International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 04 | Apr 2020 www.irjet.net p-ISSN: 2395-0072

HIGH CAPACITY DUAL DATA HIDING IN ENCRYPTED IMAGES USING MSB PREDICTION

Rugma M[1], Vijitha G[2]

[1]*M. Tech student, Electronics and Communication, Jawaharlal College of Engineering and Technology, Kerala, India*
[2]*Asst. Professor, Electronics and Communication, Jawaharlal College of Engineering and Technology, Kerala, India*

Abstract - *In the past few years ,data privacy and protection of multimedia data are becoming more important. Because of this, DHEI has become an investigative field. The multimedia data protection can be done with encryption or data hiding algorithms. High capacity dual data hiding in encrypted images(DHEI) is an effective technique to embed data in encrypted domain. An original image is encrypted using the secret key, still possible to embed additional data without knowing the original content of the image or the secret key. This secret message can be recovered and the initial image can be extracted in the decoding phase. Recently, reversible data hiding methods have been proposed with high capacity, but these proposed methods do not allow a large amount of embedding capacity. In this paper we propose a high capacity dual data hiding method based on MSB (most significant bit) prediction. We suggest to hide two bit per pixel by pre-processing the image to avoid prediction errors and, thereby, improving the quality of the reconstructed image. We demonstrate two approaches: high capacity reversible data hiding approach with correction of prediction errors(CPE-HCRDH) and high capacity reversible data hiding with embedded prediction errors(EPE-HCRDH).We have applied our method on various images, every cases, our results are better than those results obtained from the current methods, both of embedding capacity and reconstructed image quality.*

Keywords – CPE-HCRDH, EPE-HCRDH, High capacity dual data hiding, MSB prediction.

1. INTRODUCTION

Digital image security plays an essential role in every field particularly in computer network and has led to serious security issues where authentication, confidentiality and reputation are threaten by activities such as hacking, copying or malicious use of images. To ensure safe multimedia content transmission via the public communication channel too major strategies have been developed: Encryption and Data hiding. During the encryption step without knowing the original content or the secret key used it is possible to analyze or process the during the transmission or Archiving of the encrypted images. The aim of the encryption method is to ensure data privacy by fully or partially randomizing the content of the original images. Reversible Data Hiding (RDH) consist of embedding hidden data in a signal .It is fundamental to reconstruct the original image with minimum number of errors or preferably none at all after its extraction. The distortion of image may have a critical impact in some strict areas, like in the medical world or military.

Maetal [1] introduce a reversible data hiding methodology for encrypted images to obtain an error free recovered images by reserving rooms before encryption with a conventional data hiding algorithm where additional data is accommodated in the reserved room. In their method, image reconstruction and data extraction are free of errors. Zhangetal [2] proposed improved reversibility method before encrypting the image, room for data embedding is vacated by shifting the histogram of estimating errors of pixels .Image recovery and data retrieving are free of errors in their method. Although these two approaches greatly increase the embedding ability and reversibility, it may be difficult to empty the content owner's space for data embedding, since reversible data hidden in encrypted image often allows the content owner to do nothing but image encryption, and the service provider is expected to conduct data embedding. Quianetal [3] proposed a separable reversible data hiding approach for encrypted image using a N-nary data hiding method and histogram modification. At the content owners side reserving room is no longer required and a error free recovered image is obtained by their method. These two reversible data hiding strategies for encrypted images based on prediction error are introduced to improve the problems. These methods can provide better visual quality of loose recovered image and improved reversibility. Further, the number of extracted incorrect bits are significantly reduced by the join method.

In this paper we present a new high capacity reversible data hiding scheme based on MSB prediction for encrypted images. Two adjacent pixel values are very similar due to the local co-relation between a pixel and its neighbors in a clear image. Of this purpose it seems normal to estimate the pixel value by using already decrypted previous one as in many image codding and compression schemes. For some instances, however there are some errors. So the first step of

our method is to define all errors of prediction in the original image and store this information in a error location binary map. After that , we proposed two different approaches : The CPE-HCRDH (High capacity reversible data hiding with correction of prediction errors) and the EPEHCRDH (High Capacity reversible data hiding with embedded prediction errors). The CPE-HCRDH approach consist of correcting the prediction error prior to encryption. In order to remove all the prediction errors the original image is pre-processed and then this image is encrypted based on the error location map. EPEHCRDH approach, the original image is encrypted directly, after this encryption the location of prediction errors is embedded (EPE).In both approaches during the data hiding Phase, the MSB value of each available pixel is substituted by a bit of secret message in the encrypted images. By the end of this process , the embedded data can be extracted without any errors and the original image can be losslessly reconstructed by using MSB prediction.

2. PROPOSED METHOD

This System uses a new reversible data hiding method for encrypted images based on MSB prediction with a very high capacity. We adapt the message to be inserted to highlight the problematic pixels without significantly reducing the embedding capacity to avoid the prediction errors. The encoding phase comprises of three steps: MSB prediction error detection, joined MSB error consideration and encryption, reversible data hiding by MSB substitution. This Process is shown in Fig.1. There are three possible outcomes in the decoding phase. The receiver has only the encryption key they can only retrieve the original image, but not the embedded message. On the contrary if they have only the water marking key, they can just extract the hidden message. Obviously when they are having both the encryption and water marking keys, the recipient can extract the secret message as well as reconstruct the original images.

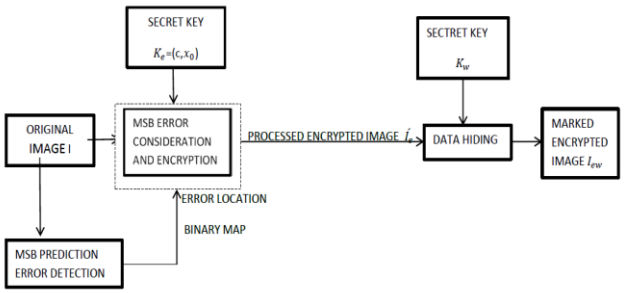

Fig. 1 Overview of general encoding method.

2.1) Prediction error detection

We first analyze the original image content to detect all the prediction errors in order to detect all the possible prediction errors we first analyze the original image content.

- Consider the current pixel p(i,j) where 0≤i<m and 0≤j<n and its inverse value which is inv(i,j)=(p(i,j)+128)mod 256. • Note that the difference between those two values is equal to 128.
- Calculate the value pred(i,j) from the previously scanned neighbors of p(i, j) which is considered as a predictor during the decoding stage.
- Calculate the absolute difference between pred(i,j) and p(i, j) as well as pred(i,j) and inv(i,j).Record the results as Δ and Δ^{inv},so that

Δ=| pred(i,j)− p(i,j)|

(1) Δ^{inv}=| pred(i,j)− inv(i,j)|

- Compare the values of Δ and Δ^{inv}.If Δ<Δ^{inv} there is no prediction error since the original value of p(i, j) is equal to the predictor than the inverse value of the predictor itself. Otherwise an error occurs, and we store the information in a binary map of the error position.

2.2) Image Encryption

The original image is encrypted by using an encryption key K_e = (c, x_o), as shown in fig.2. The encryption is done by using a chaotic generator which generates a pseudo-random sequence. As a result a sequence of pseudo random bytes s(i,j) are obtained and the encrypted pixels p(i, j) can be calculated through exclusive-or (XOR) operation.

$$p_e(i,j)=s(i,j)\oplus p(i,j) \quad (2)$$

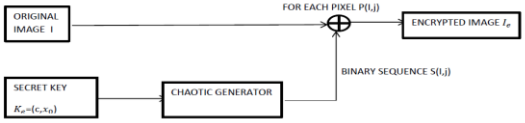

Fig.2 Encryption step.

2.3) Data Embedding

In this Phase its is possible to embed data in the encrypted image without knowing either the encryption key used or the original content of the image . The message to be inserted is first encrypted by using the data hiding key K_w ,in order to prevent its detection after embedding in the marked encrypted image. Next , the encrypted image pixels are scanned from left to right , then from top to bottom (Scanned line Order) and the MSB of each available pixel substituted by one bit b_k, with 0 ≤ k < m ×n, of the secret message.

$$P_{ew(i,j)=b_k} \times 128 + (P_e(i,j) mod 128) \quad (3)$$

2.4) Data Extraction and Image Recovery

Since this method is separable it is possible to extract the secret message and reconstruct the clear image $\tilde{I}$ separately during the decoding phase. $\tilde{I}$ may be same as like the original image I itself or a processed image $\grave{I}$ very close to the original image, based upon which approach is used. There are three possible outcomes:

1) the recipient has only the data hiding key K_w,
2) the recipient has only the encryption key K_e,
3) the recipient has both keys.
An overview of the decoding method is presented in Fig. 3.

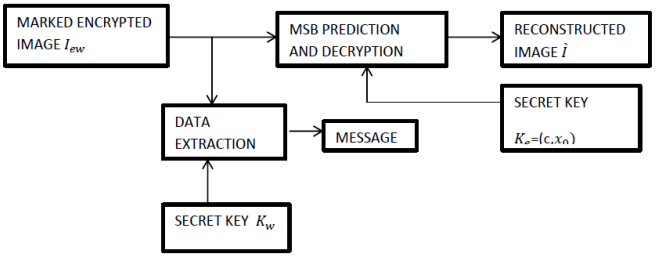

Fig.3 Overview of general decoding method

If the recipient has only data hiding key K_w,the pixels of the marked encrypted image are scanned in the scan line order and the MSB of each pixel are extracted in order to retrieve the encrypted message.

$$b_k = p_{ew}(i,j)/128 \quad (4)$$

Where 0≤k<m×n refers to the index of the recovered bit in the message. Then, corresponding plain text can be obtained by using the data hiding key K_w.

In the second scenario, if the recipient only has *encryption key* K_e,the image $\tilde{I}$ can be retrieved by continuing as follows before the data hiding and encryption steps:

1) The $K_e$encryption key is used to produce the s(i, j) sequence with pseudo-random bytes of m× n.

2)The pixels of the marked encrypted image are scanned in the order of scan line, and the seven LSB values are retrieved by XORing the marked encrypted value P_{ew}(i,j) with the associated binary sequence s(i,j) in the pseudo-random stream

$$\tilde{P}(i,j) = s(i,j) \oplus P_{ew}(i,j) \quad (5)$$

where $\oplus$represents the XOR operation.

3) The MSB value is predicted:

- The value of the predictor pred*(i,j)* is computed by using the values of the previously decrypted adjacent pixels.
- The pixel value is determined with MSB = 0 and with MSB = 1 and the variations between each of these two values and pred*(i,j)* are computed. These values are recorded as Δ^0 and Δ^1:

$$\Delta^0 = |\text{pred}(i,j) - \tilde{P}(i,j)^{MSB=0}| \quad (6) \qquad \Delta^1 = |\text{pred}(i,j) - \tilde{P}(i,j)^{MSB=1}|$$

- The lowest value between Δ^0 and Δ^1 gives the pixel value searched:

$$\tilde{P}(i,j) = \begin{cases} \tilde{P}(i,j)^{MSB=0}, & if \Delta^0 < \Delta^1 \\ \tilde{P}(i,j)^{MSB=1}, & else \end{cases} \quad (7)$$

A. CPE-HCRDH Approach

As shown in Fig.4, we first pre-process the original image in the CPE-HCRDH approach (high-capacity reversible data hiding approach with correction of prediction errors) to avoid all the prediction errors so as to reconstruct the image during the decoding phase. After this process, the pre-processed image can be encrypted without any problems. Each pixels of the encrypted image are marked with one bit of the message during the embedding process.

1) Predictor Used

we proposed to use the preceding pixels to estimate the value of the current pixel. In this method(except for the first row and the first column) we consider the average of the left and the top pixels as a predictor pred*(i,j)* for example:

$$\text{pred}(i,j) = (p(i-1,j) + p(i,j-1))/2 \quad (8)$$

2)Image Pre-Processing

We propose to pre-process the original image after prediction error detection phase in order to obtain an image $\acute{I}$ without any prediction errors. For each problematic pixel, we note the amplitude of the error and we determine the value of the minimal pixel modification change required to prevent this error. Eq. 8 indicates the provision required to prevent any errors in the prediction during the decoding phase:

$$|\text{pred}(i,j) - p(i,j)| < 64 \quad (9)$$

3)Data Extraction and Image Recovery

During the decoding process, the marked encrypted image $\acute{I}_{ew}$ is scanned and the MSB of each pixel is simply extracted to extract the secret message. On the other hand, without any modification the pre-processed image $\acute{I}$ can be reconstructed. To obtain the seven less significant bits we first decrypt the marked encrypted image $\acute{I}_{ew}$ and, then predict the MSB value. The reconstructed image resembles very similar to the original one.

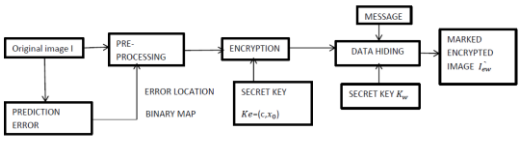

Fig.4 CPE-HCRDH approach encoding phase.

B. EPE-HCRDH Approach

The main objective of the EPE-HCRDH approach (high-capacity, reversible data hiding method with embedded prediction errors) is precisely to recreate the original image . In this case, the payload may decrease a little because error position information being stored. To highlight the prediction errors, we adjust the information to be inserted according to the error location binary map, created during the of the prediction error detection process. The original image is then encrypted and the error location information is inserted in the encrypted image immediately afterwards. We can hide only one bits of the secret message within the available pixels during the data hiding step. Using this error location information, the original image can be reconstructed at the end of the decoding step, without any apparent alteration, which is indicated by a PSNR which tends to +∞. Fig.5 provides a regional scheme of this strategy.

1) Predictor Used

We have two possible predictors in this scheme for each pixel : the left pixel p(i; j - 1) and the top pixel p(i-1;j). The absolute difference with the current pixel p(i;j) is calculated and the closest value is chosen to determine which of those values is considered to be a predictor,

if |p(i-1,j)- p(i; j)|<| p(i,j-1)- p(i; j)|,
then, pred(i,j)=p(i-1,j), (10)
else, pred(i,j)= p(i,j-1),

2)Embedding of the Error Location Information

The location of the prediction errors is stored in the error location binary map during prediction error detection. Then, the original image I is encrypted. The encrypted image I_e is adapted before the embedding step to avoid prediction errors. The encrypted image I_e is then split into eight pixel blocks and scanned by block in the scan line order. If, according to the binary error location map, at least one prediction error is found in a block the current block is surrounded by two flags by replacing the MSB of each pixel in the previous and the subsequent blocks by one. In the scurrent block,if there is a prediction error the MSB value of a pixel is replaced by 1 and 0 if no error is detected as in Fig. 5.If there is no error in the current block, and it does not serve as a flag, and then the eight pixels of this block are used for data hiding. When error occurs in the two adjacent blocks, the flag which indicates the end of the error sequence and will be moved b without error until the next block. When the flags are used for more than one prediction error the loss of embedding capacity becomes less important.

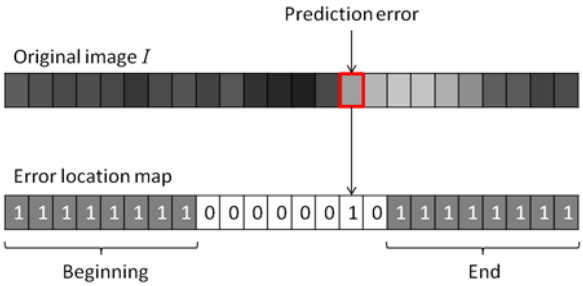

Fig.5 prediction error highlighting

3) Data Extraction and Image Recovery

The secret message can be extracted during the decoding step.

- The pixels of the marked-encrypted image I_{ew} are scanned in the order of the scan line and the MSB value is extracted and stored for each pixel. We assume the extracted values are bits of the embedded message before the first eight MSB series equals 1.
- When a sequence of this type is detected, it indicates the start of the error sequence. Since the next pixels are not marked during the data hiding phase, pixels are scanned until the next sequence where eight MSB are equal to 1, which indicates the end of the error series.
- Repeat the process until the end of the image.

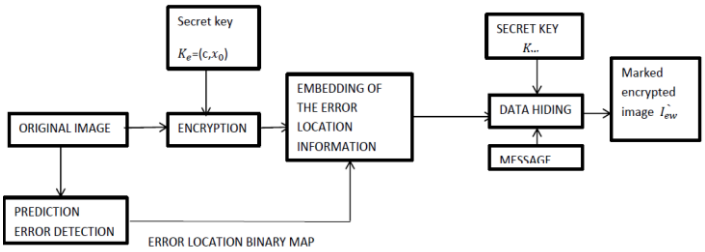

Fig.6 EPE-HCRDH approach encoding phase.

3. RESULT AND ANALYSIS

Throughout this section we present the results obtained by implementing our method using the CPE-HCRDH approach (high-capacity reversible data hiding approach with predictive error correction) and the EPE-HCRDH approach (high-capacity reversible data hiding approach with embedded predictive error). We use two metrics with complete reference which are peak-signal-to-noise ratio (PSNR) and structural similarity (SSIM) to evaluate the reconstructed image quality in comparison to the original one. We first applied our two approaches on different original image also applied to files of different formats like BMP, TIF. Fig. 5.1 shows the result obtained with CPE-HCRDH and fig .5.2 with the EPE-HCRDH approach. In fig 5.1.a shows the original image and fig 5.2.a ,in white, indicates the location of all the pixels with prediction errors. We can observe that, we have neither the same

prediction errors, nor the same number of errors, since we do not use the same predictor in these two approaches, but they are in the same order of magnitude globally.

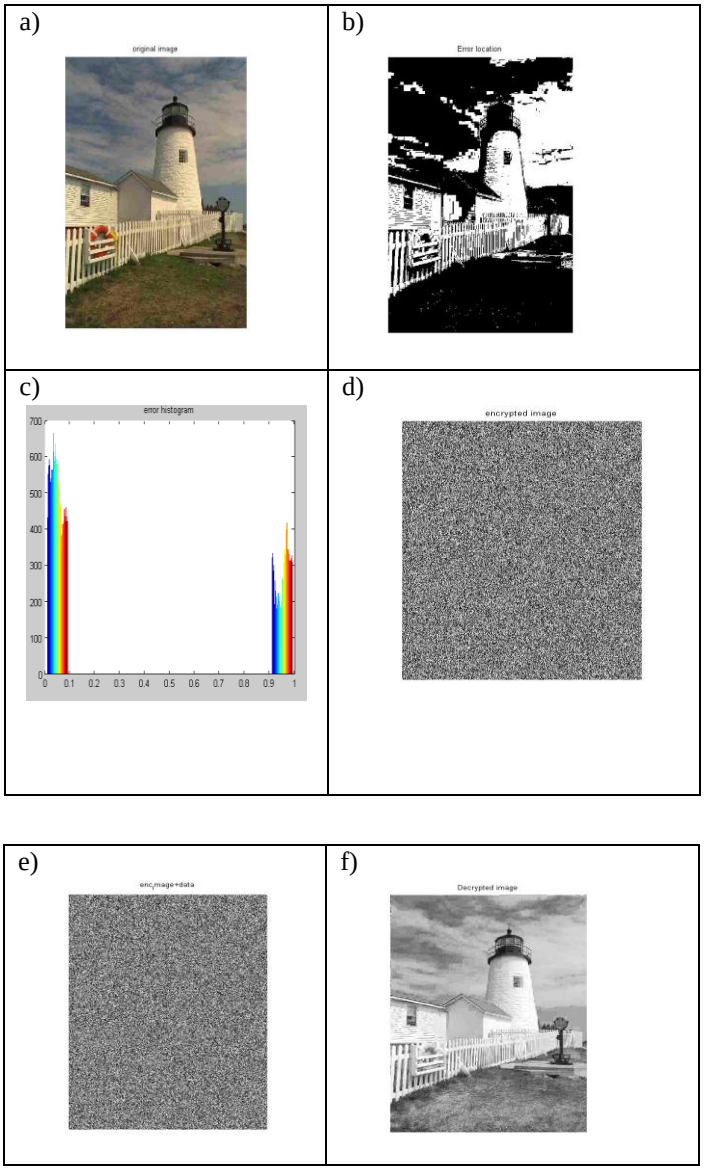

Fig 7:Experiment using CPE-HCRDH approach a) original image I b) error location, number of errors=117235 c) error histogram d) encrypted image $\grave{I}_e$ e)Marked encrypted image $\grave{I}_{ew}$ f) reconstructed image $\grave{I}$

In the CPE-HCRDH approach (Fig. 7.1.a), indicates the original image in which we are applying the process. (Fig. 7.1.b), indicates the original image pixels whose MSB would be badly predicted if we did not change their values during the pre-processing phase. The histogram in (Fig. 7.1.c) demonstrates the prediction error distribution while using the CPE-HCRDH approach and shows the required pixel modifications values to avoid all the prediction errors and (Fig. 7.1.d) represents the encrypted image using the encryption key. (Fig. 7.1.e) illustrates the marked encrypted image obtained during the final encoding step.(Fig .7.1.f) indicates the reconstructed image after decoding process.

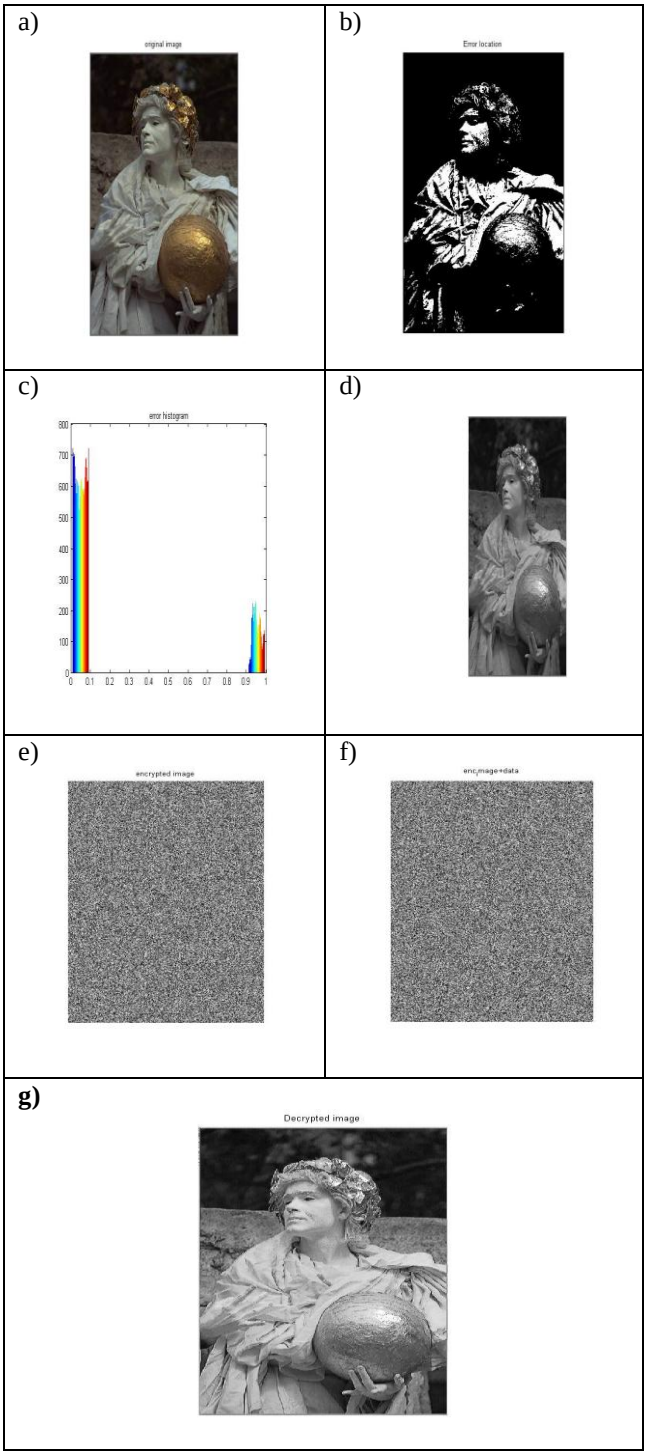

Fig 8. Experiment using EPE-HCRDH approach a) original image I b) error location, number of errors=117235 c) error histogram (d) pre-processed image e) encrypted image $\grave{I}_e$ f)Marked encrypted image $\grave{I}_{ew}$ (g) reconstructed image $\grave{I}$

In the EPE-HCRDH approach (Fig. 8.2.a), indicates the original image in which we are applying the process. (Fig. 8.2.b), these are original image pixels whose MSB would

be poorly predicted if we do not adapt their values during the pre-processing step. The histogram in (Fig. 8.2.c) illustrates the distribution of the prediction errors while using the EPE-HCRDH approach then shows the required pixel value modifications to avoid all the prediction errors and (Fig. 8.2.d) represents the pre-processed image. (Fig 8.2.e) represents the encrypted image using the encryption key.(Fig. 8.f) illustrates the marked encrypted images, obtained during the final encoding step.(Fig .8.2.g) indicates the reconstructed image after decoding process. Note that in both approaches the secret message is always extracted without any errors.

Table I illustrates the performance measurements obtained for the test images. In most of the cases, when there is no prediction error the two approaches are fully reversible. In this case, original images are recovered without any errors, as a SSIM equal to 1. Furthermore, for low contrast images, the reconstructed image quality is high.

		BEST CASE	WORST CASE
CPE-HCRDH approach	PSNR(Db)	44.5599	42.0128
	SSIM	0.9997	0.9992
EPE-HCRDH approach	PSNR(Db)	+∞	32.7750
	SSIM	1	0.9952

Table I Performance measurements of the two approaches.

4. CONCLUSIONS

In this study, we proposed an efficient method of reversible data hiding in encrypted images with a very high embedding capacity based on MSB prediction, which outperforms the current state-of-the-art methods. From our knowledge this is one of the first approaches proposing to use MSB for an RDHEI instead of LSB. Since MSB prediction in original domain is easier than LSB prediction and also degradation image quality is not a problem in the encrypted domain, we are then able to have a very high capacity. By analyzing the original image content, the prediction errors are identified and an error location binary map is created. The original image is slightly modified in the CPE-HCRDH approach in order to remove all the prediction errors. After that, it is possible to hide one bit per pixel by substituting all MSB in the image. Besides this maximal payload equal to 1 bpp, the reconstructed image quality is high (SSIM close to 1).In the EPE-HCRDH method, information about the location of the prediction errors are stored in the encrypted image according to the error location binary map. By substituting most of the MSB values in the encrypted image, a large message can be embedded(close to payload 1 bpp) and the original image can be losslessly recovered during the decoding phase(PSNR =+∞).In addition, we have also seen that the proposed scheme offers a good security level and can be used to preserve the confidentiality of the original image content, while at the same time providing authenticity or integrity check.

ACKNOWLEDGEMENT

I am ineffably indebted to my guide Mrs. Vijitha G for her active guidance and encouragement to accomplish this assignment and Wikipedia for the correct source of information.

REFERENCES

[1] K.Ma,W.Zhang, X.Zhao, N.Yu,F.Li, Reversible data hiding in encrypted images by reserving room before encryption, IEEE Trans. Inf. ForensicsSecur.8(3)(2013)553–562.

[2] W.Zhang, K.Ma, .Yu, Reversibility improved data hiding in Encrypted images, SignalProcess.94(2014)118–127.

[3] Z.Qian, X.Han, X.Zhang, Separable reversible data hiding in encrypted images by n-nary histogram modification, in:TheThird International Conference.

[4] Pauline Puteaux, William Puech,An Efficient MSB Prediction- Based Method for High-Capacity Reversible Data Hiding in Encrypted Images, Transactions on information forensics and security.

[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.

BIOGRAPHIES

Rugma M received the B.Tech degree from Calicut University, India, in 2016. She is currently a final year M.Tech student of APJ Abdul Kalam Technological University. Her work has focused on multimedia security in particular in image processing in the encrypted domain.