Reversible Image Data Hiding In Encrypted Images by MSB Prediction Method

Ashish Abraham[1] M. Ravikumar[2] Dr. D. Chitra[3]
[1]PG Student [2,3]Assistant Professor
[1,2,3]Department of Electronics and Communication Engineering
[1,2,3]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 encrypted image has a lot of attention from the communities of privacy, security and protection. This paper presents a highly efficient reversible data hiding in encrypted image by 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 Correction of Prediction Error (CPE – MHCRDH) approach.

Keywords: 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 technique s 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.

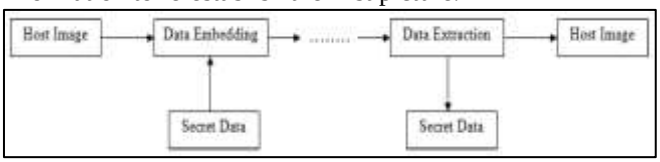

Fig. 1: General Block Diagram of RDH

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.

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

The previous RDH methods are not able to hide a large amount of information with very high embedding capacity as well as it does not provide a very good reconstructed image quality. This paper introduces high productive reversible information stowing away in scrambled picture by MSB expectation technique. In this method RDH is a process to embedded useful data into a cover media or encrypted image using MSB prediction. It is a twostep data hiding procedure, first embed data inside a media file and second, the hidden data and the original image can be loss

lessly extracted. Here present High-Capacity Reversible Data Hiding on MSBs with Correction of Prediction Error (CPE – MHCRDH). Before transmitting the data embedded image to the receiver, we can use image compression techniques to reduce the amount of data required to represent an image.

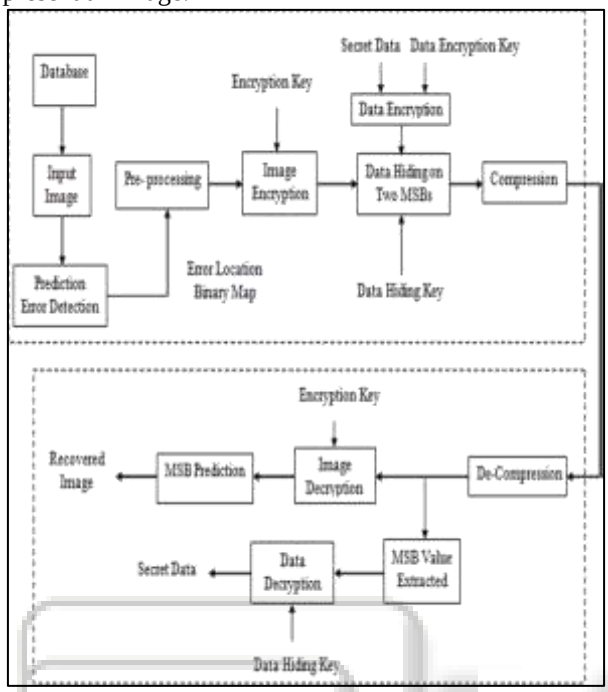

Fig. 2: Block Diagram of Proposed CPE – MHCRDH Method

The block diagram of proposed CPE-MHCRDH method is shown in Fig 3.3. In this method, we propose to embed the secret message (2 bit per pixel) by MSB substitution with very high embedding capacity and visual quality. The goal of our proposition is that an original image I, with m × n pixels, could be encrypted by using a secret key Ke and that another person could embed a message by using a data hiding key Kw, without knowing Ke [1].

The encoding phase consists of four steps: the prediction error detection, the image encryption, the 2-bit data hiding by MSB substitution and compression as shown in fig 3.5. For the decoding phase, there are three possible outcomes. If the recipient has just the encryption key, they can only obtain the original image, but not the embedded message. If the recipient has only data hiding key, the can obtain the secret message, but not the original image.

A. Prediction Error Detection

In this method, the input image is taken from the data base. First predict all the prediction errors in the input image i.e., we can embed the secret message (2 bit per pixel) by MSB substitution, the original MSB values are lost after the data hiding step. It is important, during the decoding phase, to be able to predict them without any errors. Indeed, in order to reconstruct the original image, we propose to use the previous pixels to predict the current pixel value [1]. So, the first step consists of analysing the original image content to detect all the possible prediction errors.

1) Consider the current pixel P (i, j), with $0 \leq i < m$ and $0 \leq j < n$, and its inverse value, which is inv (i, j) = (P(i, j) + 128) mod 256.
2) From the previously scanned neighbours of P (i, j), compute the value Perror (i, j) which is considered as a predictor during the decoding step.

	$p(i-1,j)$
$p(i,j-1)$	$p(i,j)$

Fig. 3: Context of a pixel P (i, j)

3) Calculate the absolute difference between Perror (i, j) and P (i, j) and between Perror(i, j) and inv(i, j).
4) Compare the values of Δ and Δinv. If Δ < Δ', there is no prediction error because the original value of P (i, j) is closer to its predictor than the inverse value. Otherwise, there is an error and we store this information into an error location binary map.
5) After the prediction error detection phase, we propose to pre-process the original image I in order to obtain an image I' without any prediction errors. For each problematic pixel, we observe the amplitude of the error and we compute the value of the minimal pixel modification necessary to avoid this error.

B. Image Encryption

In order to make the original image I unreadable, we encrypt it by using an encryption key Ke, as shown in figure 3.5. The elements of this key are used as parameters of a chaotic generator, based on the Piecewise Linear Chaotic Map (PWLCM). By using chaotic generator, a sequence of pseudo-random bytes S (i, j) is obtained and the encrypted pixels Pe (i, j) can be calculated through exclusive-or (XOR) operation.

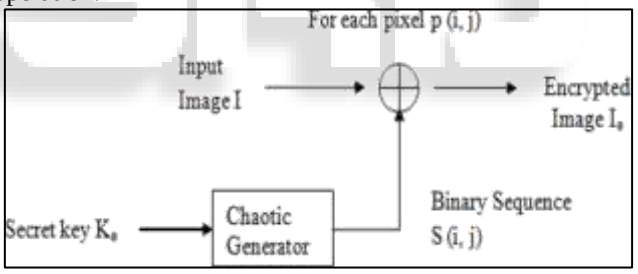

Fig. 4: Encryption Step

C. Data Embedding

In the data embedding phase, it is possible to embed data in the encrypted image without knowing either the encryption key Ke used during the previous step or the original content of the image. By using the data hiding key Kw, the to-be-inserted message is first encrypted in order to prevent its detection after embedding in the marked encrypted image. Next, pixels of the encrypted image are scanned from left to right, then from top to bottom (scan line order) and the MSB of each available pixel is substituted by two bit bT, with $0 \leq T < m \times n$, of the secret message.

D. Compression

After this process, we can compress the data embedded image using image compression techniques. Image compression is reducing the size without degrading the quality of the image to an unacceptable level. Here we use LZ77 compression technique. LZ77 compression works by discovering grouping of information that is repeated. The

term "sliding window" is used; all of it really means that at any given point in the data, there is a record of what characters went before. A 32K of sliding window means that the compressor and decompressor have a record of what the last 32768 (32*1024) characters were. The next sequence of characters to be compressed is indistinguishable to the characters found within the sliding window, the sequence of characters is replaced by two numbers: a distance is representing how far back into the window the sequence starts, and a length, is representing the number of characters for which the sequence is identical.

E. Data Extraction and Image Recovery

For the decoding phase, since our method is separable, we can extract the secret message and reconstruct the clear image IR separately. Before that we can decompressed the data embedded image. IR may be exactly like the original image I itself, depending upon which approach is used. If the recipient has a key Kw, the pixels from the decompressed image are scanned in the scan line order and the MSB of each pixel are extracted in order to retrieve the encrypted secret message.

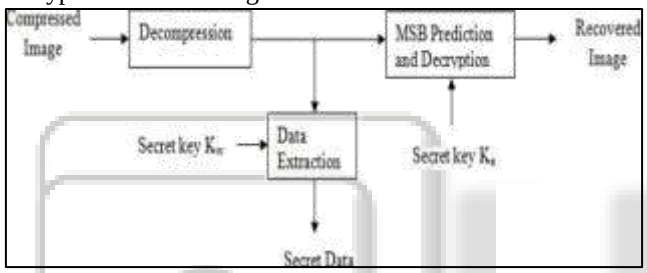

Fig. 5: Decryption Step

IV. RESULT

We are using Matlab for simulation results. In the CPE-MHCRDH approach, they are pixels of the original image whose the MSB would be badly predicted if we do not adapt their values during the pre - processing phase. After this pre -processing step, the adapted images are obtained. This is similar to original image. The compression reduces the quantity of bits required to represent a picture. At the decoding phase the compressed image can be decompressed then extract the data and the image. Finally, after data extraction, reconstructed images are exactly the same as pre - processed images and very similar to original image. Fig. 6 shows the results obtained with the CPE-MHCRDH approach. In Fig. 6(b) in white, we can see the location of all the pixels with prediction errors.

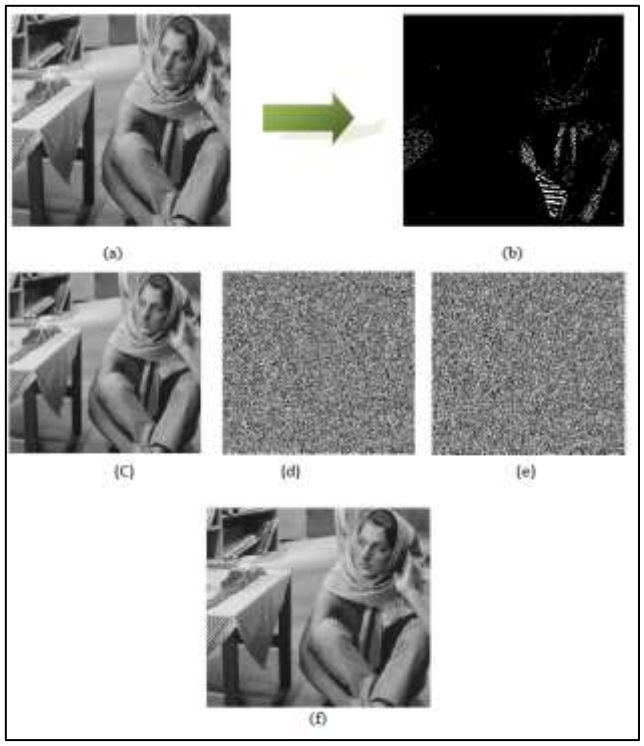

Fig. 6: Proposed CPE – MHCRDH Method Results: (a) Input Image, (b) Prediction Error Map, (c) Error Corrected Image, (d) Encrypted Image, (e) Data Embedded Image, (f) Decrypted Image.

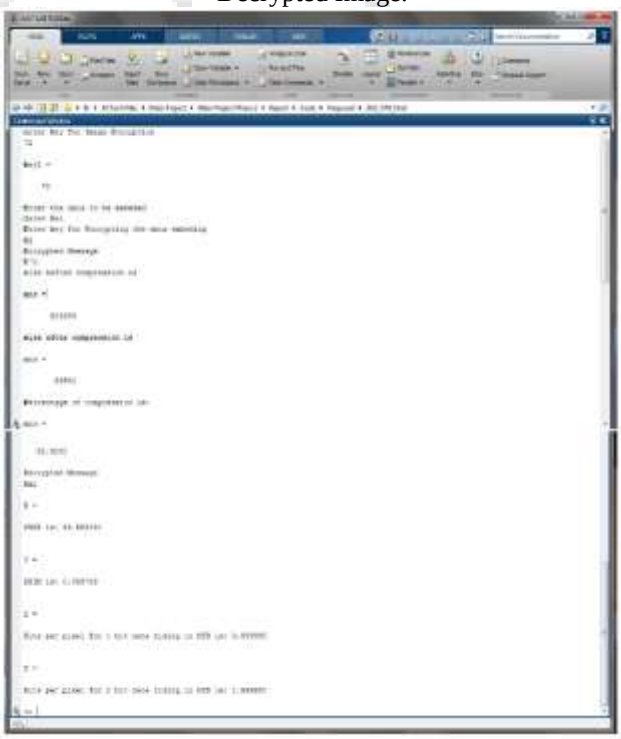

Fig. 7: Encryption and Decryption of Embedding Data in CPE – MHCRDH Method

V. CONCLUSION

In this paper, propose a high-capacity reversible data hiding method in encrypted images based on the MSB prediction. Indeed, by replacing all the MSB in the image, it is possible to hide two bit per pixel. In addition to this excellent

embedding capacity, the reconstructed image quality is high. By analysing the content of the original image, all the prediction errors are highlighted and the encrypted image is modified accordingly. After that, by substituting most of the MSB values in the image, it is possible to hide a large message and compression reduces the number of bit used to represent an image. There for we can reduce the bandwidth required to transmit and receive an image. Finally, in the extraction phase, the compressed image is decompressed and the original image is reconstructed without any errors and the secret message is perfectly extracted.

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 forSustainable Global Development (INDIACom).
[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. 199–202.42
[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

