ISSN:0975-9646

Image Steganography for Secret Transmission of Data Using Cryptography Approach for Encryption of Data

Teena Rani[1], Shifali Singla[2]

1. Student, Yadwinder college of Enginnering, Talwandi sabo

2. Assistant Professor. Yadwinder college of Enginnering, Talwandi sabo

Abstract- Steganography is a technique for the secure transmission of data over the network. In this process, the secret information is transmitted by hiding this behind a signal or image or video. Image stenography is another approach which utilizes an image for the secure transmission of data by hiding it behind a cover image. This paper includes the brief description on steganography, cryptography and Least significant bit algorithm. The issue in this research is security for prevention image from stegnalysis attack and the secret data is available in such a manner as it transmitted.

1. Introduction

The word steganography is derived from the Greek words "stegos" meaning "cover" and "grafia" meaning "writing" defining it as "covered writing". Steganography is one such pro-security advancement in which mystery information is inserted in a spread. Steganography is the craft of secured or concealed composition. The motivation behind steganography is undercover correspondence to conceal a message from an outsider. This contrast from cryptography, the craft of mystery composing, which is planned to make a message indistinguishable by an outsider, however does not shroud the presence of the mystery correspondence. In spite of the fact that steganography is divided and unique from cryptography, there are numerous analogies between the two, and a few writers arrange steganography as a manifestation of cryptography since shrouded correspondence is a type of mystery composing (Bauer 2002). In any case, this paper will treat steganography as a different field.

Despite the fact that the term steganography was just coined toward the end of the fifteenth century, the utilization of steganography goes back a few centuries. In antiquated times, messages were covered up on the again of wax composing tables, composed on the stomachs of rabbits, or tattooed on the scalp of slaves. Imperceptible ink has been being used for quite a long time for entertainment only by kids and understudies and for genuine surveillance by spies and terrorists.

Steganography hides the secretive message however not the way that two gatherings are corresponding with one another.

The steganography handle for the most part includes setting a shrouded message in some vehicle medium, called the transporter. The mystery message is inserted in the transporter to structure the steganography medium. The utilization of a steganography key may be utilized for encryption of the concealed message and/or for randomization in the steganography plan.

There are many different protocols and embedding techniques that enable us to hide data in a given object. However, all of the protocols and techniques must satisfy a number of requirements so that steganography can be applied correctly the following is a list of main requirements that steganography techniques must satisfy:

a) The integrity of the hidden information after it has been embedded inside the stego object must be correct.
b) The stego object must remain unchanged or almost unchanged to the naked eye.
c) In watermarking, changes in the stego object must have no effect on the watermark.
d) Finally, we always assume that the attacker knows that there is hidden information inside the stego object.

1.1 CRYPTOGRAPHY

In today's data age, data offering and exchange has expanded exponentially. Cryptography can be characterized as the change of information into a mixed code that can be deciphered and sent over an open or private system. Cryptography utilizes two principle styles or manifestations of scrambling information; symmetrical and topsy-turvy. Symmetric encryptions, then again calculations, utilize the same key for encryption as they accomplish for decoding. Different names for this sort of encryption are mystery key, imparted key, and private-key. Cryptography is the art of utilizing science to encode also decode information. Cryptography empowers you to store delicate data or transmit it crosswise over shaky systems (like the Web) so it can't be perused by anybody aside from the planned beneficiary. While cryptography is the exploration of securing information, cryptanalysis is the art of investigating and breaking secure correspondence. A cryptographic calculation, alternately figure, is a scientific capacity utilized as a part of the encryption also decoding procedure. A cryptographic calculation meets expectations in mix with a key—a statement, number, or expression to scramble the plaintext. The same plaintext encodes to diverse cipher text with distinctive keys. The security of encoded information is altogether subject to two things: the quality of the cryptographic calculation and the mystery of the key.

1.2 LSB

The concept of LSB Embedding is simple. It exploits the fact that the level of precision in many image formats is far greater than that perceivable by average human vision. Therefore, an altered image with slight variations in its colors will be indistinguishable from the original by a human being, just by looking at it. In conventional LSB technique, which requires eight bytes of pixels to store 1byte of secret data but in proposed LSB technique, just four bytes of pixels are sufficient to hold one message byte. Rest of the bits in the pixels remains the same. A basic methodology for installing data in spread picture is utilizing Least Significant Bits (LSB). The least complex steganography systems embed the bits of the message specifically into least significant bit plane of the spread picture in a deterministic arrangement. Modulating the least significant bit does not bring about human-noticeable distinction on the grounds that the abundance of the change is little. To hide a mystery message inside a picture, a fitting spread picture is required. Because this system utilizes bits of every pixel as a part of the picture, it is important to utilize a lossless pressure group, overall the hidden data will become mixed up in the changes of a lossy pressure calculation.

Steganography is done for secure transmission of data on network. Various phases for data steganography are described below.

Phase 1

Select on cover image for data embedding cover image should be a color image containing red, green and blue pixels.

Phase 2

In the second phase least significant bits and intermediate significant bits for implemented for the predictions of No. of least significant bits available in that according to pixel value.

Phase 3

In this phase secret data is embedded into the LSB and ISB of cover images. Secret data that has to be embedding has been covert into cipher text that has to been generated by cryptographic approaches.

2 FLOWCHART

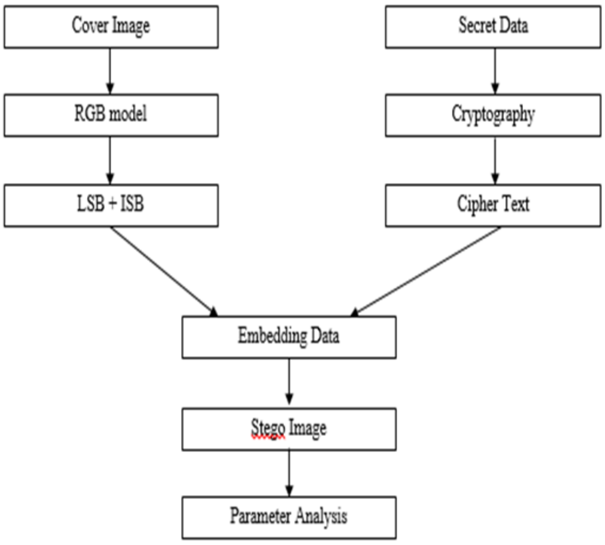


Fig.1 Flow of Work

3. RESULTS AND DISCUSSIONS

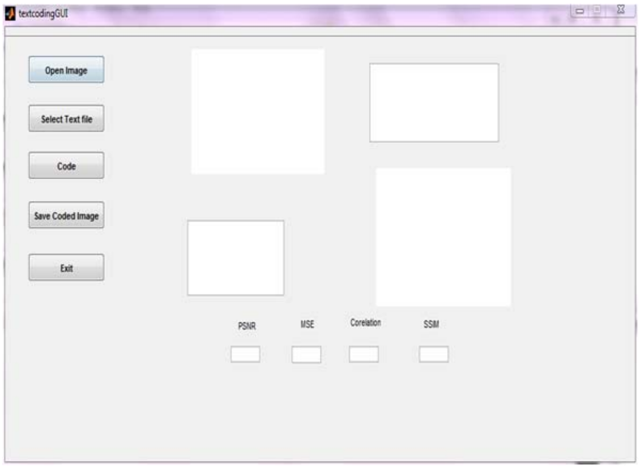


Fig 2 GUI Representation for Image Stegnography

This figure is use to represent GUI for image stegnography. In this GUI various buttons axes & edit boxes have been used for various operations to be performed. These buttons perform various actions.

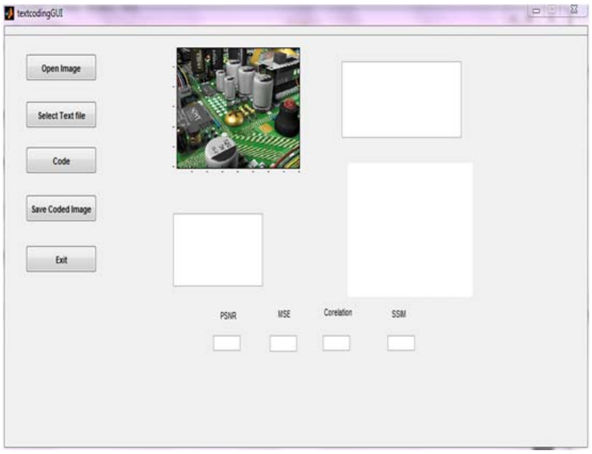
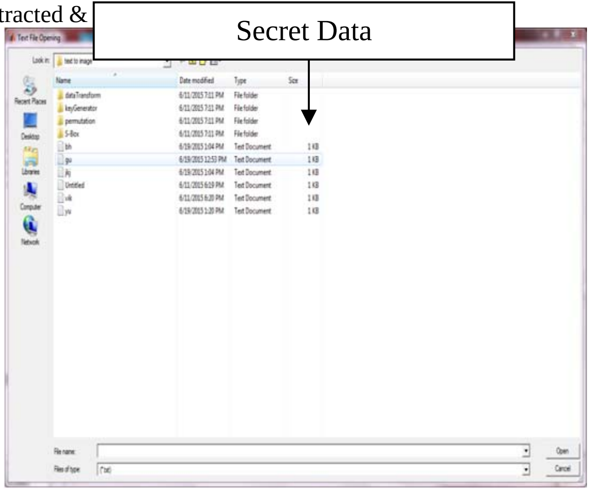


Fig 3 Input Images for Hidden Text

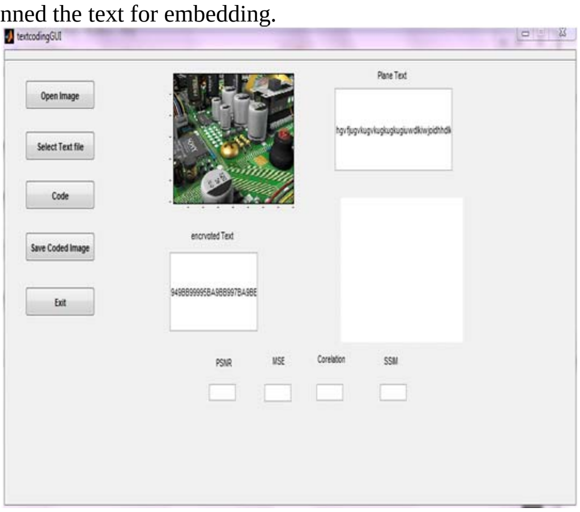
This figure is use to represent input image has been loaded for stegnography. In this image the R, G, B Components have been extracted &



Name	Date modified	Type	Size
dataTransform	6/11/2015 7:11 PM	File folder	
keyGenerator	6/11/2015 7:11 PM	File folder	
permutation	6/11/2015 7:11 PM	File folder	
S-Box	6/11/2015 7:11 PM	File folder	
bh	6/19/2015 1:04 PM	Text Document	1 KB
gu	6/19/2015 12:53 PM	Text Document	1 KB
jkj	6/19/2015 1:04 PM	Text Document	1 KB
Untitled	6/11/2015 6:19 PM	Text Document	1 KB
vik	6/11/2015 6:20 PM	Text Document	1 KB
yu	6/19/2015 1:20 PM	Text Document	1 KB

Fig 4Wind for selection of Text File

This figure is use to represent the user interface for selection of text file for embedding behind the mage. This text file is loaded & scanned the text for embedding.



Plane Text

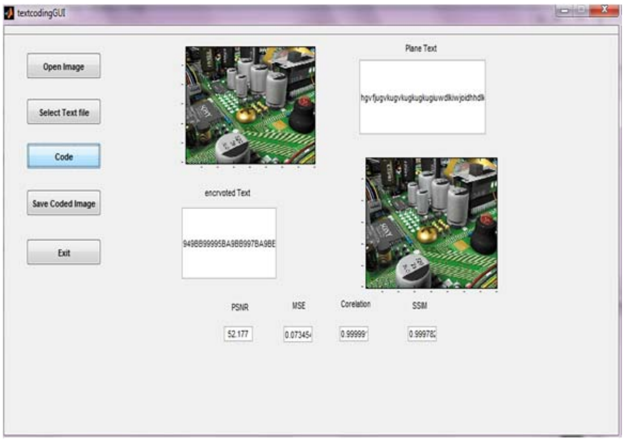
hgvfjugvkugvkugkugkugiuwdkiwjoidhhdk

encrvoted Text

949BB99995BA9BB997BA9BE

Fig 5 Encryption of text data using AES Encryption

This figure is use to represent the encryption of the best reusing AES Encryption scheme. This encryption standard use round keys for mixing, shifting of rows & columns. Then this approach converts the plain text in to cipher text.



Plane Text: hgvfjugvkugvkugkugkugiuwdlkiwjpidhhdk

encrvoted Text: 949BB99995BA9BB997BA9BE

PSNR: 52.177

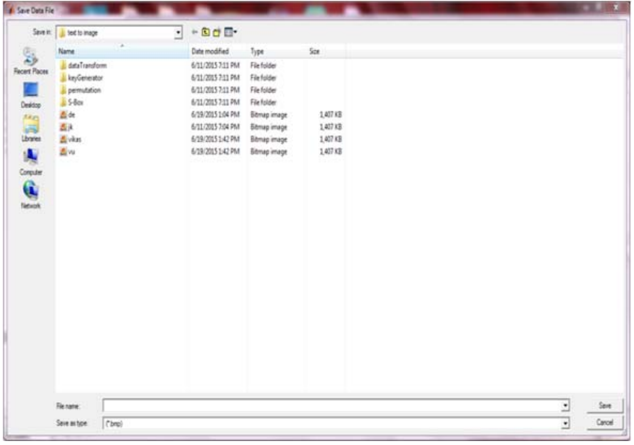
MSE: 0.073454

Corelation: 0.99999

SSIM: 0.99978

Fig 6 Embedding of encrypted data behind image

This figure is use to represent the embedding of data behind the least significant of R, G & B region of the cover image. These regions have been extracted from red, green & blue region. After extraction of the region the least significant bit has between computed. The text has been converted in to binary format so that it can be embedded behind the cover object least significant bit using XOR operation. These regions have been reconstructed to develop true caller stegno image.



Save in: text to image

Name	Date modified	Type	Size
dataTransform	6/11/2015 7:11 PM	File folder	
keyGenerator	6/11/2015 7:11 PM	File folder	
permutation	6/11/2015 7:11 PM	File folder	
S-Box	6/11/2015 7:11 PM	File folder	
de	6/19/2015 1:04 PM	Bitmap image	1,407 KB
jk	6/11/2015 7:04 PM	Bitmap image	1,407 KB
vikas	6/19/2015 1:42 PM	Bitmap image	1,407 KB
vu	6/19/2015 1:42 PM	Bitmap image	1,407 KB

File name:

Save as type: (*.bmp)

Fig 7 User interface for saving stego image

This figure is use to represent the user interface that has been used for saving of stego image to a save on hard drive. This is done by using input file function.

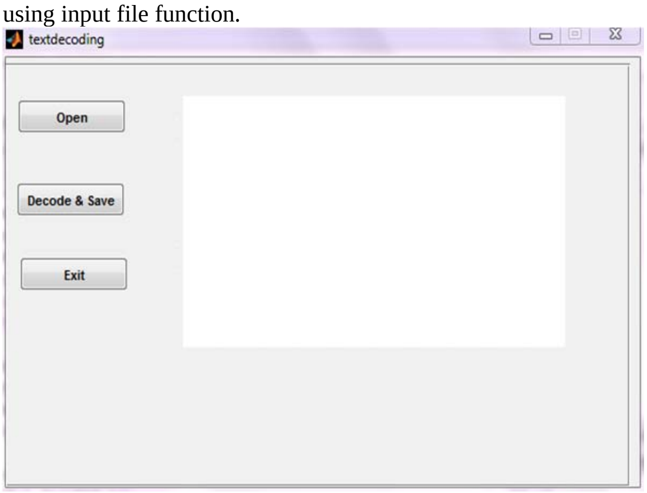


Fig 8 GUI for encryption of data

This figure is use to represent GUI for image stegnography. In this GUI various buttons axes & edit boxes have been used for various operations to be performed. These buttons perform various actions.

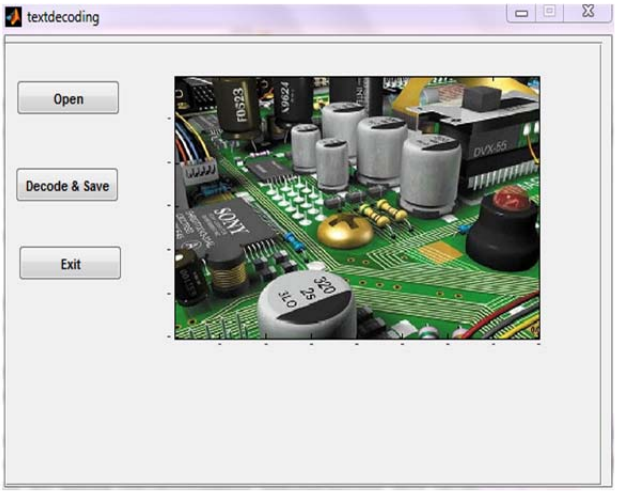


Fig 9Stego image loaded for encryption of data

This figure is use to represent the stego image has been loaded to the system. This image is divided into three different red, green & blue regions. The least significant bit has been computed & data is extracted that has been hidden behind these objects. This data is reshaped in to a vector factor that represents cipher text. This cipher text is decrypted by using AES decryption & stored in a text file for further access.

4. Conclusion

Steganography is a technique for the secure transmission of data over the network. In this process, the secret information is transmitted by hiding this behind a signal or image or video. Image stenography is another approach which utilizes an image for the secure transmission of data by hiding it behind a cover image. In this process image is divided into different regions for the detection of least significant bits available in different images. Image pixel available in the image is a combination of three different colors red, green and blue. This combination of image pixels contains 8 bit for each color that have 24 bit true color. These 8 bits of each color contains different LSB and MSB from these bits. In the previous works LSB has been detected and status bit has been used from different MSB available in the three MSBs of RGB. The MSB of these three colors has been divided into two different regions using lighter and darker portion. According to lighter and darker region these bits has been divided for status bits. These status bits utilized for embedding the message into different least significant bits. The issue in this is security for prevention image from stegnalysis attack and the secret data is available in such a manner as it transmitted. We got various types of parameters & on the basis of these parameters we conclude that our system gives us better results.

References

[1] Lip Yee Por "Information Hiding: A New Approach in Text Steganography" *7th WSEAS Int. Conf. on applied computer & applied computational science*, 2008, pp 6-8.

[2] Lingjun Li "A Statistical Attack on a Kind of Word-Shift Text-Steganography", *IEEE Conf. on Intelligent Information Hiding and Multimedia Signal Processing,* 2008, pp 1503 – 1507.

[3] Neha Rani "Text Steganography Techniques: A Review" *IEEE International Journal of Engineering Trends and Technology (IJETT)*, 2013, PP 3013-3015.

[4] Debnath Bhattacharyya "Text Steganography: A Novel Approach" *International Journal of Advanced Science and Technology,* 2009, PP 79-89.

[5] WesamBhaya "text steganography based on font type in ms-word documents*", IEEE Conf. on Journal of Computer Science*, 2013, pp 898-904.

[6] JinsukBaek, Fisher, P.S. , Hongyang Chao "Secret sharing approach based on steganography with gray digital images", *IEEE International Conference onWireless Communications, Networking and Information Security*, pp. 325 – 329, 2010.

[7] Moon, S.K, Kawitkar, R.S. "Data Security Using Data Hiding", *International Conference onComputational Intelligence and Multimedia Applications,* pp. 247 – 251, IEEE, 2007.

[8] Saravanan, V. ,Neeraja, A. "Security issues in computer networks and stegnography", 7th International Conference onIntelligent Systems and Control, pp. 363 – 366, IEEE, 2013.

[9] Gutub, A. "Pixel Indicator Technique for RGB Image Steganography", *Journal of Emerging Technologies in Web Intelligence,* Vol. 2, pp. 193-198, IEEE, 2010.

[10] Bailey, K. "An evaluation of image based steganography methods", *Journal of Multimedia Tools and Applications*, Vol. 30, pp. 55-88, IEEE, 2006.

[11] Mahata, S.K. "A Novel Approach of Steganography using Hill Cipher", *International Conference on Computing, Communication and Sensor Network*, pp. 975-888, IEEE, 2012.

[12] Xikai Xu, Wei Wang, Tieniu Tan "Video steganalysis based on the constraints of motion vectors" *20th IEEE International Conference onImage Processing,* pp. 4422-4426, 2013.