Reversible Data Hiding in Enciphered Images with High-Capacity MSB Prediction

Sneha Chandrakant More[1], Vikas Nandgaonkar[2]
[1] *Nutan Maharashtra Institute of Technology, Talegaon Dabhade, Pune,*

[2] *Nutan Maharashtra Institute of Technology, Talegaon Dabhade, Pune.*

Abstract- *Unpredictable data hiding in encrypted images is an effective technique to implant data in the encrypted domain. Original image is encrypted with a secret key and during or after its communication, it is also possible to embed or insert additional information in the encrypted image, without knowing the original information of the image or encrypted image. During the process of decoding, the secret message can be removed and the actual image can be reconstructed. Research interest has been started by RDHEI. Certainly, with the Growth of cloud computing, data privacy has become a real issue. No existing methods allows us to hide a huge amount of information in a reversible manner. In this paper, we presented a new reversible method based on MSB (most significant bit) predication with a very high capacity. We present two proposals, these are: high capacity reversible data hiding with embedded prediction errors (EPE-HCRDH) and high capacity reversible data hiding with correction of prediction errors (CPE-HCRDH) with this two method, our results are better than those obtained with current state of the methods, both in term embedding capacity and also in terms of reconstructed image quality.*

KEYWORDS- *IMAGE ENCRYPTION, IMAGE SECURITY, REVERSIBLE DATA HIDING, MSB PREDICTION, DATA PRIVACY.*

INTRODUCTION

Reversible data hiding is a method to embed message into some effect free unsatisfactory Cover media. It is needed in the fields such as military, medical images, with a reversible manner are use so that after extraction of hidden message original cover content can recovered perfectly. As we know that cryptography provides for secure communication in the presence of harmful third-parties known as adversaries. Encryption is a major component of cryptography it uses an algorithm and a key to transform an input into an encrypted output. Algorithm are used to transform the same plaintext into the same cipher text if same key is used. Algorithms are secure if an attacker cannot determine any properties of the plaintext and key given the cipher text. An attacker should not be able to determine anything about a key given many plaintext or cipher text the combinations of both which used the key. Digital image security plays a significant role in all fields especially in highly confidential areas like the medical and military. With the development of cloud computing, the growth in information technology has been led to a very serious security problems such as where the confidentiality, authentication and integrity are constantly threatened by illegal activities such as hacking, copying or malicious or harmful use of information. The main motive of encryption methods is to guarantee data privacy by fully or partially randomizing the content of original images.

Steganography is an encryption technique that can be used also with cryptography as an secure method in which to protect data. Steganography techniques can be applied to images, a video files or an audio file. Typically, however, steganography is written in characters including hash marking, but its main is usage within images is common. During the transmission or the archiving of encrypted images it is often necessary to do analysis or to process them without knowing the original content of image, or the secret key used during the enciphered phase. Methods of reversible data hiding in the encrypted domain (RDHEI) have been designed for data enrichment and authentication in the encrypted domain, when the encryption phase is necessarily done in the first place as, for example, in a cloud computing scenario. Without knowing the original content of the image or the secret key used to encrypt the image, it is then possible to embed a secret message in the encrypted image. During the decoding phase, the original image must be perfectly recoverable, and the secret message must be extracted without error. Therefore, there exists a trade-off between the embedding capacity and the quality of the reconstructed image. In recent years, many methods have been designed. As the space to embed the message may be vacated after or before the encryption phase and during the decoding phase image reconstruction and data extraction can be processed at the same time or separately.

In all cases, the presented methods are not able to propose a high embedding rate together with a very good reconstructed image quality. As RDHEI schemes have been proposed in past years. One of the most common techniques is based on manipulating the least-significant-bit that is LSB planes by directly replacing the three LSBs of the cover-image with the message bits, which is kind of the pixel-level compressive methods essentially. The encrypted image is divided into several non-overlapped blocks, while each block is divided into two sets. Each of the block carries one bit by flipping three LSBs of a set for predefined pixels. Specifically, they fully harness the pixels in calculating the smoothness of each block and consider the pixel correlations in the border of neigh-boring blocks. The resulting error rate of extracted-bits is thereby decreased. In the proposed method creates space to accommodate some additional data by compressing the LSBs of the encrypted image.

In this paper, we present a new high capacity reversible data hiding scheme for encrypted images based on MSB prediction. Due to the local correlation between a pixel and its neighbours in a clear image, two adjacent pixel values are very close. For this reason, it seems natural to predict a pixel value by using already decrypted previous ones, as in many methods of image coding and compression. However, in some cases, there are some errors. So, the first step of our method consists of identifying all the prediction errors in the original image and to store this information in an error location binary map.

After that, we propose two different approaches: the CPE-HCRDH (high-capacity reversible data hiding with correction of prediction errors) and the EPE-HCRDH (high-capacity reversible data hiding with embedded prediction errors). CPE-HCRDH approach consists of correcting the prediction errors (CPE) before encryption. According to the error location map, the original image is pre-processed in order to avoid all the prediction errors and then, the pre-processed image is encrypted. In the EPE-HCRDH approach, 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

a bit of the secret message. At the end of the process, the embedded data can be extracted without any errors and the clear image can be reconstructed lossless by using MSB prediction.

I. PROPOSED SYSTEM

Signal processing in encrypted images received much importance from academia due to the privacy preserving property. Reversible data hiding in encrypted images is a technique that to embedded additional information into an enciphered image without accessing the content of the original image, the embedded data can also be extracted, and the encrypted image can be recovered to the original one. There are two reversible data hiding methods introduced by adopting prediction error they are joint method and separable method. In the joint method, data extraction and the image reconstruction are performed at the same time. The reversibility, good visual quality of recovered image is maintained by improving number of incorrect extracted bits, especially when the embedding rate is high. In the separable method, data extraction and image recovery are differently separated. The separable method also provides the improved reversibility and good visual quality of recovered image for embedding high payload.

None of the existing methods succeed in combining high embedding capacity (near 1 bpp) and high visual quality (greater than 50 dB). In most cases, the methods based on prediction error analysis (PE) or using a histogram shifting technique, the LSB values of some pixels are replaced to hide bits of the secret message. However, if an image is encrypted, it is difficult to detect if it contains a hidden message or not. In fact, the pixel values of an encrypted image are pseudo-randomly generated. So, there is no correlation between a pixel and its adjacent neighbours. 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 during the decryption, the prediction of the MSB values is easier to obtain than those of the LSB.

II. ARCHITECTURE

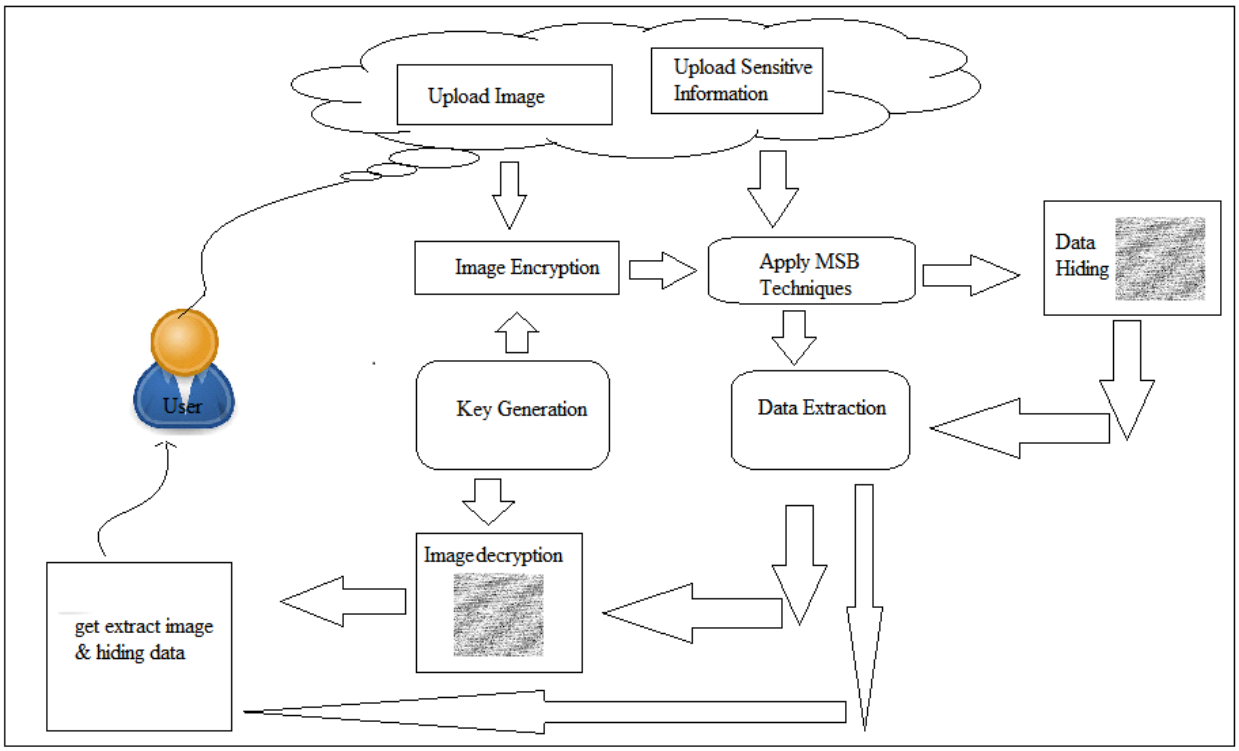

Fig.1. Architecture of data hiding and extracting data

Reversible data hiding are group of techniques used to put secure data in host media like images with small failure in host and the means to extract the secure data afterwards.

As in fig 1:

- User uploads image and also it uploads sensitive information.
- We perform encryption on uploaded image.
- Encryption is process of encrypting data in coded form we generate key.
- Key Generation is process of generating keys in cryptography. A key is used to encrypt and decrypt data whatever data is being encrypted or decrypted.
- Now the sensitive information is uploaded we perform MSB technique on the sensitive image being uploaded here we are applying steganography.
- By applying MSB technique we are able to embed secret message in the most significant bit of the pixel of the image.
- Now by use of most significant data is been hidden.
- Now as data is been hidden fetching of data is also necessary.
- Data extraction is done by using the MSB technique to get the hidden data.
- As we have encrypted the image it is necessary to decrypt the image.
- By using key on encrypted image it is able to decrypt image.
- Now finally we get both the sensitive hidden data and extracted data.

III. ALOGORITM

Input: get secret message sm and image im
Output: hide message into image
Steps:
Step 1: Read secret message

$$sm = message$$

Step 2: Convert secret message into binary

$$smb[\ \ ] = toBinary(sm)$$

Step 3: Read the image

$$fori = 0\Im.width$$
$$forj = 0\Im.height$$

Fetch RGB value of image

Step 4: Apply the AES algorithm

$$pixel' = AES$$

Step 5: Apply MSB

$$pixel = MSB(pixel', smb[j])$$

Step 6: Set pixel to image

$$\Im[i][j] = pixel$$

Step 7: End

IV. MATHEMATICAL MODULE

S={s, e, X, Y,Φ}
Where,
s = Start of the program.
1. Login with System.
2. Initialize System.
e = End of the program.
Accurate Embeded the textual message into image.
X = Input of the program.
Input of this system is upload Image and sensitive information.
Y = Output of the program.
First, we are going to preprocessing calculate textual data sizing in binary. If binary value i less than image size then embeded msg.
X, Y ∈ U
Let U be the Set of stress datasets.
U= {I,C,S}
Where I,C,S are the elements of the set.
I= Image File
C=Cryptography
S=Steganography
Space Complexity:
The space complexity depends on Textual and image Size.
Time Complexity:
Check No. of binary value of text = n
If (n>1) then retrieving of information can be time consuming. So, the time complexity of this algorithm is O(n^n).
Φ = Failures and Success conditions.
Failures:
- Software failure.

Success:
- Accurate book recommendation.

This is NP- Complete Problem

V. MOTIVATION

In cloud computing security issue generated by data sharing, to pass information without leak we implement some special algorithm to hide data. To last few years some techniques are implemented but data cannot recover fully, or hacker can easily find where something is wrong. To avoid problem, we implement Reverse Data Hiding in Encrypted Image. Using these techniques, we cannot use any private or public key to data hiding process.

Aim:

The aim of encryption methods is to guarantee data privacy by full you're partially randomizing the content of original images.

CONCLUSION AND FUTURE WORK

Data hiding is very crucial steps in network. To secure our sensitive information we implement combination of cryptography and stenography techniques. It's a reverse data hiding techniques using MSB algorithm. The result and accuracy of techniques is much higher in existing algorithm.

REFERENCES

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

[2] T.-H. Chen and K.-H. Tsao, "User-friendly random-grid-based visual secret sharing," IEEE Transactions on Circuits and Systems for Video Technology, vol. 21, no. 11, pp. 1693–1703, 2011.

[3] X. Gao, L. An, Y. Yuan, D. Tao, and X. Li, "Lossless data embedding using generalized statistical quantity histogram," IEEE Transactions on Circuits and Systems for Video Technology, vol. 21, no. 8, pp. 1061–1070, 2011.

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

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

[6] P. Korshunov and T. Ebrahimi, "Scrambling-based tool for secure protection of JPEG images," in Image Processing (ICIP), 21th IEEE International Conference on, pp. 3423–3425, 2014.

[7] Z. Ni, Y.-Q. Shi, N. Ansari, and W. Su, "Reversible data hiding," IEEE Transactions on Circuits and Systems for Video Technology, vol. 16, no. 3, pp. 354–362, 2006.

[8] K. Ma, W. Zhang, X. Zhao, N. Yu, and F. Li, "Reversible data hiding in encrypted images by reserving room before encryption," IEEE Transactions on Information Forensics and Security, vol. 8, no. 3, pp. 553–562, 2013.

[9] B. Ou, X. Li, Y. Zhao, R. Ni, and Y.-Q. Shi, "Pairwise prediction-error expansion for efficient reversible data hiding," IEEE Transactions on Image Processing, vol. 22, no. 12, pp. 5010–5021, 2013.

Puteaux, D. Trinel, and W. Puech, "High-capacity data hiding in encrypted images using MSB prediction," in Image Processing Theory Tools and Applications (IPTA),