Implementation of Secure Data Hiding Technique for Encrypted Images

Ms. Divyashree K B
IV Sem M.tech,
A.P.S. College of Engineering,
Bangalore, India.

Prof. Bhagyashree R
Assistant Professor, Dept. of CSE,
A.P.S. College of Engineering,
Bangalore, India.

***Abstract*: This paper proposes reversible and reliable data hiding in images .Nowadays system encryption and security has become a challenging thread for the society. Thus, we have made a move towards understanding and developing an enhanced version of reversible encryption technique under critical scenario of design. The system aims to achieve a high threshold value analysis under a reduced SNR (Signal to Noise Ratio) and PSNR (Peak Signal to Noise Ratio) ratio of channel. The signals obtained are defined under a range of programmed and parametric values. This paper poses a scheme of secure data hiding in encrypted images using distributed source coding. After encrypting the original image with a stream cipher, some bits of MSB planes are selected and compressed to make room for the additional secret data. On the receiver side, all hidden data can be extracted with the embedding key only, and the original image approximately recovered with high quality using the encryption key only. When both the embedding and encryption keys are available to the receiver, the hidden data can be extracted completely and the original image recovered perfectly.**

Key words: ***Reversible data hiding; Peak Signal to Noise ratio; Signal to Noise ratio; Slepian-Wolf encoding; Secure data hiding.***

I.INTRODUCTION

Image Processing is a system to upgrade crude pictures got from camera/sensors put on satellites, space tests and aircrafts or pictures taken in typical everyday life for different applications. Different systems have been produced in picture handling amid the last four to five decades. The majority of the strategies are produced for improving pictures acquired from anonymous shuttles, space tests and military observation flights. Picture preparing frameworks are getting to be mainstream because of simple accessibility of effective staff PCs expansive size memory gadgets, representation programming and so on. Image processing is used in various applications such as remote sensing, Medical imaging, Non-destructive analysis, Forensic studies, Textiles, Material science, Military, Documentary processing, Graph art. The common steps in image processing are image scanning, storing, enhancing and interpretation.

System encryption and security has become a challenging aspect for the society and thus we have made a move towards understanding and developing an enhanced version of reversible encryption technique under critical scenario of design. The system aims to achieve a high threshold value analysis under a reduced SNR and PSNR ratio of channel. The signals obtained are defined under a range of programmed and parametric values.[4]

II.EXISTING SYSTEM

Many Robust image data hiding algorithms have already been developed, such as image compression-based, difference expansion based, histogram shift (HS)-based, image pixel pair based, and dual/multi-image hiding methods. To hide data in encrypted domains, some digital watermarking based schemes are proposed. Besides, the commutative watermarking and ciphering schemes for digital images are introduced. As the entropy of encrypted images is maximized, it is difficult to losslessly vacate room after encryption. The data manager may want to embed additional messages into the encrypted image for authentication or steganography, even though the content of the original image is unknown to him. In this situation, hiding data in the encrypted image is an intuitive and effective way to meet such requirement.[1]

In existing system, specifically the sender scrambles the first picture, and the information hider implants the extra bits by changing a few bits of the encoded information.On the collector side, information extraction and picture recovery are acknowledged by investigating the neighborhood standard deviation in the middle of decoding of the stamped scrambled picture.This technique requires that picture unscrambling and information extraction operations must be done together. At the end of the day, extraction and unscrambling are entwined.[2]
Disadvantages:

- Due to the requirement of privacy protection, the cover owner usually encrypts and lack of conversions
- It has to be more no of data loss occurring after data extraction.
- Low accuracy.
- The technique involves predated data exchange policies
- Protocol such as RSA and Diffie Hellman are outdated with current technological strengths.
- Binary locking of data with private and public key are not protected as spoofers attack are more seen in current environment.

III. PROPOSED SYSTEM

This paper proposes a scheme of reversible data hiding in encrypted images using distributed source coding. After encrypting the original image with a stream cipher, some bits of MSB planes are selected and compressed to make

room for the additional secret data. On the receiver side, all hidden data can be extracted with the embedding key only, and the original image approximately recovered with high quality using the encryption key only. When both the embedding and encryption keys are available to the receiver, the hidden data can be extracted completely and the original image recovered perfectly. The system aims to achieve a high threshold value analysis under a reduced SNR and PSNR ratio of channel. The obtaining signals are defined under a range of programmed and parametric values.

The proposed estimation algorithm can also be used to find empirical error probability q of the virtual channel. With a database containing numerous natural images, can perform the estimation algorithm to generated estimated images. Calculate differences of the MSBs of the last three sub-images between the original and estimated images. To overcome the drawback of inseparability a separable Robust Image Data Hiding scheme was proposed for encrypted images. Reversible data hiding(RDH) methods for plaintext images have been proposed. In this situation, hiding data in the encrypted image is an intuitive and effective way to meet such requirement.

Advantages:

- In proposed system, a gray scale 250-* 250 size images is used as a cover image. This improves the system security as decoding 250 * 250 results in $^{250}C_{250}$ Combinations of keys.
- In SLEPIAN-WOLF algorithm, previously 16 and 32 bit were used and thus security is low bit error rate(B.E.R) is calculated for the transferred image. BER can fetch detailed information on data tampering
- Spoofing attacks on the system is trackable as the parity and LSB bit is used for BER Calculation.

IV. SYSTEM DESIGN

The data is collected and correlated under with adding MSB bit tampering under SLEPIAN-WOLF encoding technique. The proposed systems also consist of an embedding unit for twin image composition for transferring the same under an un trusted channel for communication. At the receiver end the system is programmed to design, acquire images under encrypted and embedded state. Each is fetched and retrieved with defaming unit. The system is also improvised in observing Peak Signal to Noise Ratio (PSNR) and SNR ratio for entire communication channel.

The proposed estimation algorithm can also be used to find empirical error probability q of the virtual channel. With a database containing numerous natural images, we perform the estimation algorithm to generated estimated images. Calculate differences of the MSBs of the last three sub-images between the original and estimated images. To overcome the drawback of inseparability a separable Robust Image Data Hiding scheme was proposed for encrypted images. RDH methods for plaintext images have been proposed.

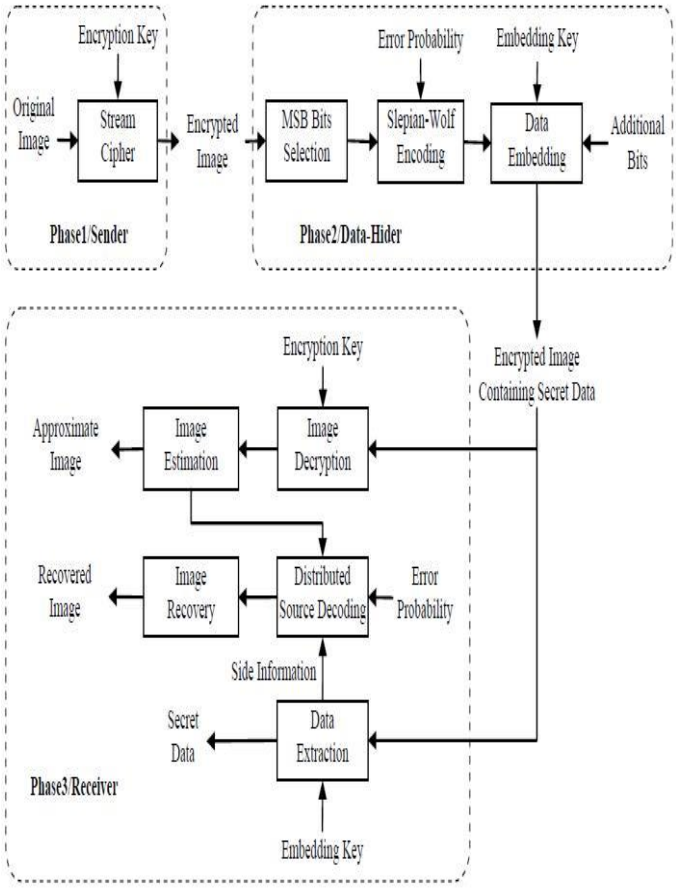

Figure 1: System architecture diagram

Algorithm: Slepian-Wolf encoding.

INPUT: Image from the service provider under sender environment encrypted or cipher text from the third party, for transmission.

OUTPUT: Successful transmission of the data hidden into it, this output image is initialized for comparisons to obtained full edged data under a protective environment.

//Pseudo Code:

STEP 1: Input the image and load to "I"
STEP 2: if (I is not gray scale
image) Do
RGB to gray (I);
STEP 3: For every value of image (I) fetch the pixel rate for more reliable Region of Interest (ROI) for data hiding.
STEP 4: Fetching data from the third party to transfer under secure channel through this algorithm.
STEP 5: Append Algorithm (Wolf)
Algorithm_wolf_S (I, N)
Perform
K ← Value of data hidden in image
I ← Image
Ik ← Encrypted image with information
I1 ← Informative and processed image if
(Image (I) >= value of data(x, y)

Perform
Encryption algorithm as
For (image (I1) up to nth pixel rate) Fetch value of pixel rate analyze the ratio. End for

End if.
Load image as Ie
Where encrypted image

STEP 6: Algorithm Decryption ((Ie , n) x ,y)
Perform
For (image (Ie) up to nth pixel rate
Fetch value ratio and analyze.
Load image (Ie)
STEP 7: Perform step 6 and 5 for image (I)
STEP 8: Compare the ratio of encrypted image (Ie) and I1 for fetching the value ratio.

V. FRAMEWORK OF PROPOSED SYSTEM

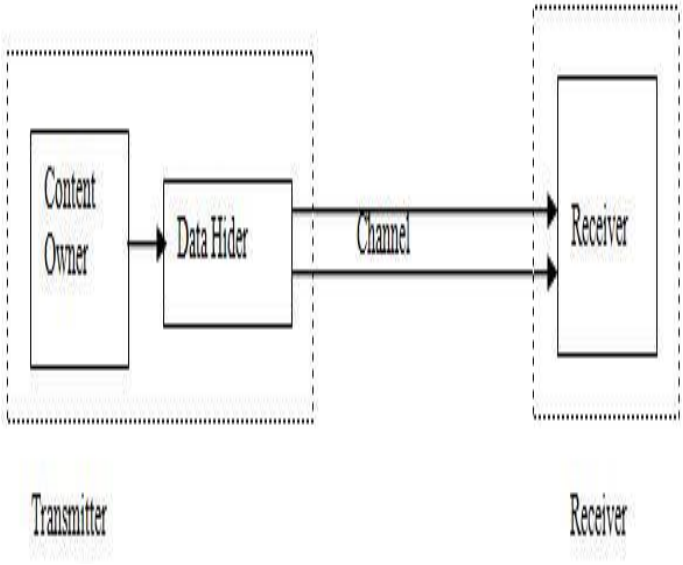

Figure 2: Framework of proposed Reversible Data Hiding

The Proposed system is basically divided into three modules they are:

i) Content owner ii) Data hider iii) Receiver
i) Content owner module:

The content owner part deals with
a) Choosing an image
b)Reserving room for embedding
c) Image encryption.

a) *Choosing image as Input:* Color image is taken as the original cover image.
b) *Reserving room:* Room or space is reserved for hiding the secret data before encryption.
c) *Image encryption:* The content owner encrypts Image. Encrypted image so formed is passed as an input to the data hider. Next module is data hider, where actually the secret data is hidden.

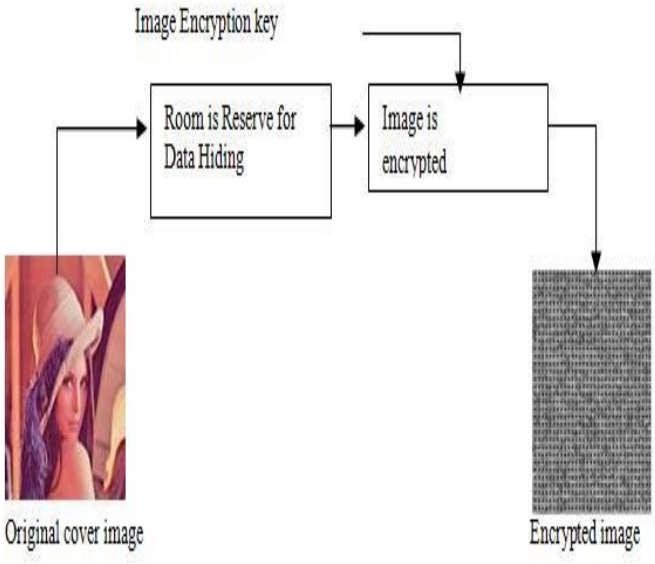

Figure 3: Framework of content owner module.

ii) Data hider module:

In data hider, this section deals with Text encryption and embedding. Refer Figure 4.

a) *Encrypted image as Input:* Encrypted image from the content owner modules is given as an input to data hider module. In addition to this, data to be hidden is also taken as another input.
b) *Encryption of Data:* Data to be hidden is encrypted using RSA asymmetric encryption key to form encrypted data.
c) *Data embedding:* Secret data to be embedded is concealed using data hiding key into the encrypted image to form an encrypted stegno image. Encrypted stegno image so formed is passed as an input to the receiver. [3]

Next module is Receiver module. Where actually the information is received or extracted.

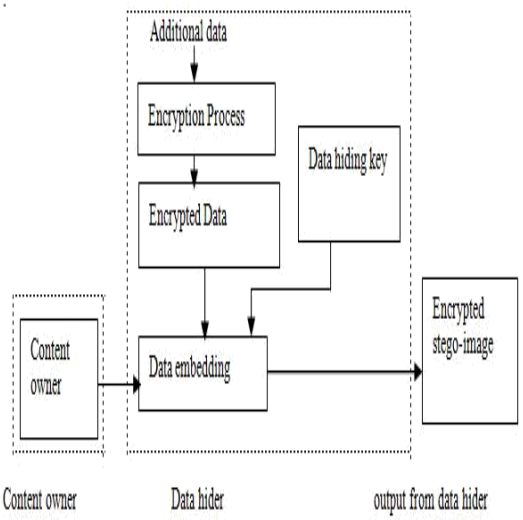

Figure 4 : Frame work shows block diagram for Data hider module.

iii) Receiver Module

Receiver can be either the content owner or any authorized person having the key. Since this paper uses asymmetric key for encryption and decryption of text, the receiver will have different key for decryption.[1]

a) *Image decryption:* The receiver receives encrypted stegno image so formed from the data hider. Image is decrypted using decryption key.
b) *Data extraction:* After the image is decrypted, text is extracted in encrypted form only.
c) *Data decryption:* Lastly, the data is decrypted using the relevant key. The decrypted image is the lossless recovery of original image.

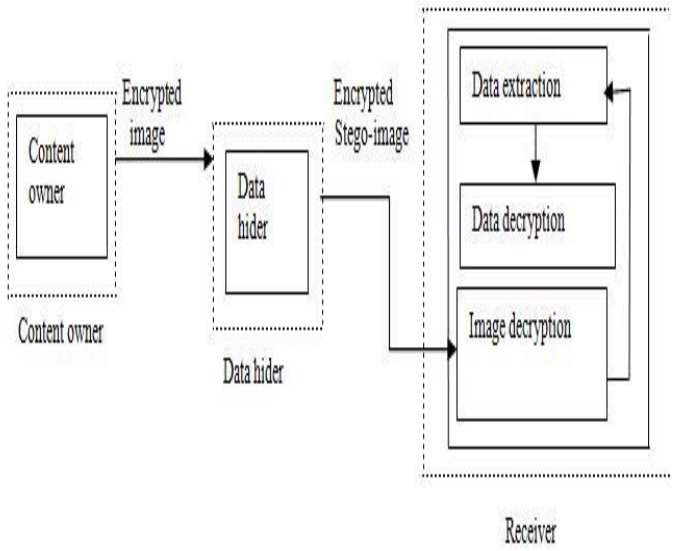

Figure 5: Framework of Receiver module.

VI.IMPLEMENTATION

The proposed system is implemented under MATLAB environment and the same is retrieved from the practical approach. The outputs achieved are shown below for detailed analysis.

Figure 6: Cover Image

Figure 7: Secret Image

Figure 8: Embedded Image

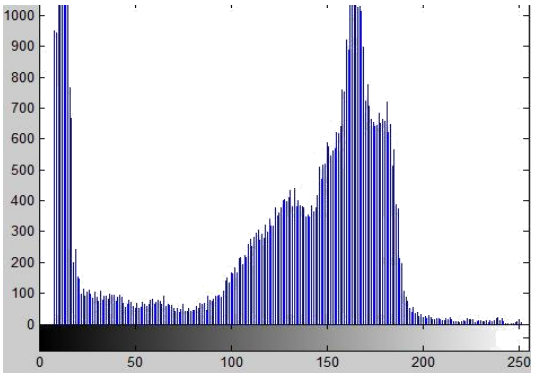

Figure 9: Decrypted Image Histogram

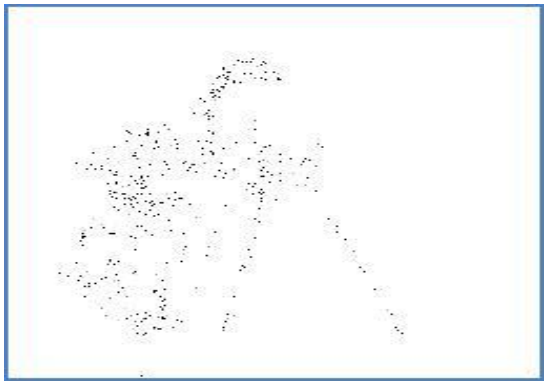

Figure 10: Data Scattered Image under Cover Image

The results shown above are retrieved and analyzed from system modeling under transmission, the system designed and developed are low ubiquity to noise ratio and thus the embedded image v/s SNR is plotted and is shown in Figure 11.

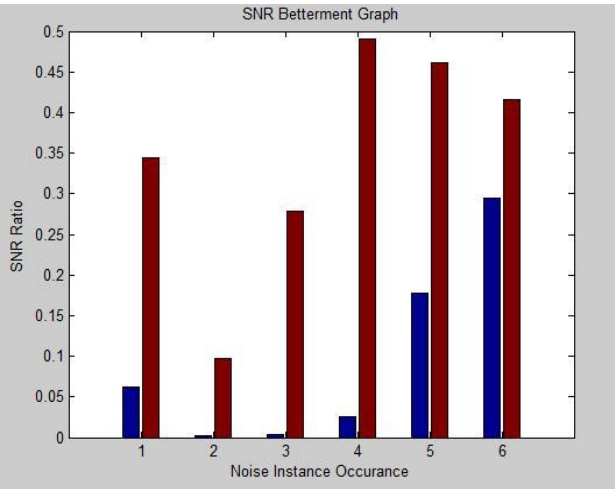

Figure 11: SNR v/s Embedded Image

For a detailed view on analysis, the system has also incorporated clustering results for previous system and current system comparison ratios are shown in Figure 12.

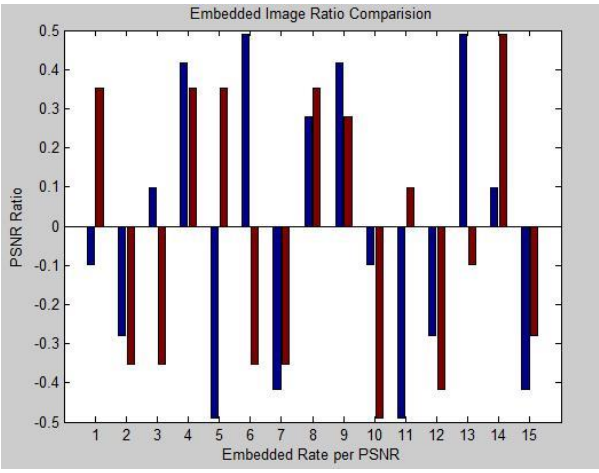

Figure 12: Comparison between previous and current technique.

VII. CONCLUSION AND FUTURE ENHANCEMENT

The proposed system is simulated under a technical standard of retransformation and regeneration of images under reverse encryption modeling. Each image process under this is implemented and correlated under system behavior of SLEPIAN WOLF algorithmic approach. The proposed system successfully fetches the overall protocol of designed and analyzed system, this includes the system embedding the cover and secret images under protocol embedding approach.

The proposed system also has achieved a narrow up parametric value of improvising PSNR and SNR values with respect to embedding rate as shown in early implementation stages. The reverse encryption technique is well suited and performed well in the critical scenarios of data morphing and masking.

Reversible data hiding can be applied to video file or encrypted video file. New technique in reversible data hiding in encrypted images with better PSNR and minimum error along with increasing payload must be found.

REFERENCES

[1] Zhenxing Qian, Xinpeng Zhang, “Reversible data hiding in encrypted images usin destributed source encoding”IEEE 2014-15.
[2] X. Zhang, “Separable reversible data hiding in encrypted image,” IEEE Trans. Inf. Forensics Security, vol. 7, no. 2, pp. 826–832, Apr. 2012.
[3] K. Ma, W. Zhang, et al. “Reversible Data Hiding in Encrypted Images by Reserving Room Before Encryption,” IEEE Trans. Inf. Forensics Security, vol. 8, no. 3, 553-562, 2013.
[4] X. Zhang, G. Feng, Y. Ren and Z. Qian, “Scalable Coding of Encrypted Images,” IEEE Trans. Inform. Forensics Security, vol. 21, no. 6, pp.3108-3114, June 2012.
[5] M. Deng, T. Bianchi, A. Piva, and B. Preneel, “An efficient buyer-seller watermarking protocol based on composite signal representation,” in Proc. 11th ACM Workshop Multimedia and Security, 2009, pp. 9–18
[6] S. Lian, Z. Liu, Z. Ren, and H. Wang, “Commutative encryption and watermarking in video compression,” IEEE Trans. Circuits Syst. Video Technol., vol. 17, no. 6, pp. 774–778, Jun. 2007.
[7] W. Puech, M. Chaumont and O. Strauss, “A reversible data hiding method for encrypted images,” Proc. SPIE 6819, Security, Forensics, Steganography, and Watermarking of Multimedia Contents X, 68191E, Feb. 26, 2008, doi:10.1117/12.766754.
[8] X. Zhang, “Reversible data hiding in encrypted images,” IEEE Signal Process. Lett., vol. 18, no. 4, pp. 255–258, Apr. 2011.
[9] W. Hong, T. Chen, and H. Wu, “An improved reversible data hiding in encrypted images using side match,” IEEE Signal Process. Lett., vol. 19, no. 4, pp. 199–202, Apr. 2012.
[10] M. Johnson, P. Ishwar, V. M. Prabhakaran, D. Schonberg, and K. Ramchandran, “On compressing encrypted data,” IEEE Trans. Signal Process., vol. 52, no. 10, pp. 2992–3006, Oct. 2004.
[11] W. Liu, W. Zeng, L. Dong, and Q. Yao, “Efficient compression of encrypted grayscale images,” IEEE Trans. Image Process., vol. 19, no. 4, pp. 1097–1102, Apr. 2010.
[12] Z. Qian, X. Han and X. Zhang, “Separable Reversible Data hiding in Encrypted Images by n-nary Histogram Modification,” 3rd International Conference on Multimedia Technology (ICMT 2013), pp. 869-876, Guangzhou, China, 2013.
[13] W. Zhang, K. Ma and N. Yu, “Reversibility improved data hiding in encrypted images,” Signal Processing, vol. 94, pp. 118–127, 2014.
[14] Z. Erkin, A. Piva, S. Katzenbeisser, et al., “Protection and retrieval of encrypted multimedia content: When cryptography meets signal processing,” EURASIP Journal on Information Security 2007, 2008.
[15] J. Fridrich and M. Goljan, “Lossless data embedding for all image formats,” in Proc. SPIE Proc. Photonics West, Electronic Imaging, Security and Watermarking of Multimedia Contents, San Jose, CA, USA, Jan. 2002, vol. 4675, pp. 572–583.
[16] J. Tian, “Reversible data embedding using a difference expansion,” IEEE Trans. Circuits Syst. Video Technol., vol. 13, no. 8, pp. 890–896, Aug. 2003.
[17] Z. Ni, Y. Shi, N. Ansari, and S. Wei, “Reversible data hiding,” IEEE Trans. Circuits Syst. Video Technol., vol. 16, no. 3, pp. 354–362, Mar. 2006.