WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Privacy Preserving on Data using Reversible Data Hiding

Manikandan[1], Niranjan[2], Sakthivel[3], ProfVennila[4]

[1]EGS Pillay Engineering College (Autonomous), Nagapattinam, Tamilnadu, IndiaE-Mail:manikandan73@gmail.com
[2]EGS Pillay Engineering College (Autonomous), Nagapattinam, Tamilnadu, IndiaE-Mail:niranjanniranjan0019*@gmail.com*
[3]EGS Pillay Engineering College (Autonomous), Nagapattinam, Tamilnadu, IndiaE-Mail:*lsakthivel334@gmail.com*
[4]Assistant professor, EGS Pillay Engineering College (Autonomous), Nagapattinam, Tamilnadu, IndiaE-Mail:*vennila@egspec.org*

ABSTRACT

Reversible data hiding in encrypted images (RDHEI) is a useful data security approach. The majority of current RDHEI approaches do not yet produce a suitable payload. We present a new RDHEI approach with hierarchical embedding to solve this problem. There are two ways in which we can help. For the bit-planes of plaintext images, a novel hierarchical label map generating technique is proposed. The hierarchical label mappings are created using a prediction algorithm and compressed before being placed in the encrypted image. This embedding strategy hierarchically splits prediction mistakes into three types: small-magnitude, medium-magnitude, and large-magnitude, which are each labelled differently, in order to attain a high embedding payload. In the hierarchical embedding technique, pixels with small magnitude/large magnitude prediction errors are both employed to accommodate hidden bits, and so contribute a high embedding payload, in contrast to conventional techniques. The suggested RDHEI approach is validated through experiments on two standard datasets. In terms of payload, the findings show that the suggested RDHEI method beats some state-of-the-art RDHEI methods. For the BOWS-2 dataset and the BOSS base dataset, the proposed RDHEI method's average payloads are 3.4568 bpp and 3.6823 bpp, respectively.

Keywords: Reversible data hiding, Encrypted images, Lossless compression, Hierarchical embedding, High payload.

INTRODUCTION

Data hiding and data encryption are two useful ways for protecting multimedia data. The focus of this research is on data concealing techniques. The cover image and secret data are the two components of the data concealment mechanism. The goal of traditional data concealment is to integrate hidden information into a cover image with little distortion. It focuses on correct data extraction but ignores the recovery of the original cover image. However, the original cover image must be restored without error in particular applications, such as medical image processing and law enforcement. To meet this need, reversible data hiding (RDH) is presented, which allows both hidden data and the cover image to be recovered without difficulty. Lossless compression, difference expansion (DE), histogram shifting (HS), and prediction error expansion(PEE) are the most common RDH techniques. To embed hidden data, such as statistical or prediction mistakes of pixel pairs, these RDH methods typically use spatial correlation among local pixels. These techniques are suitable for plaintext photographs;however, they are not good for encrypted images due to the uncorrelated pixels in encrypted images. Researchers have proposed RDH methods for the use of encrypted photos in recent years. RDH in encrypted image (RDHEI) is a technique that tries to safeguard both the original photos and the secret data at the same time. Content-owner, data-hider, and receiver are the three users in RDHEI. A content owner encrypts the original image and uploads it to the server using the encryption key. The data-hider embeds secret data into the encrypted image using the data-hiding key, and without the encryption key, he or she cannot access the original image content. Under specific authority, the receiver can access the original image, secret data, or both. There are primarily two RDHEI frameworks: reserving room before encryption and encryption before reserving room.

METHODOLOGY

First, we present a new RDHEI approach based on hierarchical embedding that can conduct data extraction and image recovery without error in this project. The suggested approach has three stages,

1) Image encryption is performed by the content owner using an encryption key

2) Data hiding is performed by the data hider using a data-hiding key

3) Data extraction and image decryption are performed by the receiver.

Before picture encryption, a label map for each bit-plane of the original image is created hierarchically from the 8th bit-plane to the 2nd bit-plane, and this label map is also known as bit-plane label map. Following encryption, each bit-plane label map is compressed using arithmetic coding to reduce its size, and the compressed version is then inserted into the encrypted image's associated bit-plane. Secret bits are hierarchically embedded into bit-planes of the encrypted picture from the 8th bit-plane to the 2nd bit-plane using a bit replacement technique based on bit-plane label mappings during the embedding stage. Finally, using the data-hiding key and encryption key, data extraction and image recovery may be done individually, and the extracted data and restored image are both error-free.

Inthisdatahiding and image Encrypted system,thebelowmethodsareused:

- Image Encryption
- Image Decryption
- Data Extraction
- Data Embedding

MODELINGANDANALYSIS

Our goal is to design a system where an unauthorized user cannot access the original image or secret data in RDH-EI. As a result, both the original image and the secret data must be safeguarded. A stream cypher is used to modify the bits in order to safeguard the secret data. It is incredibly impossible to divulge the secret data without the data hiding key. To encrypt the image, a pseudo-random matrix created by PRNG is employed. To verify the security level, a statistical analysis of histogram is used. In general, an image's histogram depicts the distribution of pixels based on intensity values. In comparison to the original image, the histograms of the encrypted image created with our method are evenly distributed. It's impossible to use them to get information about the image's original content. In addition, the original images' histogram statistics and the associated encrypted images' histogram statistics. The following figure 1. describes the Privacy Preserving on Data Using Reversible Data Hiding process.

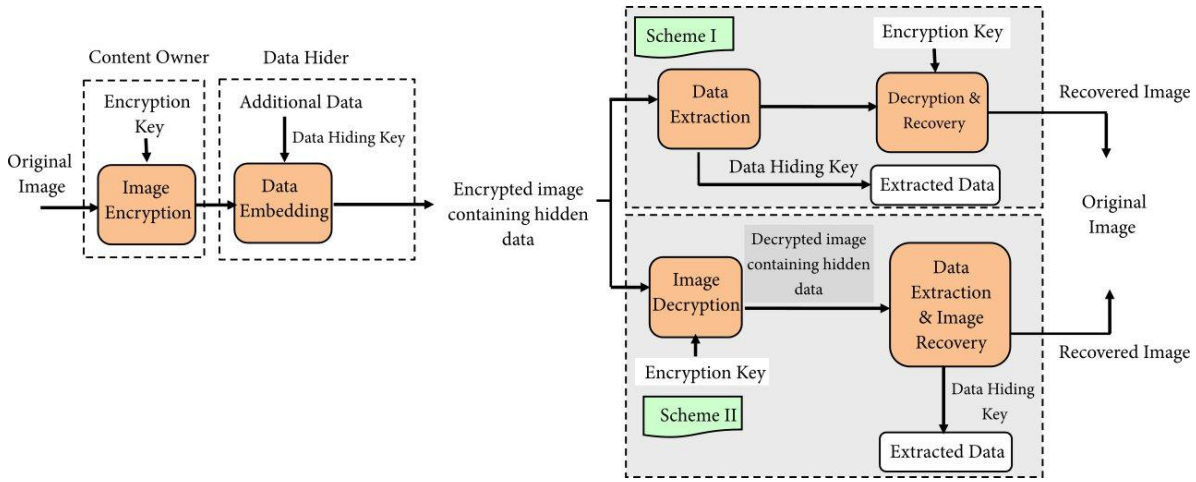

Figure 1. Process of Privacy Preserving on Data using Reversible Data Hiding

Objective

- Image encryption, data embedding in encrypted image.
- Providesthealertsystematthetimeofunauthorizedsystemaccess.
- Creating an encrypted framework for data.

RESULTS AND DISCUSSION

1. A specific modulo operation is utilized to encrypt the image.
2. Asaresult,the data-hider can embed the additional data into the encrypted image by using difference histogram modification.
3. Experimental results show that the visual quality of marked decryptedimage is ery high.
4. As a result, Data extraction is separable from image decryption Proposed System.

It is possible to extract data and recover images without losing quality. However, prior to encrypting the image, histogram shifting should be performed. Our technique, on the other hand, directly encrypts the image, which is more sensible.

Data FlowDiagram

Thebelowfigure2 and 3describestheDataflow ofdata hidingsystem using reversible data hiding method.

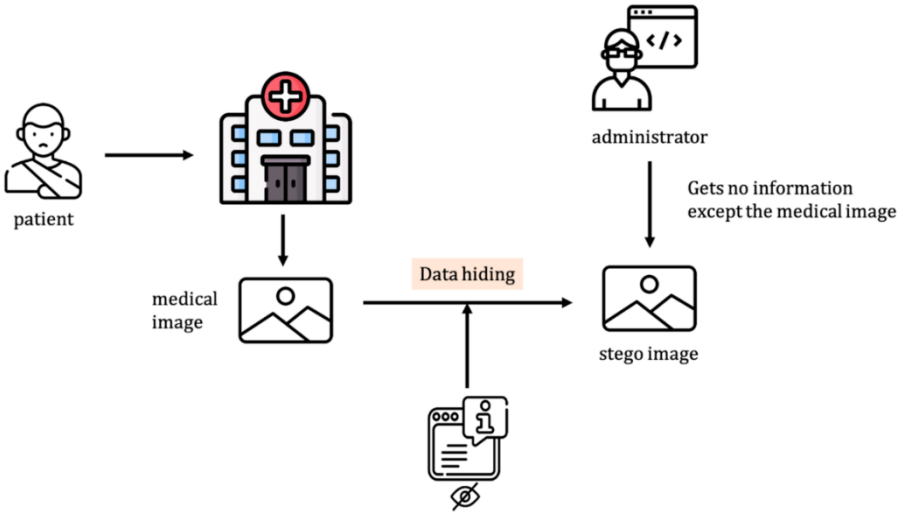

Figure2.Dataflow Based ReversibleData Hiding for Medical Imagesystem.

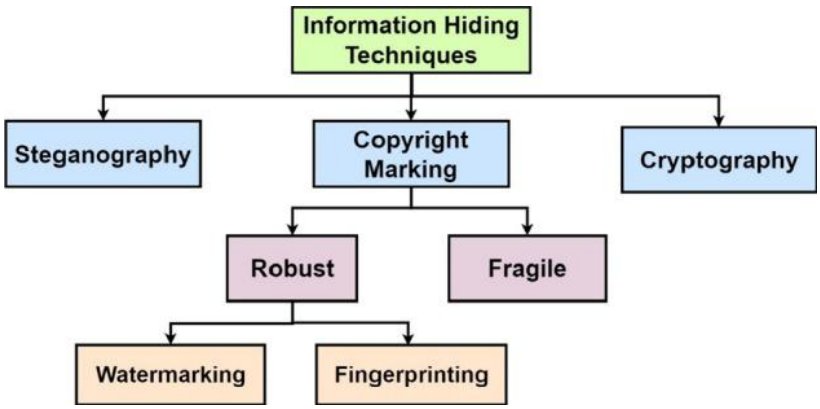

Figure3.Processof Bio-Signal Data Sharing Security

CONCLUSION

An effective framework for RDH-EI is described in this data hiding method. To encrypt the image, a special modulo operation is used, which preserves some association between neighbouring pixels. Using differential histogram modification and the preserved correlation, the data-hider can insert the additional data within the encrypted image. Our technique protects content secrecy because the embedding procedure is done on encrypted data. Data extraction can be done apart from picture decryption, which means that the extra data can be extracted in either the encrypted or decrypted domain. The visual quality of the designated decrypted image is quite high, and the resulting payload is sufficient to embed some more data, according to experimental results. True reversibility, on the other hand, can be achieved, implying that the secret data and original image can be restored without error.

REFERENCES

[01] Z. Tang, S. Xu, H. Yao, C. Qin, and X. Zhang, "Reversible data hiding with differential compression in encrypted image," Multimedia Tools Appl., vol. 78, no. 8, pp. 9691–9715, Apr. 2019.

[02] Y. Fu, P. Kong, H. Yao, Z. Tang, and C. Qin, "Effective reversible data hiding in encrypted image with adaptive encoding strategy," Inf. Sci., vol. 494, pp. 21–36, Aug. 2019.

[03] Z.-L. Liu and C.-M. Pun, "Reversible data-hiding in encrypted images by redundant space transfer," Inf. Sci., vols. 433–434, pp. 188–203, Apr. 2018.

[04] C. Qin, X. Qian, W. Hong, and X. Zhang, "An efficient coding scheme for reversible data hiding in encrypted image with redundancy transfer," Inf. Sci., vol. 487, pp. 176–192, Jun. 2019.

[05] S. Yi and Y. Zhou, "Separable and reversible data hiding in encrypted images using parametric binary tree labeling," IEEE Trans. Multimedia, vol. 21, no. 1, pp. 51–64, Jan. 2019.

[06] P. Puteaux and W. Puech, "An efficient MSB prediction-based method for high-capacity reversible data hiding in encrypted images," IEEE Trans. Inf. Forensics Security, vol. 13, no. 7, pp. 1670–1681, Jul. 2018.

[07] Z. Yin, Y. Xiang, and X. Zhang, "Reversible data hiding in encrypted images based on multi-MSB prediction and Huffman coding," IEEE Trans. Multimedia, vol. 22, no. 4, pp. 874–884, Apr. 2020.

[08] Y. Wu, Y. Xiang, Y. Guo, J. Tang, and Z. Yin, "An improved reversible data hiding in encrypted images using parametric binary tree labeling," IEEE Trans. Multimedia, vol. 22, no. 8, pp. 1929–1938, Aug. 2020.

[09] P. Puteaux and W. Puech, "A recursive reversible data hiding in encrypted images method with a very high payload," IEEE Trans. Multimedia, vol. 23, pp. 636–650, 2021.