent of payload capability, visioning quality on the stego image, complexity of the algorithm (Padmaa *et al*., 2011). The different types of reversible steganography may be mentioned as pure, public and secret key (Stefan and Fabin, 2000).

Pure steganography: Pure steganographic routine embeds the data in to the cover image without using private keys. This type of steganography doesn't provide the better security because it is easy for extracting the message if the unauthorized `person becomes aware of the rooting procedure.

Secret key steganography: It is another process of steganography is similar to symmetric key algorithm. It uses the same key for embedding the data into cover in addition to extract data from it.

Public key steganography: This type of steganography uses two unlike keys one to encrypt and another key to decrypt. The key used for encryption is a private key and public key be in support of decryption.

For both encrypting and decrypting text messages using the secret keys, steganographic system uses algorithms known as steganographic algorithms. The mostly used algorithms for embedding data into images are:

- LSB (Least Significant Bit)
- JSteg algorithm
- F5 algorithm

LSB algorithm: LSB substitution aligns the cover pixels' least significant bits (Chan and Cheng, 2004). This is one simpleton practice for infixing message into the image. Within images, modification of bits in the last four LSB's won't cause any change for human's eye perceptibility. The four LSB inclusions change as per the bits contained in the image. For 8 bit images, the 8th bit in every byte is altered to that of the secret. For 24 bit images, the colors in all components like RGB are changed. LSB sounds good for BMP image formats as they endure lossless compression. However, one should use an outsized image as carrier.

JSteg algorithm: This steganographic technique is used for embedding data into JPEG images. The hiding process will be done by replacing Least Significant Bits (LSB). Jsteg modus operandi supersedes LSBs belonging to quantized Discrete Cosine Transform (DCT). In this process the hiding means bounds off the entire coefficients having values of 0 or else 1. This algorithm is resistant to visual attacks and proffers venerable capacity. By and large, Jsteg means buries the covert message within images of lossy compression. This work delivers high capacity and compression ratio of 12%. JSteg algorithm is restricted for visual attacks and it is less immune for statistical attacks. Normally, JSteg embeds only in JPEG images (Zhang *et al*., 2009).

F5 algorithm: Westfeld (2001) introduced F5 run with the intention of avoiding the security problem when embedding the data into the JPEG images. It engrafts the secret information in stochastically selected coefficients of Discrete Cosine Transform. It utilizes matrix to implant which reduces the alterations to be made to the length of certain message. The F5 Algorithm provides high steganographic capacity and can prevent visual attacks. F5 algorithm is also resistant to statistical attacks. This algorithm uses matrix encoding such that it reduces the modification needed to root data of definite extent. It also prevents chi-square test as there is no swapping or proxy of bits. This kind of confrontation is soaring for arithmetical and visual assaults. F5 has eminent embedding capability (above 13%) supporting various image formats. Its recital diverges as per data source and cover file.

PROPOSED METHODOLOGY

In this study, a data hiding technique had been proposed to enhance the secrecy of the data with encryption and compression. Secret data was compressed with shanon-fano encoding technique and encrypted using the rail fence cipher followed by ceaser cipher. The encrypted secret was embedded in cover image with the help of key based embedding method. The block diagram of this study is shown in Fig. 1. Observational results of images for this scheme and that of the LSB method are revealed in Fig. 2-4.

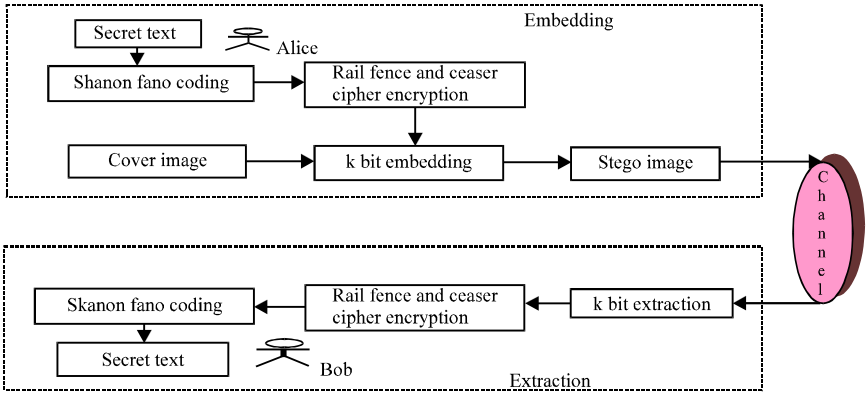

Fig. 1: Block diagram for proposed system

Algorithm for embedding

Input: Cover image(C), Secret text(S), key

Output: Stego image(O).

- Split the cover image into Red, Green and Blue planes
- Apply shanon fano encoding method for the plain text
- Convert the compressed text in to cipher text (CT) using rail fence cipher algorithm and ceaser cipher algorithm
- Get the key value and store it in k
- Convert k in binary form
- Find the position of one's in the key in LSB of the k
- For each pixel in the cover image do the following
- Embed the cipher text in the LSB according to the position of one's in the key in R, G and B planes
- Store resulting output as Stego image
- Calculate the MSE and PSNR for all the planes

Algorithm for rail fence cipher

Input: Secret text, k

Output: Cipher text

- For each character in the secret text do the following
- For each column in the two dimensional array
  - Store the character row wise starting from 1 to k.
  - Go to the next column.
- Read the character from the array row wise and store in cipher text.

Algorithm for recovery

Input: Stego image(O), Key

Output: Cover image(C), Secret text

- Split the image into Red, Green and Blue planes
- Using K bit extraction algorithm, retrieve the cover image and the encrypted data
- Using rail fence and Ceaser cipher algorithm, the data is decrypted
- Shannon Fano encoding method is used to decompress the data to get the secret text

RESULTS AND DISCUSSION

The algorithm is modeled in MATLAB 7.1 with Lena, Flower and Temple as the cover images. The observed results are tabled and compared with simple LSB method. From the table, it is noticed that Flower image has higher PSNR value of 62.34dB, which is much above 33 dB, fair

Fig. 2(a-c): Flower image (a) Cover image (b) Stego image for proposed method and (c) Stego for LSB

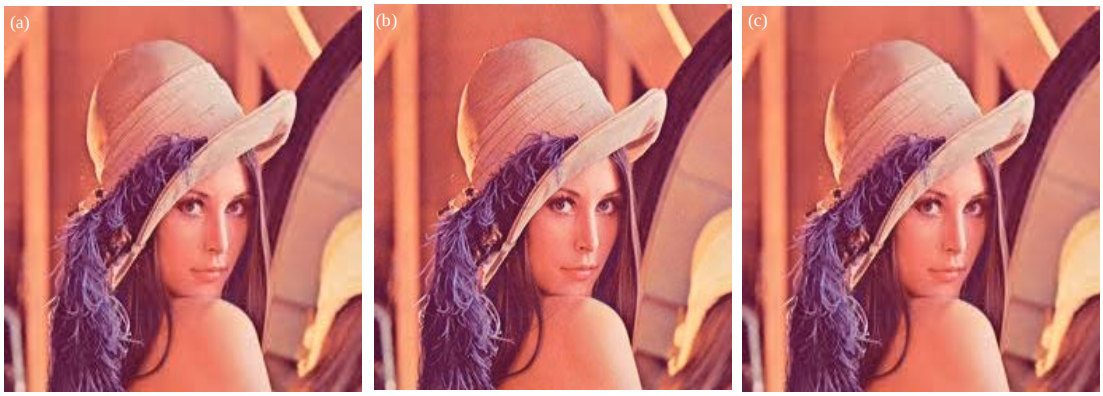

Fig. 3(a-c): Lena image (a) Cover image (b) Stego image for proposed method and (c) Stego for LSB

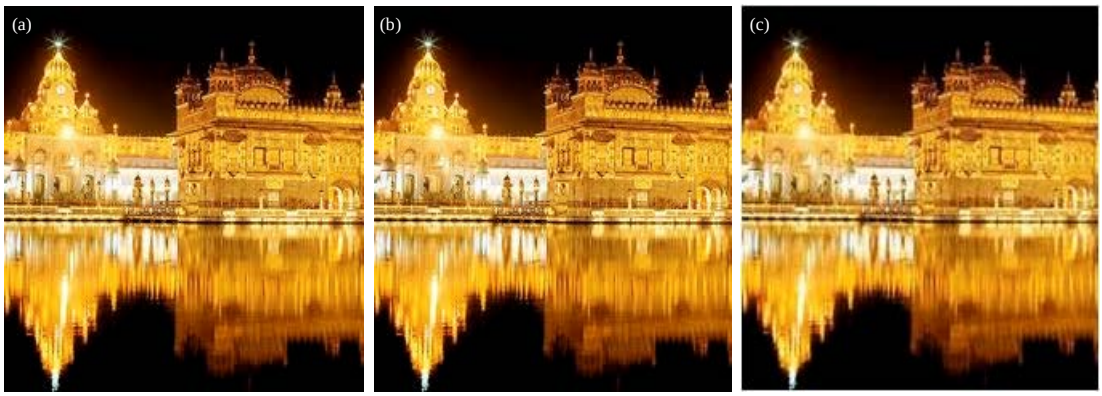

Fig. 4(a-c): Temple image (a) Cover image (b) Stego image for proposed method and (c) Stego image for LSB

value of imperceptibility. Thus all the three images exhibit good imperceptibility. In simple LSB substitution also, Flower image has high PSNR; but the proposed method has more of its nature. Image parameters are expressed as:

Table 1: MSE, PSNR values for proposed method and simple LSB method

		Proposed method						LSB method					
		Channel 1 red		Channel 2 green		Channel 3 blue		Channel 1 red		Channel 2 green		Channel 3 blue	
Cover image	Payload	MSE	PSNR	MSE	PSNR	MSE	PSNR	MSE	PSNR	MSE	PSNR	MSE	PSNR
Lena	110KB	0.1230	57.2309	0.1242	57.1865	0.1174	57.4307	0.1670	55.9049	0.1664	55.9200	0.1661	55.9276
Flower	110KB	0.0379	62.3444	0.0384	62.2846	0.0401	62.0912	0.1611	56.0591	0.1650	55.9558	0.1658	55.9354
Temple	110KB	0.1658	55.9324	0.1712	55.7948	0.1754	55.6889	0.1679	55.8802	0.1658	55.9350	0.1651	55.9529

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

where, $C_{i,j}$ is the original image and $O_{i,j}$ is the stego image:

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

where, I_{max} is the 255 for colour image.

Analytical results of this study for the three images and its comparison with the existing LSB method is given in Table 1. As far as Temple image is concerned, the PSNR value differs by a considerable margin thus increases the importance of the suggested routine. This is, of course, likely the case for Lena image too. From planes' point of view, in simple LSB Blue offers rich characteristics while Red plane takes the credit in proposed method. Moreover, steganalysis is an incubus task since unless and until one knows about the maneuver of compression and encryption. But which is in this case is a baffling one. Needless to mention here is the difficulty and refuge the paper offers thus making it skillful in all bounds of steganography.

CONCLUSION

With the fruition in technology in various bailiwicks people are heading towards up-to-the-minute platform in all the things which indeed has come up with out of the question security issues. Since all sorts of image processing are now being practiced widely, plentiful offenses have also been witnessed. This is where cryptography and steganography come into play. Both being antediluvian, their electronic versions are now being employed extensively in communicating cloistered information. This study paints one more picture in image steganography by meshing two broad knowledge bases namely compression and encryption. Both cryptographic and steganographic security is guaranteed and is justified by the tentative results. Moreover, stego images also leave no trace to hunch. Thus, this study is determined to be good when compared with simple LSB substitution and brags about its commercial effectuation.

REFERENCES

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

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.

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.

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

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

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.

Salem, Y., M. Abomhara, O.O. Khalifa, A.A. Zaidan and B.B. Zaidan, 2011. A review on multimedia communications cryptography. Res. J. Inform. 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 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.

Westfeld, A., 2001. F5 a steganographic algorithm: High capacity despite better steganalysis. Proceedings of the 4th Information Hiding Workshop, Apr. 25-27, Springer-Verlag, Pittsburgh, PA, USA, pp: 289-302.

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

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.

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

Zhang, Q., Y. Liu, S. Zhang and K. Chen, 2009. Classification method of Jsteg stego-images and F5 stego-images. Proceedings of the 4th International Conference on Innovative Computing, Information and Control, December 7-9, 2009, Kaohsiung, pp: 394-397.

Zhao, Z. and H. Luo, 2012. Reversible data hiding based on Hilbert curve scan and histogram modification. Inform. 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. Inform. Technol. J., 10: 1983-1988.