Data Transfer through an Image and Its Recovery Causing Minimum Distortion in the Carrier Image: A Survey

Vrishali U. Gaikwad
Post Graduate Student
Department Of Computer Engineering
JSPM's Imperial College of Engineering and Research
Wagholi Pune, Maharashtra, India
89gaikwad1vrishali@gmail.com

***Abstract*—** This paper, tries to address the problem of transmitting the huge amount of data over a communication channel hidden into an image and making sure that there is minimum distortion created into the image carrying that secret data. In this project the sender or the data owner who wants to send his data first encrypts the data and then store that encrypted data in such an efficient way that it required minimum number of bits to be altered to hide the data into an Image. This efficiency is created using the LFSR algorithm which is applied on the secret key which in turn creates a unique set of keys which are checked and used for hiding the data. The data too is not hidden sequentially into an image, it is hidden randomly based on the secret key making it more complicated. Once the data is hidden the image the, it is encrypted using the AES algorithm. Here too it adds the encryption in parallel where the image is divided into equal parts and then the AES algorithm is applied to all the parts of the image simultaneously, thus saving our time in the encryption process. Thus shows a significant time saving in case the large images are used. This image when encrypted is send to the receiver and at the receivers end ,the one who has the correct keys can only get back the original image and the secret data. This makes sure that the receiver get the correct data and the image with minimum distortion.

Keywords: *Data Hiding, LFSR, AES, LSB Steganography, UIQI.*

*****

I. EXISTING SYSTEM

A content owner encrypts the original image using an encryption key, and a data-hider can embed additional data into the encrypted image using a data-hiding key though the receiver does not know the original content. With an encrypted image containing additional data, a receiver may first decrypt it according to the encryption key, and then extract the embedded data and recover the original image according to the data hiding key. In this system, the data extraction is not separable from the content decryption i. e the additional data must be extracted from the decrypted image, so that the original content of original image is detected before data extraction, and, if someone has only the data hiding key but not the encryption key, receiver cannot extract any information from the encrypted image containing additional data.

II. ENCRYPTION ALGORITHM:

RC4 is a stream cipher algorithm which needs a secure exchange of a shared key. The symmetric key algorithm is used identically for encryption as well as decryption, wherein the data streams are simply XOR'ed with the generated key sequences. This algorithm is known as serial algorithm as it needs successive exchanges of state entries based on the generated key sequence so that the implementation can be very intensive.

The key streams are absolutely independent of the plaintext being used. It doesn't use a fixed length key and can vary from 1 to 256 bit to initialize a 256-bit state table. The state table is used for generation of random bits which in turn generates a pseudo-random bit stream which is XORed with the plain text to obtain the cipher text.

III. IMAGE ENCRYPTION AND DATA EMBEDDING

Image Encryption:

In this system firstly the content owner is responsible for the encrypting the image in which the data is going to be hidden and then is sent to the receiver. The content owner uses the Encryption Key to encrypt the image .The Encryption algorithm used is RC4 algorithm, where in the original image is given as an input and it is XOR'ed with the randomly generated key sequence creating a ciphered image or an Encrypted Image. This encrypted image is then given as an input to the Data Hider, where the data is hidden or embedded into an Encrypted Image.

 ISSN: 2321-8169
4248 - 4251

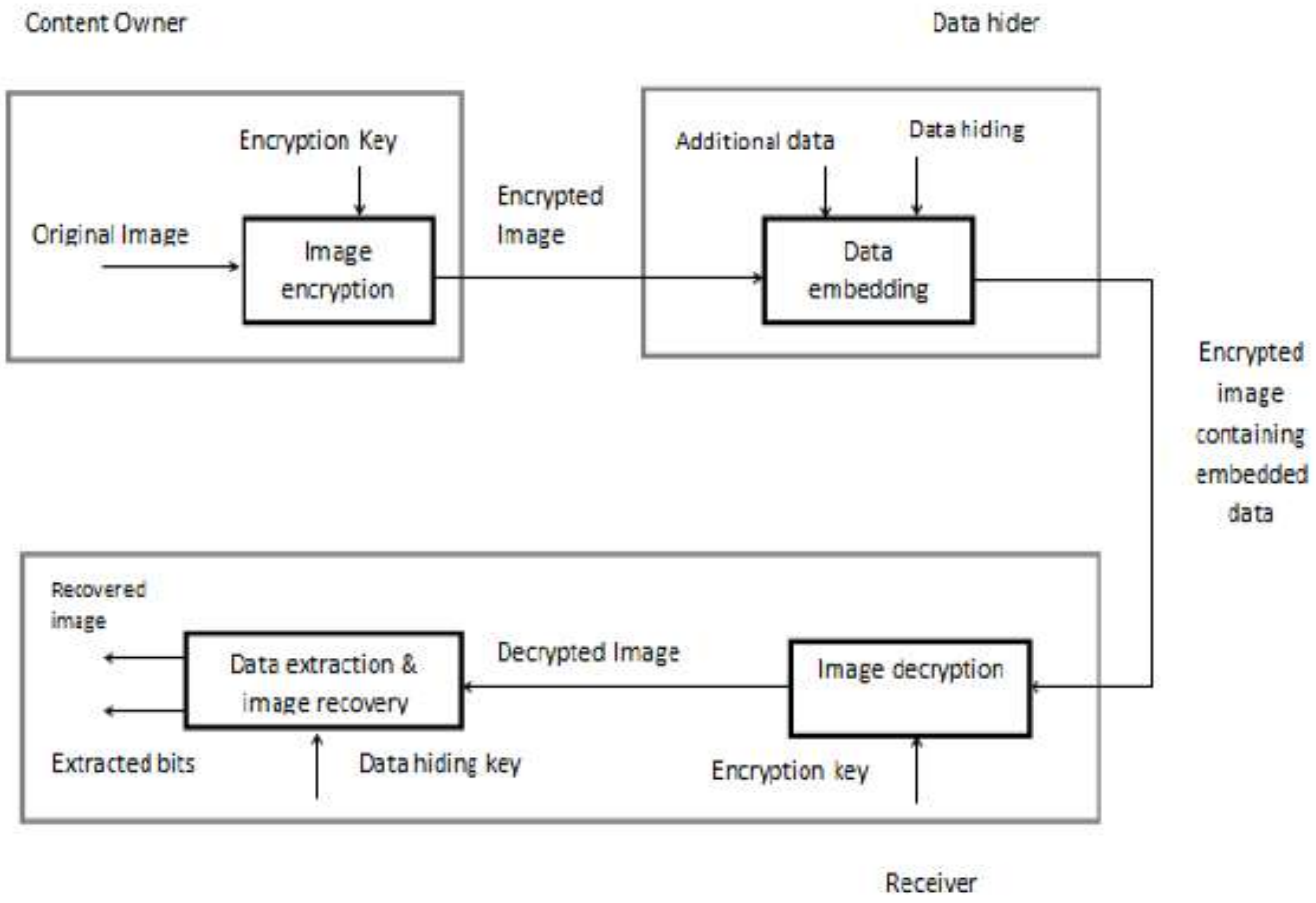

Figure 1: Block Diagram for Non separable reversible data hiding in encrypted image.

Data Embedding:

In this data embedding phase, certain parameters are embedded into few number of encrypted pixels of the image, and the LSB of the remaining encrypted pixels are compressed to create some space for embedding the additional data and the original data at the positions occupied by the parameters. According to a data-hiding key provided,the data hider randomly selects Np encrypted pixels which will be used to carry the parameters for data hiding, where Np is an small positive integer. The other (N-Np) remaining encrypted pixels are pseudo-randomly permuted and divided into a number of groups, each group containing L number of pixels. The way in which the permutation will be carried out is also determined by the data-hiding key. For each pixel-group, collect the M least significant bits of the L pixels, and denote them as B(k,1),B(k,2)…B(k, M. L) where k is a group index within[1,(N-Np)/L] and M is a positive integer which is less than 5. The data-hider also generates a matrix G sized (M.L-S)×M.L, which is composed of two parts.

$$G= [IM.L-SQ]$$

Where the left most part is an (M.L-S) × (M.L-S) identity matrix,the right part Q sized (M.L-S) ×S is a pseudo-random binary matrix derived from the data-hiding key. S is a small positive integer. Now,embed the values of the parameters M,L and S into the LSB of NP selected encrypted pixels.

IMAGE AND DATA EXTRACTION

In this phase the receiver who possess both the Data Hiding key and the encryption key will be able to get the original image as well as the embedded secret data.

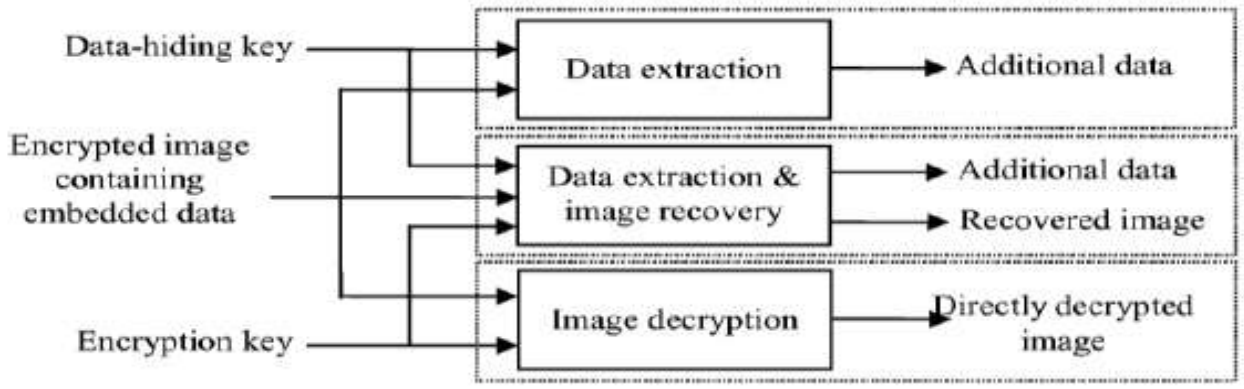

Figure 2: Block Diagram Image and Data Extraction

LIMITATIONS OF EXISTING SYSTEM

- ✓ The existing system works on 8 bit Gray Scale Images.
- ✓ The existing system uses RC4 algorithm which is a steam cipher and is vulnerable to attacks.
- ✓ Existing system compresses the LSB's to add secret data to it causing more distortion to the original Image.
- ✓ There is no double encryption to the secret data.
- ✓ Requires more time for the system to generate the receiver ready encrypted Image.
- ✓ It shows relatively low PSNR ratio for the recovered image ,which can be improved.
- ✓ Compression technique for storing the data, can limits the amount of data that can be stored into an image.

IV. PROPOSED SYSTEM

OVERVIEW

The new system proposes the way in which it provides double security to the secret data by providing double encryption to the secret data, also making sure that the image undergoes minimum distortion when data is hidden into it so that the recovered image is the same when compared to the Original Image. The proposed system uses AES algorithm which is a block cipher to encrypt the data and the image, also the encryption is carried out in parallel so as to save tie required for encryption. This factor is significant in case the images are large in size. Here the secret data will not be stored in the sequential form into the pixel using LSB replacement but will be stored in random sequence after generating the optimal index which will make sure that minimum number of bits are changed into the image to accommodate the data making it more complex, causing minimum change to the cover image and making it full proof from any potential threat.

V. OPTIMAL KEY GENERATION FOR DATA EMBEDDING

The proposed system first takes the input as the 32 bit carrier image in which the encrypted data will be hidden. Once carrier image is specified calculation for the amount of data that can be sent based on the size of the image is done. After receiving the carrier image the key (k1) is taken with which the data is to be embedded and hidden into the carrier image. The key received is in the plain text format which is converted into a 32 bit sequence. This 32 bit sequence is then passed to the LFSR algorithm which then creates a unique set of 32 bit keys. This unique set of 32 bits is obtained by XORing the fixed numbered bits(e.g:2,4,8 numbered bits) and by shifting all the bits one place to the left and put the result bit of XORing in the first position of 32 bit sequence. This process is carried out until the original 32 bit sequence back is generated again .After having all the 32 bit key ,the file is obtained which has the users secret data in the chunk of 32 bits and XOR it with the 1st key of the key set until all done with the complete data of the Data file. This XORed data is then checked against the Least Significant Bit values of the RGB channel extracted from all the image pixel. While doing this track is kept of how many bits are needed to be changed to put this data into an image. This count helps us to do Noise estimation for each key. This process of getting the data from data file and XORing it with different key is carried out for all the keys in the key set and estimation of noise is done for each key in the key set. The key for which the Noise is minimum is used for hiding the data into the Image. This way the data is hidden with minimum loss to the Original Image. Once this is done image is ready for committing LSB Steganography for finally storing the data with the Optimal Key.

VI. DATA HIDING AND IMAGE ENCRYPTION

Data Hiding:

Once the secret data after XORing with the optimal key is obtained then it is ready for hiding this data into an Image. The data hiding into an image will be carried out using an method called LSB Steganography. In this method the secret data bits are stored into the LSB's of the R,G,B channels of each pixel of the cover image. This process of replacing the image bits with the data bits is carried out where ever there is mismatch of the bits and that too is carried out in random sequence. This random sequence is created using the Key K1 which was given by the sender or the content owner. So this random-ness will change with the change of the Key K1 making it more secure as the person which gives the correct Key K1 will only get the correct secret data. Thus achieving minimum distortion to the original image and also the random ness of hiding the data will increase its complexity.

Encryption:

Once the XOR'ed data is hidden randomly into the image, the image is ready to be encrypted using the AES algorithm. To improve the time requirement for the encryption, the encryption of the image is carried out in parallel so that minimum time is required to encrypt the entire image. Content owner uses the Key K2 to perform the encryption .This system will divide the image into equal parts and then apply the AES to each part simultaneously. So that the encryption process is carried out in parallel on all the parts of the image and thus saving the time required. This approach will contribute significantly when the images used are of large size, making system fast and reliable.

Finally this project uses UIQI [Universal Image Quality Index] to determine along with PSNR for evaluating the image quality after its recovery at the receivers end.

VII. CONCLUSION

Steganography is an effective way of hiding the sensitive information. This approach has used the LSB technique on images to get the secure stego-image which is encrypted and then sent to the receivers. As here only the last bit of each channel of every pixel is altered so there is non-significant change in the image and also it is checked and uses the key that makes minimum changes in the bit pattern for every pixel. This system focuses on hiding more data fatser while increasing the PSNR and reducing the distortion rate. It also focuses in getting the QIUI to close to 1 so that there is minimum distortion in the decrypted Image.

REFERENCES

[1] "Announcing the ADVANCED ENCRYPTION STANDARD (AES,"csrc.nist.gov/publications/_ps/_ps197/_ps-197.pdf.

[2] "A Secure Image Steganography Using LSB Technique and Pseudo Random Encoding Technique,"pdf.

[3] "Linear feedback shift register,"from Wikipedia, the free encyclopedia.

[4] Mukesh Patil and Prakash Kadam",Separable Reversible Encrypted Data Hiding in Encrypted Image Using AES algorithm and Lossy Tech-nique.",Proceedings of the 2013 International Conference on Pattern Recog-nition, Informatics and Mobile Engineering (PRIME) February 21-22.

[5] V. Suresh and C. Saraswathy.,"Separable Reversible Data Hiding Using Rc4,".pdf,Proceedings of the 2013 International Conference on Pattern Recognition, Informatics and Mobile Engineering (PRIME) February 21-22.

[6] Xinpeng Zhang,"Separable Reversible Data Hiding in Encrypted Image," IEEE Transactions on Information Forensics and Security, VOL. 7, NO. 2,APRIL 2012.

[7] Zhou Wang,"A Universal Quality Index,"Student Member IEEE and Alan C.Bovik,Fellow,IEEE.

[8] K. Naveen BrahmaTeja,Dr. G. L. Madhumati,K. Rama Koteswara Rao,"Data Hiding Using EDGE Based Steganography",International Journal of Emerging Technology and Advanced Engineering Website:www.ijetae.com (ISSN 2250-2459, Volume 2, Issue 11, November 2012).

[9] Kede Ma, Weiming Zhang, Xianfeng Zhao,Nenghai Yu, and Fenghua Li "Reversible Data Hiding in Encrypted Images by Reserving Room Before Encryption",IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 8, NO. 3, MARCH 2013.

[10] Ravindra Gupta, Akanksha Jain, Gajendra Singh,"Combine use of Steganography and Visual Cryptography for Secured Data hiding in Com-puter Forensics",International Journal of Computer Science and Information Technologies, Vol. 3 (3) , 2012,4366 - 4370.

[11] Xu Bo, Wang Jia-zhen, Peng De-yun,"Practical Protocol Steganography:Hiding Data in IP Header",Proceedings of the First Asia International Con-ference on Modelling & Simulation (AMS'07) 0-7695-2845-70/7 $ 20.00 2007. ICOER,Pune 70 Dept. of Computer Engg.Project Report Seperable Reversible Data Hiding in a Image

[12] Nameer N. EL-Emam,"Hiding a Large Amount of Data with High Security Using Steganography Algorithm",Journal of Computer Science.