IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Reversible Image Data Hiding in Encrypted Images by MSB Prediction with Embedded Prediction Errors

[1]Ashish Abraham, [2]M. Ravikumar, [3] Dr. D. Chitra

[1]P.G Student, [2]Assistant Professor, [3]Associate Professor

[1]Department of Electronics and Communication Engineering,

[1]Mahendra engineering College (Autonomous), Mahendhirapuri, Mallasamudram, Namakkal, India

Abstract: Data Privacy has received considerable attention in all fields. In the last few years, data and visual privacy has become a major problem. Because of this, Reversible Data Hiding (RDH) in the encrypted image has a lot of attention from the communities of privacy, security, and protection. This paper presents highly efficient reversible data hiding in the encrypted image by the MSB prediction method. In this method, RDH is a process to embedded useful data into a cover media or encrypted image using MSB prediction. Here we present High-Capacity Reversible Data Hiding on MSBs with embedded prediction errors (EPE – MHCRDH) approach.

Index Terms **- Data Privacy, MSB prediction, Reversible Data Hiding, Prediction Error**

I. INTRODUCTION

Now a day's digital media is being immensely used in various type of applications such as medical, military, law enforcement, fine art work protection and so on. Security is the main concern which is to be taken care of while transferring confidential data on the Internet. Since text, images, audio, video are the part of digital data that are transferred over open public network so there is need to protect this digital data. From the last few decades, various methods have been developed to enforce security in various types of applications. Generally, two methods are used to secure the data i.e., cryptography and data hiding [13].

Cryptography is the art of secret writing. This is achieved by scrambling the secret information and the scrambled information is unscrambled only by some key or some program. Cryptography emphasis on data integrity, data confidentiality, authentication, non-repudiation of data etc. Data hiding is the art of hiding secret information in cover media without any perceptual distortion of the cover media [15].

Data hiding is form of subliminal communication which uses a variety of multimedia as a cover media and embeds the secret information into this media to generate marked media [14]-[12]. Data hiding techniques used for copyright protection, temper detection, covert communication, data integrity etc.

II. PRINCIPLE OF DATA HIDING

Embedding process and extracting process are the two main processes of data hiding. In embedding process, secret data is embedded into cover media. Cover media is modified after embedding the secret data. This modified cover media which contain secret data is known as marked data. Secret data is extracted from the marked data and recovers the original cover media.

A reversible data hiding is an approach, which can recover the original image loss lesly after the data have been extracted from the cover image. Reversible Information Implanting, which can be called lossless information installing, inserts secret information (which is known as a payload) into a computerized picture in a reversible way. As an essential necessity, the quality corruption on the spread picture after information installing ought to be low. A fascinating component of reversible information installing is its reversibility, that is, one can expel the implanted information to re-establish the first picture.

Figure 3 The reason behind for hiding data is to avoid the misuse of data, hide traces of crime, military information, blackmail purpose, personal and private data etc.

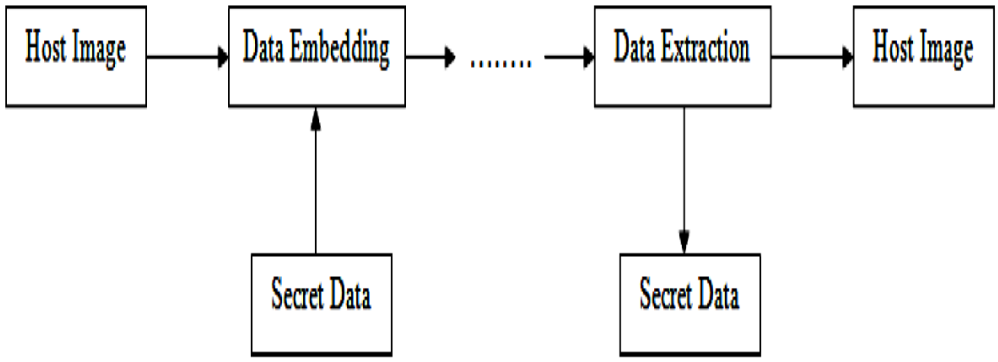

Fig -1: General Block Diagram of RDH

Reversible Data Hiding in Encrypted Images Using Side Match [6] is the good technique but the greatest challenge is that it has poor reconstructed image quality when the payload is high. A side-match mechanism is also introduced to evaluate the smoothness and uses the side-match scheme to further decrease the error rate of extracted-bits. None of the existing methods succeed in combining high embedding capacity and high visual quality. For this reason, we propose to use the MSB values instead of the LSB values to embed the hidden message. With this approach, in the encrypted domain, confidentiality is still the same and decryption is easier than previous methods.

In this work introduces an effective approach for Data Hiding in Encrypted domain. It is embedding the secret message by two-bit MSB substitution. In this plan utilizes two strategies for reversible information covering up, i.e., CPE – MHCRDH. The proposed scheme provides a good security level and can be used to preserve the original image content confidentiality, while offering authenticity or integrity. It improves the reconstructed image quality as well as the embedding capacity.

III. PROPOSED METHOD

In this method the original image is directly encrypted, but after the encryption step, the location of the prediction errors is embedded (EPE). During the data hiding phase, in both approaches, the MSB of each available pixel is substituted in the encrypted image by 2 bit of the secret message that embedded image can be loss less compressed. At the end of the process, the data embedded image can decompress and the embedded data can be extracted without any errors and the clear image can be reconstructed loss less by using MSB prediction as shown in fig 2

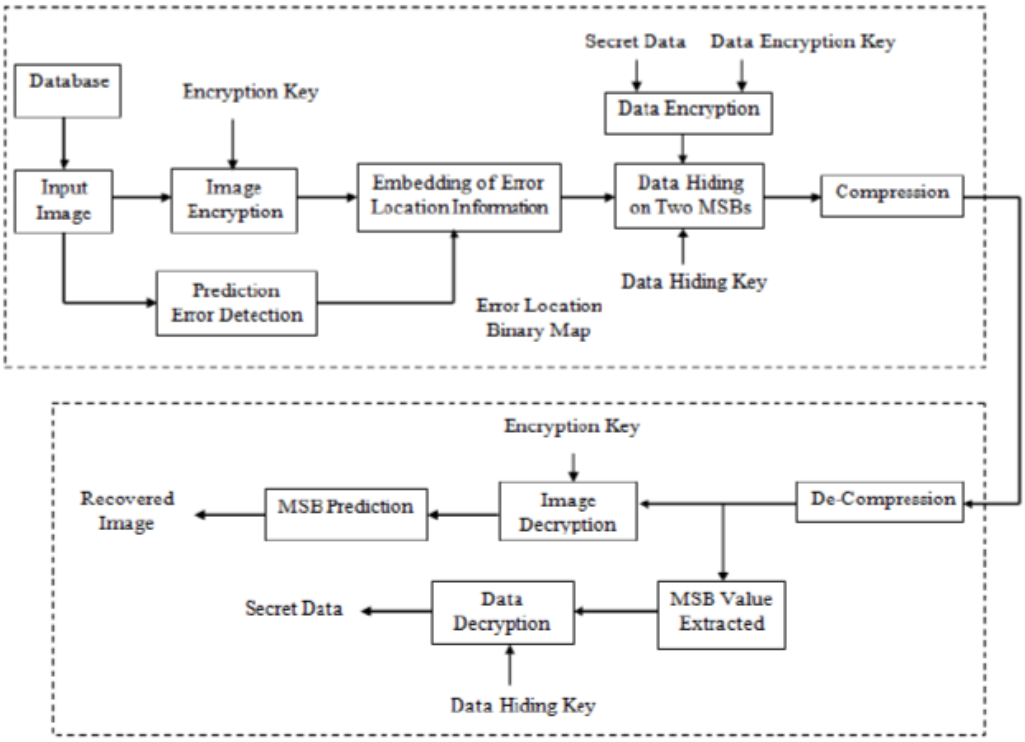

Fig -2: Block Diagram of Proposed EPE – MHCRDH

The encoding phase consists of four steps: the prediction error detection, the encryption, the embedding of the error location map and the reversible data hiding by MSB substitution.

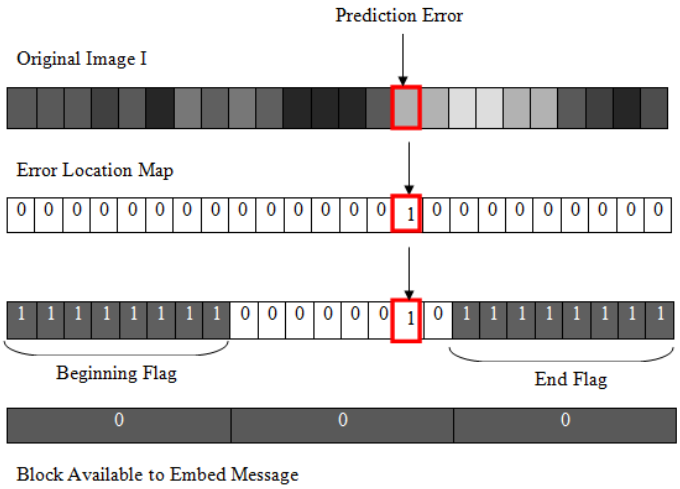

Fig -3: Finding Available Block for Data Hiding

During prediction error detection [1], the location of the prediction errors is stored in the error location binary map. Then, the original image I is encrypted by using equation

$$P_e(i,j) = s(i,j) \oplus p(i,j)$$

Before the embedding step, the encrypted image Pe is adapted to avoid prediction errors. The encrypted image Pe is then divided into blocks of eight pixels and scanned, block by block, in the scan line order. If at least one prediction error is identified in a block according to the error location binary map, the current block is surrounded by two flags by replacing the MSB of each pixel in the previous and the following blocks by 1

In this phase, three cases are considered: (1) the recipient has only the data hiding key, (2) the recipient has only the encryption key and (3) the recipient has both the encryption and the watermarking keys. In the first case, the recipient can extract the secret message by following these steps

1. The pixels of the decompressed image are scanned in the scan line order and for each pixel; the MSB value is extracted, according to below equation and stored. Before the first sequence of eight MSB equal to 1, the extracted values are bits of the embedded message.

$$b_T = p_{data}(i,j)/128$$

2. When such a sequence is encountered, it indicates the beginning of an error sequence: the next pixels were not marked during the data hiding step. So, scan pixels until the next sequence of eight MSB equal to 1, which indicates the end of the error sequence.
3. Repeat this process until the end of the image.
4. Finally, use the data hiding key to obtain the clear text of the secret message

IV. RESULTS AND DISCUSSION

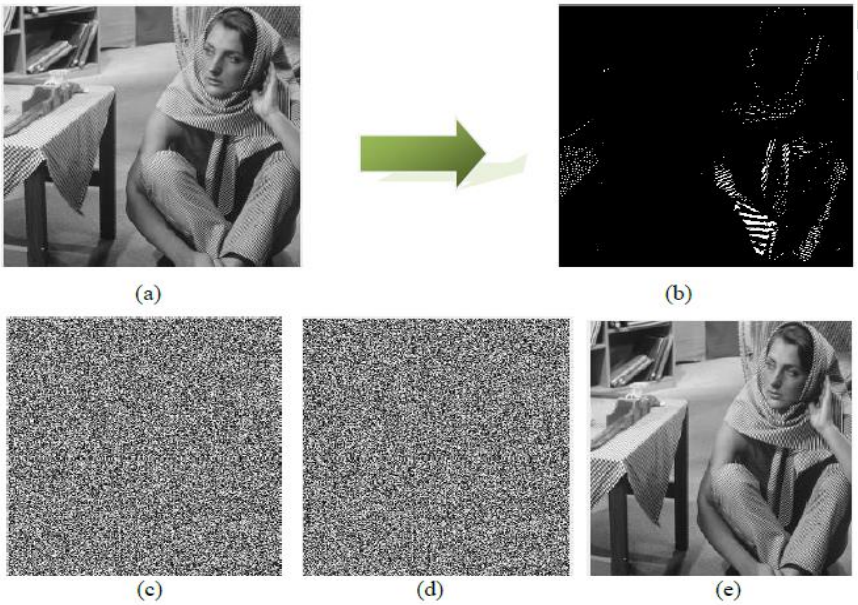

Fig -4: Proposed EPE – MHCRDH Method Result: (a) Input Image, (b) Prediction Error Map, (c) Encrypted Image, (d) Data Embedded Image, (e) Decrypted Image.

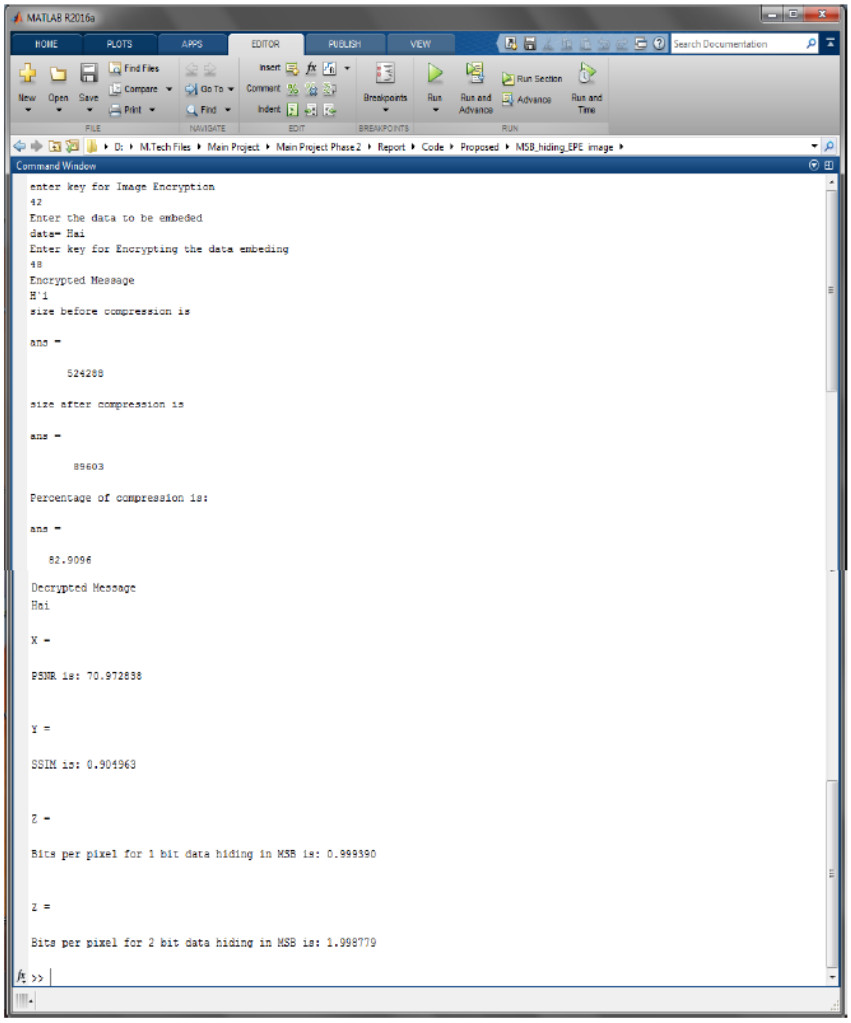

Fig -5: Encryption and Decryption of Embedding Data in EPE – MHCRDH using Matlab

In the EPE-MHCRDH approach, they indicate all the pixels which will not be marked. Indeed, in addition, in white we show the pixels which are not used to embed bits of the secret message because they are part of an error sequence. Note that the prediction errors are often on the edges and there is sometimes more than one error in the same block and if there are errors in two adjacent blocks, the flag which indicates the end of the error sequence is shifted. All other pixels, in black, are used to embed bits of the secret message. Then data embedded picture is compacted as same in the CPE – MHCRDH technique.

REFERENCES

[1] Pauline Puteaux, and William Puech (2019), "An Efficient MSB Prediction- Based Method for High-Capacity Reversible Data Hiding in Encrypted Images" IEEE Transactions on Information Forensics and Security.

[2] Pauline Puteaux and William Puech (2018), "Reversible Data Hiding in Encrypted Images based on Adaptive Local Entropy Analysis" IEEE.

[3] Weiming Zhang, Hui Wang, Dongdong Hou, Nenghai Yu (2016), "Reversible Data Hiding in Encrypted Images by Reversible Image Transformation" Computing for Sustainable Global Development.

[4] Z. Qian and X. Zhang (2016), "Reversible data hiding in encrypted images with distributed source encoding," IEEE Transactions on Circuits and Systems for Video Technology, vol. 26, no. 4, pp. 636–646.

[5] X. Cao, L. Du, X. Wei, D. Meng, and X. Guo (2016), "High-capacity reversible data hiding in encrypted images by patch-level sparse representation," IEEE Transactions on Cybernetics, vol. 46, no. 5, pp. 1132–1143.

[6] X. Zhang, J. Long, Z. Wang, and H. Cheng (2016), "Lossless and reversible data hiding in encrypted images with public-key cryptography," IEEE Transactions on Circuits and Systems for Video Technology.

[7] K. Ma, W. Zhang, X. Zhao, N. Yu, and F. Li (2013), "Reversible data hiding in encrypted images by reserving room before encryption," IEEE Transactions on Information Forensics and Security.

[8] W. Hong, T.-S. Chen, and H.-Y. Wu (2012), "An improved reversible data hiding in encrypted images using side match," IEEE Signal Processing Letters, vol. 19, no. 4, pp. 199–202.

[9] V. Itier and W. Puech(2017), "How to recompress a JPEG crypto-compressed image," IEEE Signal Processing Letters, vol.2017, no.7,2017.

[10] J. Zhou, W. Sun, L. Dong, X. Liu, O. C. Au, and Y. Y. Tang (2016), "Secure reversible image data hiding over encrypted domain via key modulation," IEEE Transactions on circuits and systems for video technology , vol. 26,no.3, pp.441-452,2016.

[11] D. Xu and W. Sun ,(2014), "Hgh –capacity reversible data hiding in encrypted data hiding in encrypted images by prediction error ," Signal processing , vol. 104, pp. 387-400, 2014.

[12] P. Puteaux, D. Trinel, and W. Puech(2016), "Hgh –capacity data hiding in encrypted images using MSB prediction ," in Image Processing Theory Tools and Application (IPTA), 2016 6TH IEEE International Conference on 2016, pp. 1-6.

[13] T. H. Chen and K.-H. Taso(2011),''User-friendly random-grid-based visual secret sharing,'' IEEE Transactions On Circuit And Systems For Video Technology , vol. 21, no. 11, pp. 1693-1703, 2011.

[14] P. Korshunov and T. Ebrahimi(2014), "Scrambling-based tool for secure protection of JPEG images ," in Images Processing (ICIP), 2014, PP. 3423-3425.

[15] C.-Y. Hsu, C.-S. Lu, and S.-C. Pei(2012), "Iages feature extraction in encrypted domain with privacy –preserving SIFT.'' IEEE Transactions on Image Processing, Vol. 21, no 11,pp. 4593-4607. 2012