OPEN ACCESS INTERNATIONAL JOURNAL OF SCIENCE & ENGINEERING

SURVEY ON SEPARABLE REVERSIBLE DATA HIDING FOR ENCRYPTED PALETTE IMAGES WITH COLOR PARTITIONING AND FLIPPING VERIFICATION TECHNIQUES

Priyanka Ugale[1], Prof. S. M. Rokade[2]

PG Student, Department of Computer Engineering, S. V. I. T. Nashik[1]
Assistant Professor, Department of Computer Engineering, S. V. I. T. Nashik[2]
ugalepriya@gmail.com[1], smrokade@yahoo.com[2]

Abstract: **The system focus on Separable Reversible Data Hiding for Encrypted Palette Images with Color Partitioning and Flipping Verification. Reversible data hiding (RDH) into encrypted images is of increasing attention to researchers as the original content can be perfectly reconstructed after the embedded data are extracted while the content owner's privacy remains protected. The proposed method adopts a color partitioning method to use the palette colors to construct a certain number of embeddable color-triples, whose indexes are self-embedded into the encrypted image so that a data hider can collect the usable color-triples to embed the secret data. By using the encryption key, the receiver can roughly reconstruct the image content. Experiments have shown that, our proposed method has the property that the presented data extraction and image recovery are separable and reversible. Our proposed method can provide a relatively high data-embedding payload, maintain high PSNR values of the decrypted and marked images, and have a low computational complexity.**

Keyword: Security, Smartphone, Secret Question

---∴∴∴---

I INTRODUCTION

Encryption of images by using the flipped verification with the data hiding key the original image can encrypted and extracted at the receiver side and the contents of that owner privacy remains secured. The palette image is used as an input for the encryption of image by using the encrypted key. In the image changes are done by using the color partition with RGB model. After the encryption of image some data is hidden. For a receiver the encrypted image is received by using the data hiding key and then after the image extracted the original image is gain.

II LITERATURE SURVEY

[1] Xinpeng Zhang, "Separable Reversible Data Hiding in Encrypted Image".

In this paper, a novel scheme for separable reversible data hiding in encrypted image is proposed, which consists of image encryption, data embedding and data-extraction/image-recovery phases. In the first phase, the content owner encrypts the original uncompressed image using an encryption key. Although a data-hider does not know the original content, he can compress the least significant bits of the encrypted image using a data-hiding key to create a sparse space to accommodate the additional data. With an encrypted image containing additional data, the receiver may extract the additional data using only the data-hiding key, or obtain an image similar to the original one using only the encryption key. When the receiver has both of the keys, he can extract the additional data and recover the original content without any error by exploiting the spatial correlation in natural image if the amount of additional data is not too large. If the lossless compression method in is used for the encrypted image containing embedded data, the additional data can be still extracted and the original content can be also recovered since the lossless compression does not change the content of the

encrypted image containing embedded data. However, the lossy compression method in compatible with encrypted images generated by pixel permutation is not suitable here since the encryption is performed by bit-XOR operation. In the future, a comprehensive combination of image encryption and data hiding compatible with lossy compression deserves further investigation.

[2] Wei-Liang Tai and Ya-Fen Chang, "Separable Reversible Data Hiding in Encrypted Signals with Public Key Cryptography".

This paper proposes a separate RDH method for images encrypted by public key cryptography. The two cipher text values are exchanged with each other for embedding the additional data. Based on additive homomorphic properties, we can directly extract the embedded data from the encrypted domain without knowing the original content. Moreover, perfect image recovery can be directly processed without prior data extraction. Since the content privacy can be securely preserved processed without prior data extraction. Since the content privacy can be securely preserved by Paillier encryption, the proposed scheme is appropriate for cloud services without degrading the security level.

[3] Dawen Xu, Kai Chen, Rangding Wang, and Shubing Su, "Separable Reversible Data Hiding in Encrypted Images Based on Two-Dimensional Histogram Modification".

In this paper, an algorithm to reversibly embed secret data in encrypted images is presented. A specific modulo operation is utilized to encrypt the image, which can preserve some correlation between the neighboring pixels. With the preserved correlation, the data hider can embed the secret data into the encrypted image by using 2D histogram modification, even though he does not know the original image content. Since the embedding process is done on encrypted data, our scheme preserves the confidentiality of content. Data extraction is separable from image decryption; that is, the additional data can be extracted either in the encrypted domain or in the decrypted domain. Furthermore, this algorithm can achieve real reversibility and high quality of marked and decrypted images. One of the possible applications of this method is image annotation in cloud computing where high image quality and reversibility are greatly desired.

[4] M. Hassan Najafi and David J. Lilja, "A High-Capacity Separable Reversible Method for Hiding Multiple Messages in Encrypted Images".

In this paper we proposed a high capacity, separable, RDH method for encrypted images which consists of image preprocessing, image encryption, data embedding, and data-extraction/image reconstruction phases. In the first phase, the image is processed to identify the unpredictable pixels and define and embedding frame. The content owner then encrypts the original image using an encryption key. One or several data hiders permute some pre specified pixels in the embedding frame of the encrypted image using their embedding keys. Each data hider uses the MSB of the assigned pixels in the encrypted image to embed an encrypted version of an additional data stream. In the data embedding phase, the data hider does not necessarily know the original content. At the receiver side, with an encrypted image containing additional data, there will be two different cases. When the receiver has one or some of the data embedding keys, the corresponding embedded data that are encrypted and hidden inside the encrypted image can be extracted. If the receiver has the encryption key, the embedded data cannot be extracted without knowing the embedding keys, but the received data can still be directly decrypted and the original image reconstructed without any errors. The receiver does not need the embedding key(s) to recover the original image perfectly even with high embedding rates.

III PROPOSED SYSTEM

The proposed scheme is made up of image encryption, data embedding and data-extraction/image-recovery phases.

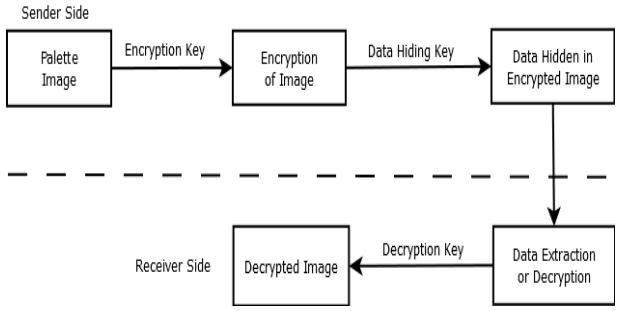

Figure 1: System Architecture

The content owner encrypts the original uncompressed image using an encryption key to produce an encrypted image. Then, the data-hider compresses the least significant bits (LSB) of the encrypted image using a data-hiding key to create a sparse space to accommodate the additional data. At the receiver side, the data embedded in the created space can be easily retrieved from the encrypted image containing additional data according to the data-hiding key. Since the data embedding only affects the LSB, a decryption with the encryption key can result in an image similar to the original version. When using both of the encryption and data-hiding keys, the embedded additional data can be successfully extracted and the original image can be perfectly recovered by exploiting the spatial correlation in natural image.

IV GOALS

By using the data hiding key and encryption key at Receiver side we can get the original Image.

V OBJECTIVES

To provide the security for transmission of image between sender and receiver.
To encrypt the image with data hiding.
To decrypt the received image and to check the authenticity of the image.
To recover the modified image.

VI CONCLUSION

In this paper, a novel scheme for separable reversible data hiding in encrypted image is proposed, which consists of image encryption, data embedding and data-extraction / image-recovery phases. In the first phase, the content owner encrypts the original uncompressed image using an encryption key. Although a data-hider does not know the original content, he can compress the least significant bits of the encrypted image using a data-hiding key to create a sparse space to accommodate the additional data. With an encrypted image containing additional data, the receiver may extract the additional data using only the data-hiding key, or obtain an image similar to the original one using only the encryption key. When the receiver has both of the keys, he can extract the additional data and recover the original content without any error by exploiting the spatial correlation in natural image if the amount of additional data is not too large. If the lossless compression method in [1] or [2] is used for the encrypted image containing embedded data, the additional data can be still extracted and the original content can be also recovered since the lossless compression does not change the content of the encrypted image containing embedded data. However, the loss compression method in [3] compatible with encrypted images generated by pixel permutation is not suitable here since the encryption is performed by bit-XOR operation. In the future, a comprehensive combination of image encryption and data hiding compatible with loss compression deserves further investigation.

REFERENCES

[1] Xinpeng Zhang, "Separable Reversible Data Hiding in Encrypted Image", IEEE, Transactions On Information Forensics And Security, Vol. 7, No. 2, April 2012.
[2] Wei-Liang Tai and Ya-Fen Chang, "Separable Reversible Data Hiding in Encrypted Signals with Public Key Cryptography", 2018.
[3] Dawen Xu, Kai Chen, Rangding Wang, and Shubing Su, "Separable Reversible Data Hiding in Encrypted Images Based on Two-Dimensional Histogram Modification", Security and Communication Networks Volume, 2018.
[4] M. Hassan Najafi and David J. Lilja, "A High-Capacity Separable Reversible Method for Hiding Multiple Messages in Encrypted Images".
Sensing System", 2016.