International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-8 Issue-1, November 2018

Secure LSB STEGO Image Transmission using Visual Cryptography and RSA Encryption

Polamarasetty Lavanya, Nihar Ranjan Panda, Y. P. M. Surya Kiran

Abstract: ***Real-time image and video Steganography applications usually belong to the range between soft and firm real-time applications. Secret Data embedding in image and video mediums introduce additional real-time requirements except the basic Steganography's. Multimedia is a common target for hiding and transmitting information. Specifically, the methods of audio hiding discussed until now include methods like LSB. This paper includes the proposal of specific case models such as Steganography of the total of Visual Cryptography schemes of black and white images. They provide security robustness and higher capacity, by definition, under the correct use.***

Keywords: Steganography, Specifically, Methods Like LSB, Cryptography Schemes of Black and White Images.

I. INTRODUCTION

The science which deals with the hidden communication is called Steganography. There are different kinds of stenographic techniques which are complex and which have strong and weak points in hiding the invisible information in various file formats. The innocent carriers are the possible cover carriers which will hold the hidden communication. A Steganography method is admirably secure only when the statistics of the cover information and the stego information are similar with each other. In other words it conveys the meaning that the relative entropy between the cover information and the stego information is zero. The LSB embedding technique suggests that data can be hidden in such a way that even the naked eye is unable to identify the hidden information in the LSBs of the cover file.

Steganography is an alternative method for privacy and security. Instead of encrypting, we can hide the messages in other innocuous looking medium (carrier) so that their existence is not revealed. Among the several advantages for employing the Steganography, secretly transmitting the secret information from source to destination is one. In this chapter, different approaches towards implementation of image Steganography have been thoroughly and clearly discussed. Among several techniques, Masking and Filtering, Algorithms and Transformations and LSB insertion are some of the methods to achieve Steganography. Among these techniques, LSB insertion is a very simple and commonly applied technique for embedding data in a cover file.

Manuscript published on 30 November 2018.
*Correspondence Author(s)
Polamarasetty Lavanya, M.Tech Student, Sanketika Vidya Parishad Engineering College, Visakhapatnam (Andhra Pradesh), India.
Nihar Ranjan Panda, Professor, Sanketika Vidya Parishad Engineering College, Visakhapatnam (Andhra Pradesh), India.
Y. P. M. Surya Kiran, Assistant Professor, Sanketika Vidya Parishad Engineering College, Visakhapatnam (Andhra Pradesh), India.

Steganography is a kind of technique which can embed a message inside a cover object. There are a number of features that characterizes the merits and demerits of the embedding techniques. The way they are applied decides the importance of each and every feature. A set of criteria are proposed to define the invisibility of an algorithm. The criteria are as follows:

- **Invisibility**

The imperceptibility of a Steganography technique is the most important necessity, since the quality of Steganography lies in its capacity to be unseen by the naked eyes.

- **Payload Capacity**

Steganography techniques used aim at hiding the embedded secret data and also maximize the amount of information embedded. The amount of information that is hidden is called payload capacity.

- **Hiding Capacity**

Concealing capacity is nothing but the size of data that could be concealed with respect to the size of the cover object. A vast concealing capacity permits the use of smaller cover images and thus decreases the data transmission needed to broadcast the stego image.

- **Perceptual Transparency**

The inability of an eavesdropper to detect hidden data is referred by Perceptual transparency.

For a 24-bit RGB image, every RGB component requires 8 bits of memory. The range of every RGB component value is in between 0 to 255 where 255 represent brightest shade of the color and 0 represents darkest shade of the color. All different colors could be produced with the combination of these ranges. Subsequently, the test image is represented by integer matrix. Every pixel is a mix of RGB values.

Fig a. Share Creation

Fig. b. 2 Combining the Shares

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

A. LSB

The easiest way to embed secret information within the cover file is called LSB insertion. In this technique, the binary representations of the secret data have been taken and the LSB of each byte is overwritten within the image. If 24-bit color images are used, then the quantity of modification will be small. As an example, supposing that we have three neighbouring pixels (nine bytes) with the following RGB encoding:

01101010	11110010	00110110
01101001	11110000	00110101
01100000	11101111	00110100

Now if we wish to embed the following 9 bits of compressed secret information:

010010011.

If we insert these 9 bits over the LSB of the 9 bytes above, we get the following sequence of bits (where bits in red color have been modified):

01101010	11110011	00110110
01101000	11110001	00110100
01100000	11101111	00110101

Note that we have successfully hidden 9 bits but at a cost of only modifying 5, or roughly 50% of the LSB bits.

B. RSA Algorithm

In Cryptography, RSAis an algorithm for public-key Cryptography. The RSA algorithm involves three steps: Key generation, encryption and decryption.

Key Generation: The keys for the RSA algorithm are generated in the following way:

Step-1: Choose two different random prime numbers p and q.

Step-2: Compute $n = p*q$.

$n$is used as the modulus for both the private and public keys.

Step-3: Compute $\varphi(n) = (p-1)(q-1)$. (φ is Euler's totient function).

Step-4: Choose an integer e such that $1 < e < \varphi(pq)$, andgcd (e, $\varphi(n)) = 1$

Step-5: Compute $d = e^{-1} \bmod [\varphi(n)]$

Step-6: Publish the public encryption key: (e; n)

Step-7: Keep secret private decryption key: (d; n)

Encryption:

The steps required to encrypt information at sender are as follows:

Step-1: Obtain public key of recipient (e; n)

Step-2: Represent the information as an integer m in [0, $n-1$]

Step-3: Compute $c = m^e \bmod n$

Decryption:

The steps required to decrypt information at receiver side are as follows:

Step-1: use private *key* (d; n)

Step-2: compute $m = c^d \bmod n$

II. RESULTS

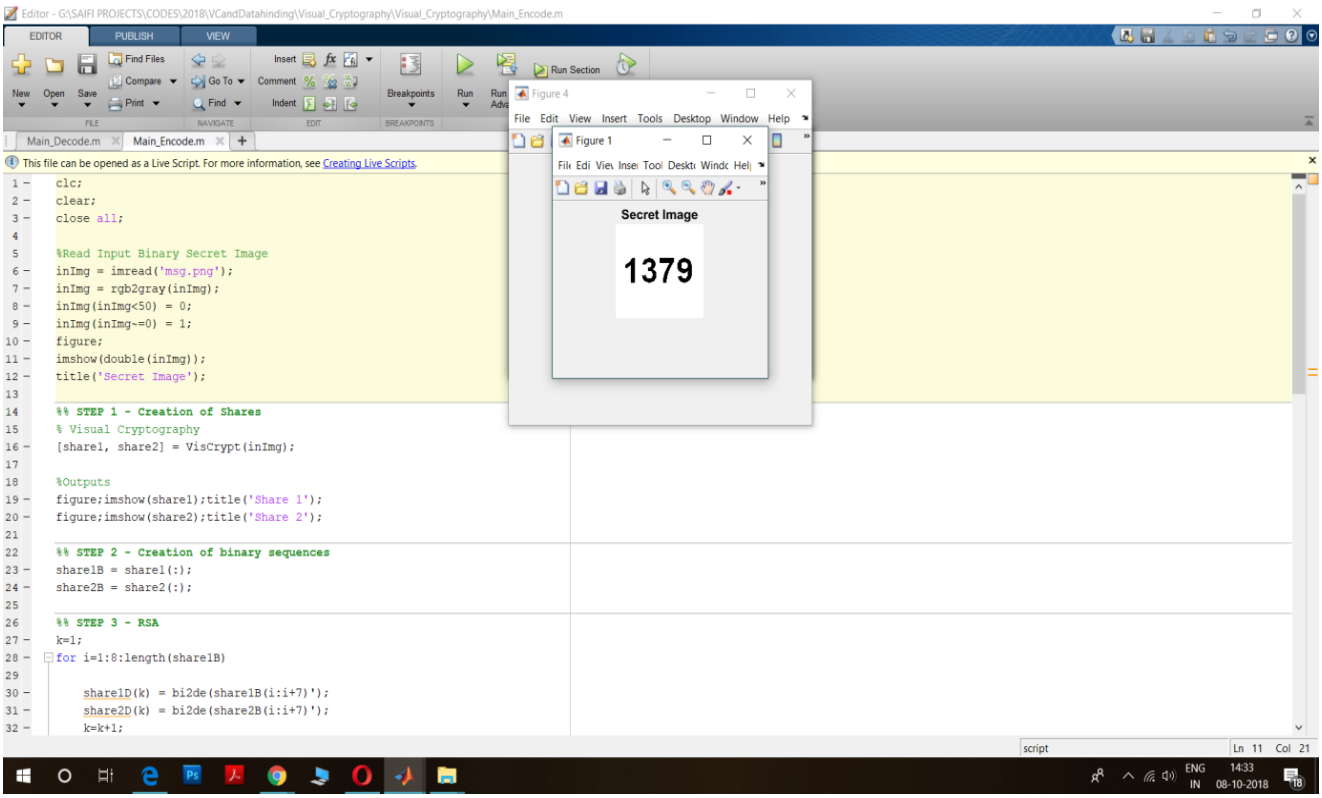

Fig-3 Secret Image

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

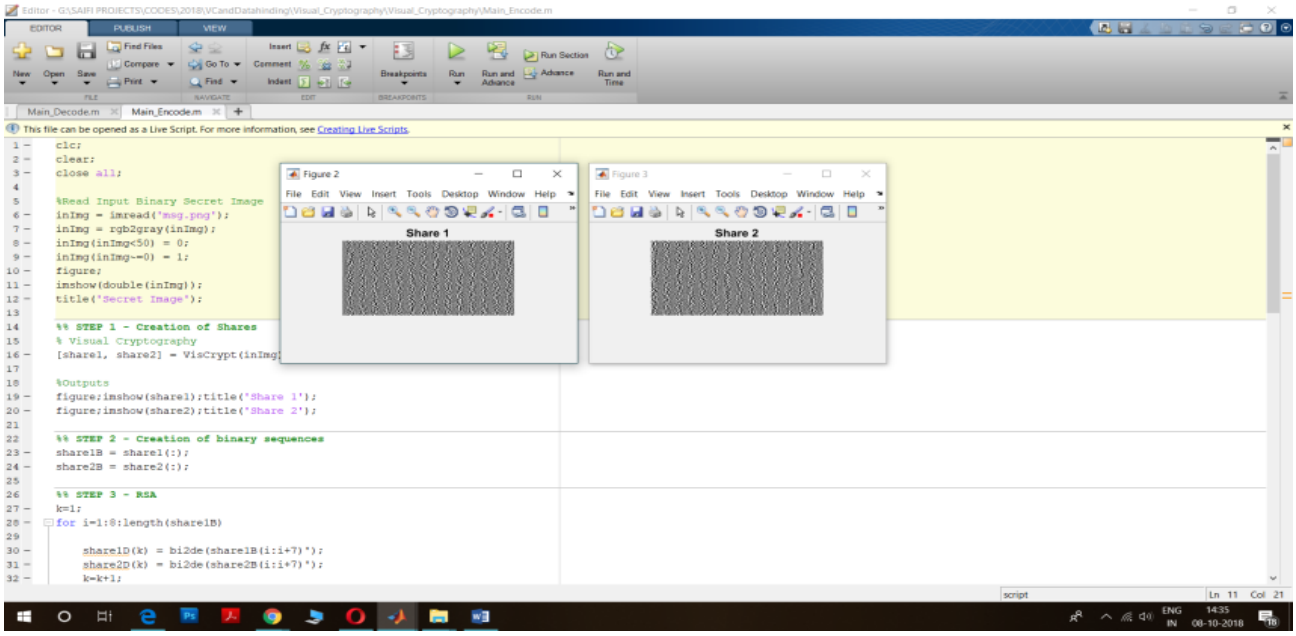

Fig-4 Visual Cryptography Image Shares

Fig-5 Cover Image

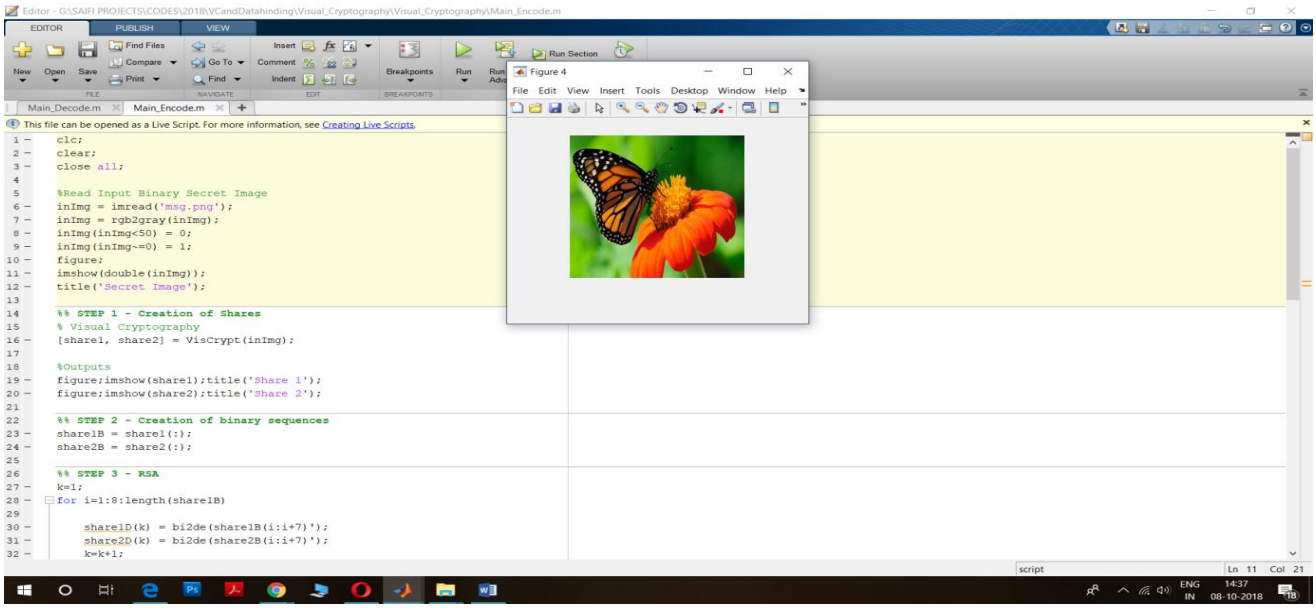

Fig-6 Stego Image

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

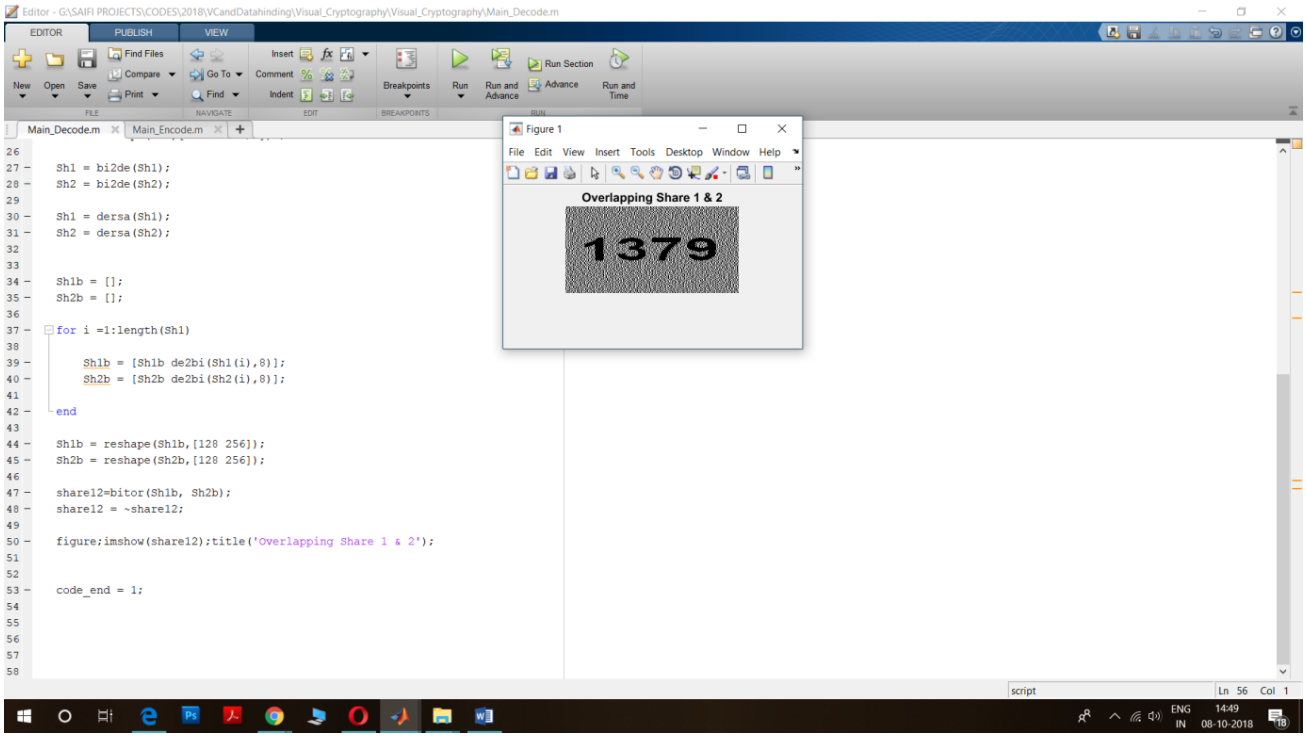

Fig-7 Visual Cryptography Output

III. CONCLUSIONS

The proposed method is very useful technique for secure communication over the Internet. In the process of Steganography, the message which is hidden is invisible. An attempt has been made to implement encryption and decryption techniques on the data to be hidden into the carrier files, so that this will provide additional security to the data. The sender and receiver only know how to hide and unhide the data into the carrier files. No other intermediate person will even know that there is a second message inside the carrier file. The sender and receiver only know the commands to hide and unhide.

REFERENCES

1. Chhabra, N.: Visual Cryptographic Steganography in Images. JCSNS Int. J. Comput. Sci. Netw. Secur. 12(4), 126 (2012) 2. Kumar, A., Pooja, K.: Steganography-A data hiding technique. Int. J. Comput. Appl. 9(7), 19 (2010)
2. Ravi Kumar Naidu, T., Gowtham Prasad, T.V.S., Mamatha, P.G.: An approach of robust high capacity audio steganography and cryptography using LSB algorithms. Int. J. Eng. Trends Technol. (IJETT). 9(10), 521–523 (2014)
3. Fallahpour, M., Megı´as, D.:High capacity method for real-time audio data hiding using the FFT transform. Span. Min. Sci. Innov. FEDER, SI2007-65406-C03-03 E-AEGIS and CONSOLIDER CSD2007-00004 ARES
4. Puech, W., Rodrigues, J., Develay-Morice, J.E.: A new fastreversible method for image safe transfer. J. Real-Time Image Proc. 2(1), 55–65 (2007)
5. Kaur, M., Kaur, M.S.: Survey of Various Encryption Techniquesfor Audio Data. Int. J. Adv. Res. Comput. Sci. Softw. Eng., 4(5), ISSN:2277 128X, (2014)
6. Tamimi, A.A., Abdalla, A.M.: An audio shuffle-encryptionalgorithm In: Proceedings of the World Congress on Engineering and Computer Science WCECS 2014, 22–24 October, 2014, San Francisco, USA
7. Fatima, Z., Khanna, T.: Audio steganography using DES algorithm. In: Proceedings of the 5th National Conference; INDIACom-2011, Computing For Nation Development, March 2011
8. Shaikh, A., Solanki, K., Uttekar, V., Vishwakarma N.: Audio Steganography And Security Using Cryptography. Int. J. Emer. Technol. Adv Eng., ISO 9001:2008 Certified Journal, 4(2), (2014)
9. Padmashree, G., Venugopala, P.S.: Audio stegnographyandcryptography: using LSB NAlgorithm at 4th and 5th LSB layers. Int. J. Eng. Innov. Technol. (IJEIT) 2(4), 177 (2012)
10. Guntupalli, N., Raju P.D.R., Cheekaty, S.: An introduction todifferent types of visual cryptography schemes. Int. J. Sci. Adv. Technol., 1(7), ISSN:2221–8386, (2011)
11. Shinde, A., Prabhudesai, N.R., Sable, S.B., Madhuri, L.: Enhanced security system for real time applications using visual cryptography. Int. J. Innov. Technol. Adap. Manag. (IJITAM), 1(10), ISSN: 2347–3622, (2014)
12. Al-Othmani, A.Z., Manaf, A.A., Zeki, A.M.: A survey onsteganography techniques in real-time audio signals and evaluation. IJCSI Int. J. Comput. Sci. Issue, 9(1), (2012)
13. Revenkar, P.S., Anjum, A., Gandhare, W.Z.: Survey of visualcryptography schemes. Int. J. Secur. Appl. 4(2), 49 (2014)
14. Suklabaidya, A., Sahoo, G.: Visual cryptographic applications.Int. J. Comput. Sci. Eng. (IJCSE) 5(6), 464 (2013)

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)