Lossless and Reversible Data Hiding in Encrypted Images with Public Key Cryptography

Zaroon Ul Hakamin[1] . Perseus Mary [2] . Kumar K Kirshnakanth[2]

[1]Faculty of Technology, Prince Mohammad Bin Fahd University, Saudi Arabia.
[2]Faculty of Engineering, University of Arad, Romania.

Received: 21 March 2022 / Revised: 30 April 2022 / Published Online: 10 June 2022

Abstract – Image processing is one of the ever green field for computation and data intelligence under MATLAB environment. In this paper, the authors have discussed on reversible and reliable data hiding. The data is most preferred to be hidden under cover and through this paper, the system has successfully achieved an improved SNR and PSNR under an active transmission channel.

Index Terms – Cryptography, lossless extraction, public key, PKC

I. INTRODUCTION

Cryptography or cryptology is the practice and study of techniques for secure communications the presence of the third parties called adversaries. More generally, cryptography is about constructing and analyzing protocols that prevent third parties or public from reading private messages. Various aspects in information security such as data confidentiality, data integrity, authentication, and non-repudiation are central of modern cryptography. Modern cryptography exists at the intersection of the disciplines of mathematics, computer science, and electrical engineering. Applications of cryptography include ATM cards, computer passwords, and electronic commerce.

Cryptography prior to the modern age was effectively synonymous with encryption, the conversion of information from readable state to apparent nonsense. The originator of an encrypted message shared the decoding needed to recover the original information only with intended recipients, thereby precluding unwanted persons from doing the same. Modern cryptology is heavily based on mathematical theory and computer science practice, cryptography algorithms are designed around computational hardness assumption, making such algorithm hard to break in practice adversary. It is theoretically possible to break such a system, but it is infeasible to do so by any known practical means. These schemes are therefore termed computationally secure, theoretical advances.

The growth of cryptographic technology has raised a number of legal issues in the information age. Cryptography potential for use as a tool for espionage and sedition has led many governments to classify it as a weapon and to limit or even prohibits its use and export. In some cases where use of cryptography is legal, laws permit investigators to compel the disclosure of encryption of keys for documents relevant to an investigation.

II. LITERATURE REVIEWS

In VRAE, the original image is encrypted directly by the sender, and the data-hider embeds the additional bits by modifying some bits of the encrypted data. The idea was first proposed by Puech et al., in which the owner encrypts the original image by Advanced

Encryption Standard (AES), and the data-hider embeds one bit in each block containing n pixels, meaning that the embedding rate is 1/n bit-per-pixel (bpp). On the receiver side, data extraction and image recovery are realized by analyzing the local standard deviation during decryption of the marked encrypted image. This method requires that image decryption and data extraction operations must be done jointly. In other words, extraction and decryption are inseparable.

With a different idea, Zhang proposed a practical RDH method for encrypted images in, in which the data-hider divides the encrypted image into blocks and embeds one bit into each block by flipping three least significant bits (LSB) of half the pixels in the block. On the receiver side, the marked encrypted image is decrypted to an approximate image. The receiver flips the three LSBs of pixels to form a new block. Due to spatial correlation in natural images, original block is presumed to be much smoother than interfered block. Thus the embedded bits can be extracted and the original image recovered jointly. Embedding rate of this method depends on the block size. If an inappropriate block size is chosen, errors may occur during data extraction and image recovery.

To overcome the drawback of inseparability, a separable RDH scheme was proposed for encrypted images. The data-hider pseudo-randomly permutes and divides the encrypted image into groups with size of L. The P LSB-planes of each group are compressed with a matrix G sized (P·L-S)×P·L to generate corresponding vectors. Thus, S bits are available for data embedding. On the receiver side, a total of (8-P) most significant bits (MSB) of pixels are obtained by decryption. The receiver then estimates the P LSBs by the MSBs of neighboring pixels. By comparing the estimated bits with the vectors in the coset Ω corresponding to the extracted vectors, the receiver can recover the original bits of the P LSBs. Because the additional bits are embedded in LSBs of the encrypted images, which can be extracted directly before image recovery, data extraction and image recovery are therefore separable. Besides, this method achieves a better embedding rate. Another separable method was proposed, in which the data-hider embeds additional bits by a histogram shifting and n-nary data hiding scheme, greatly improving the embedding payload as compared.. However, as the original image is encrypted with pixel permutation and affine transformation, leakage of image histogram is inevitable under exhaustive attack.

III. 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 untrusted 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

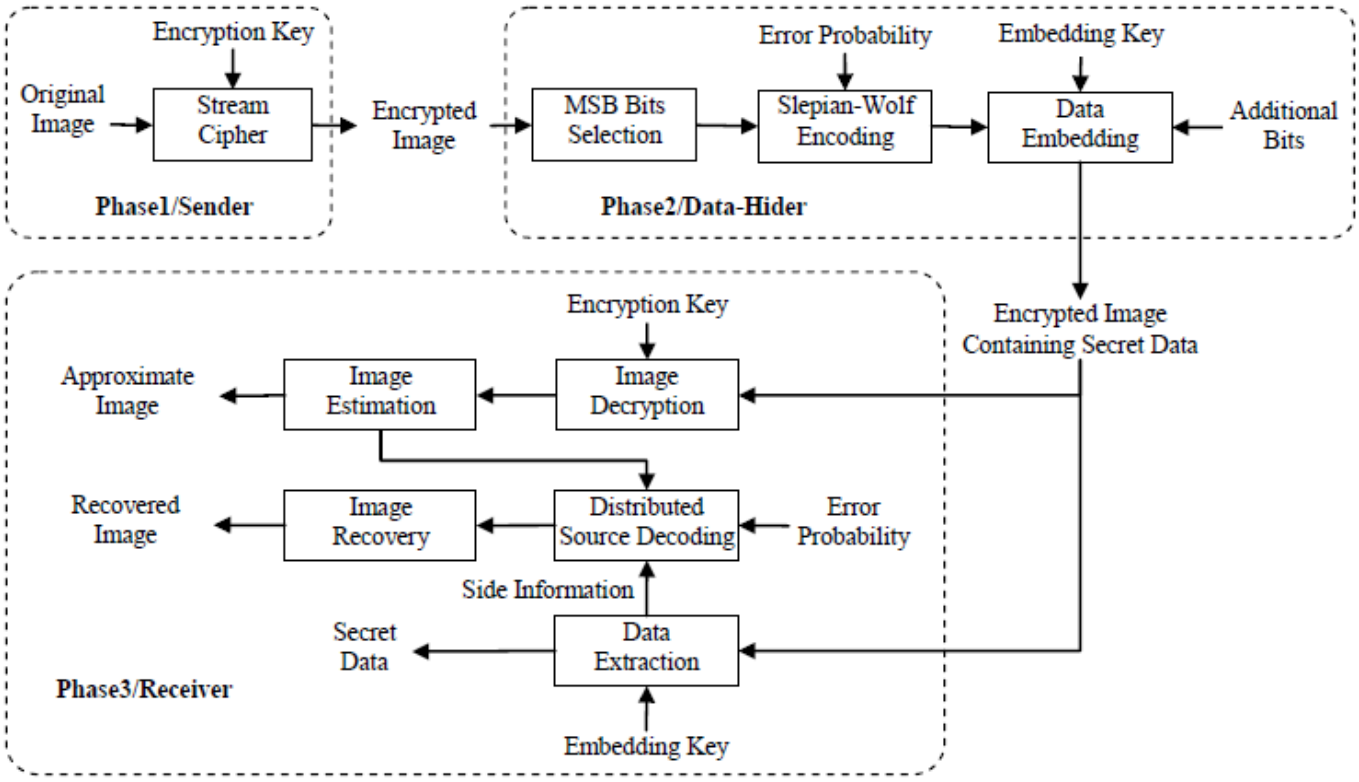

Fig 1: System architecture diagram

IV. 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

Fig 3: secret Image

Fig 2: Cover Image

Fig 4: Embedded Image

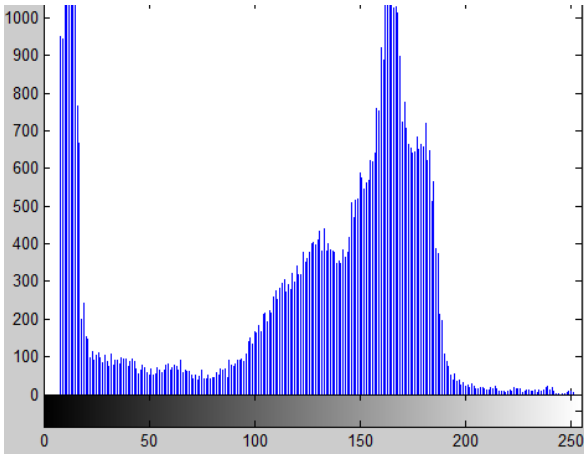

Fig **Fig 5:** Decrypted Image Histogram

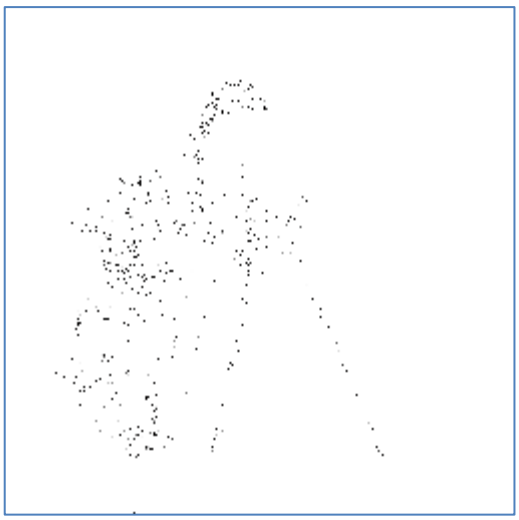

Fig 6: Data Scattered Image under Cover Image

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 Fig 7.

For a detailed view on analysis, the system has also incorporated clustering results for previous system and current system comparison ratios are shown in Fig 8.

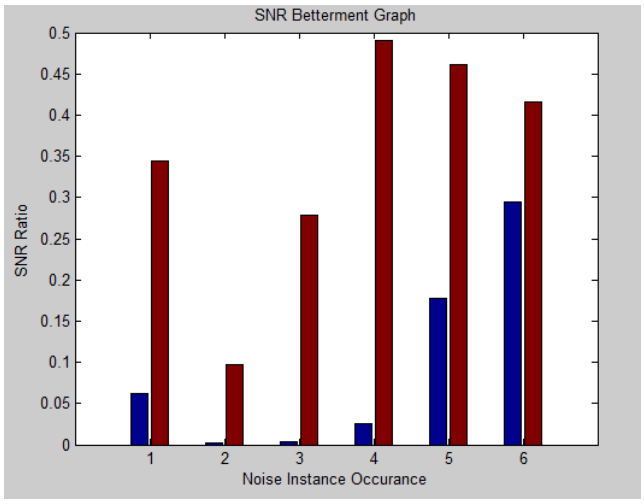

Fig 7: SNR V/s Embedded Image

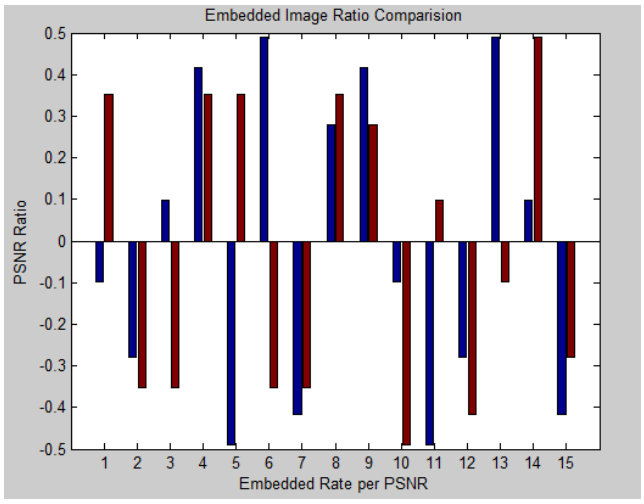

Fig 8: Comparison between previous and current technique.

V. CONCLUSION

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 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.

REFERENCES

1. Erkin, Z., Piva, A., Katzenbeisser, S., Lagendijk, R. L., Shokrollahi, J., Neven, G., & Barni, M. (2007). Protection and retrieval of encrypted multimedia content: When cryptography meets signal processing. *EURASIP Journal on Information Security*, *2007*, 1-20.
2. Liu, W., Zeng, W., Dong, L., & Yao, Q. (2009). Efficient compression of encrypted grayscale images. *IEEE Transactions on Image Processing*, *19*(4), 1097-1102.
3. Zhang, X., Feng, G., Ren, Y., & Qian, Z. (2012). Scalable coding of encrypted images. *IEEE transactions on image processing*, *21*(6), 3108-3114.
4. Deng, M., Bianchi, T., Piva, A., & Preneel, B. (2009, September). An efficient buyer-seller watermarking protocol based on composite signal representation. In *Proceedings of the 11th ACM Workshop on Multimedia and Security* (pp. 9-18).
5. Ahmed, S. S. T., Thanuja, K., Guptha, N. S., & Narasimha, S. (2016, January). Telemedicine approach for remote patient monitoring system using smart phones with an economical hardware kit. In *2016 international conference on computing technologies and intelligent data engineering (ICCTIDE'16)* (pp. 1-4). IEEE.
6. Lian, S., Liu, Z., Ren, Z., & Wang, H. (2007). Commutative encryption and watermarking in video compression. *IEEE Transactions on Circuits and Systems for Video Technology*, *17*(6), 774-778.
7. Puech, W., Chaumont, M., & Strauss, O. (2008, March). A reversible data hiding method for encrypted images. In *Security, forensics, steganography, and watermarking of multimedia contents X* (Vol. 6819, pp. 534-542). SPIE.
8. Zhang, X., Long, J., Wang, Z., & Cheng, H. (2015). Lossless and reversible data hiding in encrypted images with public-key cryptography. *IEEE Transactions on Circuits and Systems for Video Technology*, *26*(9), 1622-1631.
9. Zhang, W., Ma, K., & Yu, N. (2014). Reversibility improved data hiding in encrypted images. *Signal Processing*, *94*, 118-127.
10. Kalker, T. O. N., & Willems, F. M. (2002, July). Capacity bounds and constructions for reversible data-hiding. In *2002 14th International Conference on Digital Signal Processing Proceedings. DSP 2002 (Cat. No. 02TH8628)* (Vol. 1, pp. 71-76). IEEE..