Research Journal of Information Technology

ISSN 1815-7432

Academic Journals Inc.

www.academicjournals.com

Research Journal of Information Technology 5 (2): 249-255, 2013
ISSN 1815-7432 / DOI: 10.3923/rjit.2013.249.255

Image Hides Image: A Secret Stego Tri-layer Approach

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

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

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

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

ABSTRACT

In this pervasive world, we can access anything from anywhere. To have a secret communication, we need a technology such that no one is able to read or modify the secret message. The message should be sent without any intrusion by eavesdroppers. The secret message could be encrypted using cryptography and communicated. But a third party might suspect the presence of the secret message in this case. So, in order to hide the presence of the secret message, steganography is employed. Human eyes are imperceptible to the LSB changes in images and thus messages could be hidden in them. Image steganography will be powerful if there is not a proper sequence in the changes done to the pixels. In this proposed methodology, the secret logo is embedded in an image resulting in the stego-image 1. This is embedded in one more image resulting in stego image 2 which is again embedded in one more image to achieve 3rd level security. To get the secret logo we need to do the same process in the reverse manner. MSE and PSNR are calculated for the proposed method all levels.

Key words: Information hiding, steganography, novel cover generation methods

INTRODUCTION

Information hiding is an important technique to secure the precious data during communication (Amirtharajan and Balaguru, 2009; Amirtharajan *et al*., 2011; Amirtharajan and Rayappan, 2012a, b). Information has to be secured in a sky-scraping manner and communicated in such a way that no one can predict and corrupt the message. As a defense to protect their data against their enemies, information hiding plays a vital role (Stefan and Fabin, 2000). A person who wants to share a secret with others needs the art of steganography to have a secure communication.

In olden days, people used invisible inks, puts tattoos on shaved heads, used wax for covering words on wooden tablets and newspaper clippings. Steganography is used these days to secure data against malicious users (Padmaa *et al*., 2011) obliterating the secret content along with its being (Rajagopalan *et al*., 2012). In this field, different carriers are used to carry the secret message such as text, images, movies and protocols (Zhu *et al*., 2011; Zaidan *et al*., 2010; Hmood *et al*., 2010a, b). Thus the saying 'a picture speaks more than thousands of words' would be apt here. In nature, the fruit hides a seed. Here image is used as a fruit and seed is the text message. The chief requirements of Information hiding are capacity and imperceptibility. Imperceptibility is an inherent quality of image (Zanganeh and Ibrahim, 2011) steganography wherein the message is embedded in the cover in such a manner that both the cover and the stego-image are hard to

distinguish by the human eyes. But cryptography tries to scramble it (Rajagopalan *et al*., 2012; Schneier, 2007; Zaidan *et al*., 2010). Hiding capacity is another important requirement by which a significant number of bits have to be embedded without affecting the imperceptibility (Thanikaiselvan *et al*., 2011a, b; Thenmozhi *et al*., 2012). Images are the widely used medium in World Wide Web with the advantage of limited perception of colors.

In this study, security is largely taken good care of in conjunction with the other steganographic imputes. The primary intent of this work is to accomplish an outflanked steganographic model intended for unavowed sharing. All this model employs is K-bit embedding proficiency in all the three steps yielding difficult-to-differentiate image results ascertaining imperceptibility, confidentiality and lustiness.

RELATED WORK

Digital images are made up of pixels. The popular method of hiding in images is to insert the binary encoded data in the Least Significant Bits of the image pixels (Cheddad *et al*., 2010). Image distortion is minimal in the LSB insertion technique in which the LSB of the image pixel is replaced by the message's bit. For example if we choose the last LSB to embed then 3 bits of the message are stored in the LSB's of the Red, Green and Blue planes respectively. The resulting stego-image will be identical to the original image for the human vision (Amirtharajan and Rayappan, 2012c, d; Cheddad *et al*., 2010). In the randomized method, instead of embedding the message bits in a sequential manner, the bits are stored in random. Pseudo random number generator is used to generate the index of the pixel where the message bits are going to be embedded (Janakiraman *et al*., 2012a, b). In the block-matching procedure, the cover image with the highest similarity is searched for each block of the secret image and embedded in the LSBs of similar blocks (Amirtharajan and Rayappan, 2012a, b). A different method of steganography is proposed by mapping the pixels of the image to English letters and special characters. More surveys on steganography are available by Rajagopalan *et al*. (2012), Thenmozhi *et al*. (2012) and Cheddad *et al*. (2010) for detailed technical descriptions.

PROPOSED METHOD

In this proposed methodology, three level image hiding has been used. In the first level the secret logo embedded in the cover-image1 produces the stego-image 1. In the second level, the stego-image 1 is then embedded in another image to produce stego-image 2. In the third level the stego-image 2 is embedded in another image to give the final stego-image. The block diagrams for embedding and extracting the secret logo are given in Fig. 1 and 2, respectively.

Algorithm for level 1:

Inputs: Secret Logo, Cover Image1

Output: Stego image1 with secret logo embedded in it

- Convert the Secret logo into binary form
- Split the cover image1 C into R, G and B
- For each pixel in Secret Logo, do the following
  - Let b [6] = 2nd MSB of the current pixel of R
  - Let b [5] = 3rd MSB of the of R
  - Let b [4] = 4th MSB of the of R

Algorithm for level 1: Continue

- Let k = (number of 1s in MSB of R, G and B)+1
- If b = 000 then

Go to next pixel.

Else if b = 001 then

k-bit Embedding current pixel of B

Else if b = 010 then

k-bit Embedding current pixel of G

Else if b = 011 then

k-bit Embedding current pixel of G and B

Else if b = 100 then

k-bit Embedding current pixel of R

Else if b = 101 then

k-bit Embedding current pixel of R and B

Else if b = 110 then

k-bit Embedding current pixel of R and G

Else if b = 111 then

k-bit Embedding current pixel of all the R, G and B

- Store the resulting image as Stegoimage 1

Algorithm for level 2:

Input: Stego image1,Cover image2

Output: Stego image2 with Stego image1 embedded in it

- Split the cover image2 into Red, Green and Blue planes set k value as 3 and flag as 0
- For each pixel in coverimage2 do the following steps
  - if(flag = = 0) Call k-bit embedding in the current pixel of Red and Green planes and set flag as 1 .skip to step 3
  - if(flag = = 1) Call k-bit embedding in the current pixel of Green and Blue planes and set flag as2 skip to step 3
  - if(flag = = 2)Call k-bit embedding in the current pixel of Blue and Red planes and set flag as 0 skip to step
  - If all pixels of stego image1 is embedded then skip to step 4 otherwise move to the next pixel.
- Store the resulting image in stego image2

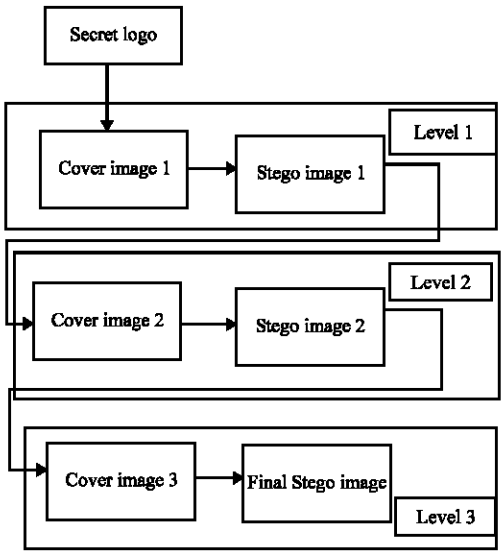

Fig. 1: Block diagram for embedding the secret logo

Algorithm for level 3:

Input: Stego image2, Cover image3

Output: Stego image3 with Stego image2 embedded in it

Split the cover image3 into Red, Green and Blue planes and set flag as 0 and k as 2

- For each pixel in cover image3 do the following steps
- if(flag = = 0) Call k-bit embedding in the current pixel of Red, Green and Blue planes and set flag as 1,skip to step 4
  - if(flag = = 1) Call k-bit embedding in the current pixel of Green, Blue and Red planes and set flag as2,skip to step 4
  - if(flag = = 2) Call k-bit embedding in the current pixel of Blue, Red and green planes and set flag as 0, skip to step 4
  - If all pixels of stego image1 are embedded

  skip to step 4; otherwise move to the next pixel
- Store the resulting image in final stego

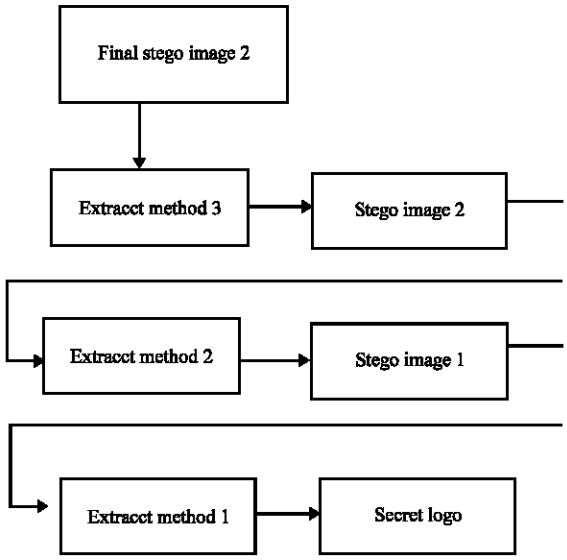

Fig. 2: Block diagram for extracting the secret logo

RESULTS AND DISCUSSION

In this study, hiding has been done by using three level hierarchy image hiding. The Secret logo has been embedded at last level to achieve high security. In each level a different algorithm has been used. The results are shown in Fig. 3-5. Figure 3 represents the result of First Level embedding. Figure 4 represents the results of Second Level Embedding and Fig. 5 represents the result of Third Level Embedding. The implementation has been simulated by using Java (jdk1.6). The calculated Mean Square Error (MSE), Peak Signal to Noise Ratio (PSNR) readings for two sample input is tabulated in Table 1 and 2.

Three level hierarchy image hiding: If one level embedding is used to hide secret logo then it gives less complexity and if the level is increased then the complexity is also increased proportionally.

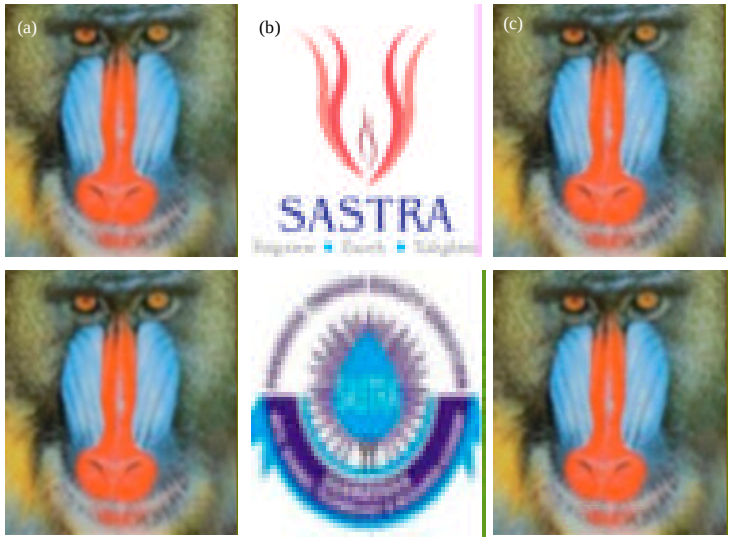

Fig. 3(a-c): First level embedding, (a) Cover image 1 (175×175), (b) Secret logol 1 (60×61) and (c) Stego image 1 (175×175)

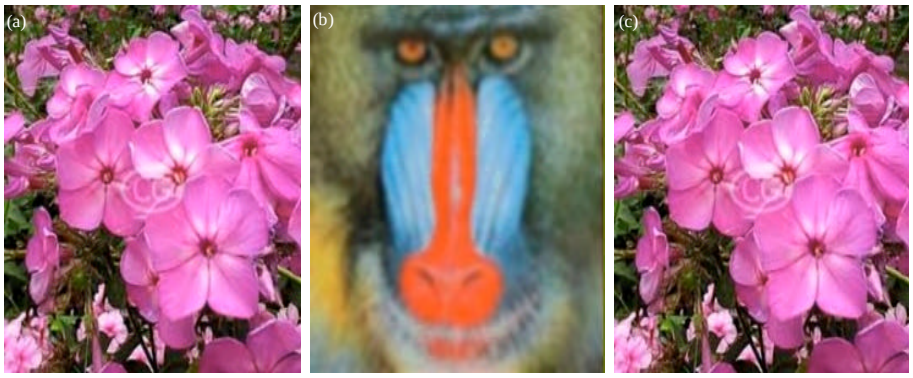

Fig. 4(a-c): Second level embedding, (a) Cover image 2 (175×175), (b) Secret logol 2 (63×59) and (c) Stego image 2 (175×175)

Fig. 5(a-c): Third level embedding, (a) Cover image 2 (350×350), (b) Secret image 1 (175×175) and (c) Stego image 2 (350×350)

Table 1: Sample input 1-Secretlogol

	Cover image 1 (at level 1)	Cover image 2 (at level 2)	Cover image 3 (At level 3)
MSE			
Red	2.513	6.850	2.481
Green	4.424	6.770	2.493
Blue	6.621	6.820	2.475
PSNR			
Red	44.128	39.773	44.184
Green	41.672	39.824	44.163
Blue	39.921	39.792	44.195

Table 2: Sample input II-Secretlogo 2

	Cover image 1 (at level 1)	Cover image 2 (at level 2)	Cover image 3 (at level 3)
MSE			
Red	1.911	6.812	2.473
Green	4.007	6.718	2.498
Blue	5.316	6.7501	2.475
PSNR			
Red	45.318	39.798	44.198
Green	42.102	39.858	44.154
Blue	40.874	39.837	44.195

CONCLUSION

In the digital era, we live in, information transmission happens in milli seconds while infiltrating happens in nano seconds. Because of this, the integrity of the information is not maintained. Certain information like the high secrets of the army if infiltrated like this would cause destruction and loss on a large scale. Cryptography and steganography are ways of encrypting and hiding data. This proposed method has triple layer protection. If the secret image adapt some existing cryptographic techniques along with this steganographic technique then its hard for hackers to decrypt it.

REFERENCES

Amirtharajan, R. and R.J.B. Balaguru, 2009. Tri-layer stego for enhanced security-a keyless random approach. Proceedings of the IEEE International Conference on Internet Multimedia Services Architecture and Applications, December 9-11, 2009, Bangalore, India, pp: 1-6.

Amirtharajan, R., R.R. Subrahmanyam, P.J.S. Prabhakar, R. Kavitha and J.B.B. Rayappan, 2011. MSB over hides LSB: A dark communication with integrity. Proceedings of the IEEE 5th International Conference on Internet Multimedia Systems Architecture and Application, December 12-14, 2011, Bangalore, Karnataka, India pp: 1-6.

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.

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.

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

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.

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

Thanikaiselvan, V., P. Arulmozhivarman, R. Amirtharajan and J.B.B. Rayappan, 2011a. Wave (let) decide choosy pixel embedding for stego. Proceedings of the International Conference on Computer, Communication and Electrical Technology, March 18-19, 2011, India, pp: 157-162.

Thanikaiselvan, V., S. Kumar, N. Neelima and R. Amirtharajan, 2011b. 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.