Data Hiding and Retrieval on Image using MSB Encoding Technique

Abhishek Dahale[1] Mayur Khairnar[2] Sameer Vaidya[3] Tanmay Kale[4] Mr. S. V. Dhande[5]
[1,2,3,4,5]Department of Computer Engineering
[1,2,3,4,5]Smt. Kashibai Navale College of Engineering Pune 411041

Abstract— This paper proposes a technique in which we use a distributed source encoding on encrypted images for hiding the data. Reversible data hiding is technique in which data in the cover image can reversibly retrieved after extracting the hidden data .Here we encrypt the image using stream cipher. After the series of bits is selected, the data hider compresses this selected bits using Slepian-Wolf encoding. If the receiver has embedding key as well as encryption key, only then the original data and image is recovered perfectly using distributed source decoding.

Key words: Image Encryption, Image Recovery, Reversible Data Hiding

I. INTRODUCTION

Sometimes there is possibility of confidential data getting hacked during the data transfer like government data, military communications, private images and passwords. While data transfer we need to maintain secure connection and its reliability but sometimes it is difficult to provide such requirements. So we provide reversible data hiding technique using two different keys.

A. Motivation

As we are in 21st century, technology is evolving day by day and internet has covered almost all the communication areas. Along with technology cybercrimes and data hacking cases are increasing rapidly. To avoid such crimes and secure the data some additional measures should be taken which motivates this project idea.

II. LITERATURE SURVEY

RDH for encrypted image are usually designed for the applications in which the data-hider and the image owner are not the same party. The data-hider cannot access the image content, and the secret message is held by the data-hider. Thus, encryption is done by the sender, hiding by the data-hider, and data extraction and/or image reconstruction by the receiver. Existing RDH methods for encrypted images can be classified into two categories: vacating room after encryption (VRAE) and vacating room before encryption (VRBE).

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.

III. PROPOSED SYSTEM

Proposed system consists of three phases image encryption, data embedding, and data extraction/image recovery. In phase I, the sender encrypts the original image into an encrypted image using a stream cipher and an encryption key.In phase II, the data-hider selects and compresses some MSB of the secret image using LDPC codes to generate a spare space, and embeds additional bits into the encrypted image using an embedding key. In phase III, the receiver extracts the secret bits using the embedding key. If he/she has the encryption key, the original image can be approximately reconstructed via image decryption and estimation. When both the encryption and embedding keys are available, the receiver can extract the compressed bits, and implement the distributed source decoding using the estimated image as side information to perfectly recover the original image.

A. Advantages of Proposed System

This method can achieve real reversibility, that is, data extraction and image recovery are free of any error. It is easy for the data hider to reversibly embed data in the encrypted image.
Lesser Error Probability than existing system.

IV. ARCHITECTURAL DESIGN

A description of the program architecture is presented. Subsystem design or Block diagram, Package Diagram, Deployment diagram with description is to be presented.

A. Architectural Design

A description of the program architecture is presented. Subsystem design or Block diagram, Package Diagram, Deployment diagram with description is to be presented.
Phase 1:
Sender encrypts the Input image into encrypted image using a stream cipher and an encryption key.
Phase 2:
Data hider selects bits and compress some MSB of the secrete image using LOPC codes to generate sparse space and embeds additional bits into the encrypted image using embedding key.
Phase 3
The receiver enters the secrete bits using an embedding key. If user has encryption key the input image can be approximately reconstructed via image decryption available the receiver can extract the compressed bits and side into to perfectly recover the input image.

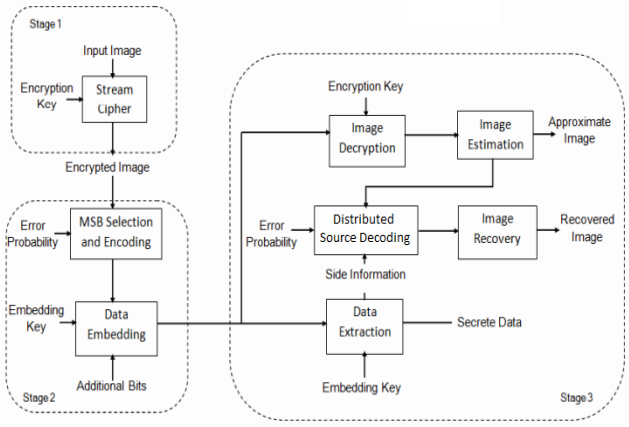

Fig. 1: Architecture

All rights reserved by www.ijsrd.com

V. FUTURE SCOPE

Many times it is observed that patient doesn't want to expose or share his private reports. such information is regularly communicated between the corresponding doctor and the patient which might be used for further assistance, so communication can be performed reliably using the proposed system. Also many times security agencies or military officials transfer very crucial information to from different locations which may contain details like troop count, their locations or data of arsenal and operation plans and agent's information. To avoid damage to this information while transfer, RDH will be an effective and secure approach. Apart from medical and military fields the system can also secure communications of industries. These communications may include purchase and expenses information, research topics and its progress details, design of any new model should not be exposed or stolen by other competitors.

VI. CONCLUSION

This paper proposes a scheme of Distributed source encoding on encrypted image using reversible data hiding. After encrypting the original image, some bits of MSB planes are selected and compressed. Whereas, on the receiver side, all hidden data can be recollected with the embedding key only, and the approximate original image can be recovered with high quality using the encryption key only. The hidden data can be extracted completely as well perfectly by using both embedding and encryption keys. As compared with the existing VRAE methods the proposed system substantially increases the payload using DSC. As embedding operations are performed to the encrypted data, the data-hider cannot access the contents of the original image. That ensures safety of the secrets in data hiding. We cannot decrypt the data and image without using these keys.

ACKNOWLEDGMENTS

I express my gratitude to all those who have provided me with valuable guidance towards the completion of this system as part of the syllabus of the Bachelor of Engineering course. I express our sincere gratitude towards co-operative department who have provided us with valuable assistance and requirements for the system development.

REFERENCES

[1] Zhenxing Qian, Xinpeng Zhang, Reversible Data Hiding in Encrypted Image with Distributed Source Encoding, IEEE Trans. Circuit and Systems for Video Technology, 2014-15.
[2] W. Liu, W. Zeng, L. Dong, and Q. Yao, Efficient compression of encrypted grayscale images, IEEE Trans. Image Process., vol. 19, no. 4, pp. 10971102, Apr. 2010.SS.
[3] 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.
[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] 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. 199202, Apr. 2012.
[6] M. Johnson, P. Ishwar, V. M. Prabhakaran, D. Schonberg, and K. Ram-chandran, On compressing encrypted data, IEEE Trans. Signal Process., vol.52, no. 10, pp. 29923006, Oct. 2004.

All rights reserved by *www.ijsrd.com*