A Novel Encryption and Extended Dynamic Histogram Shifting Modulation for Reversible Data Hiding in Encrypted Image

K.Latha M.E¹, M.Sundarambal,Phd²

¹ Student, Department of Computer Science and Engineering, Coimbatore Institute of Technology, Coimbatore, Tamilnadu, India
² Professor, Department of Electrical and Electronic Engineering, Coimbatore Institute of Technology, Coimbatore, Tamilnadu, India.

Abstract—Recently, progressive interest is paid to reversible data hiding (RDH) in encrypted images, since it preserves the original cover can be recovered without any loss after embedded data is extracted to protect the confidentiality of image content’s. Earlier method used “vacate room after Encryption” in which data can be embedded by reversibly vacating room from the encrypted images. This might cause errors while data extraction or image restoration. However this provides less PSNR value when embedding messages in Images. To address this problem, a proposed method uses Extended Dynamic Histogram Shifting Modulation (EDHS) can be done on the image content by the content owner. This method shifts the pixels of histogram based on prediction errors and its neighborhood pixels. The data can be embedded based on the space provided by the proposed histogram shifting method. After reserving space for data hiding by self reversible embedding using EDHS, Image can be encrypted by using proposed novel encryption method. Finally the receiver can restore the image and extract data by using encryption key and data hiding key. Experimental result provides greater PSNR value when compare with the existing work.

Keywords—Reversible data hiding, Image encryption, Extended dynamic histogram.

I. INTRODUCTION

REVERSIBLE data hiding (RDH) in images is a technique, by which the original image can be recovered without any loss after the embedded message is extracted. This significant technique is broadly used in military imagery, law forensics and medical imagery. In these applications distortion of the original image is not allowed. RDH has drawn considerable research interest in these fields.

In order to provide confidentiality for images, encryption is an effective and popular way as it converts the meaningful and original content to incomprehensible one. Even though several RDH techniques in encrypted images have been employed, still there are some promising applications if RDH can be applied to encrypted images. Many schemes has been introduced for providing confidentiality. A reputation-based trust-management scheme is enhanced with data colouring that is a way of embedding data into covers/images. Then software watermarking scheme, in which data encryption and coloring provides possibilities for sustaining the data integrity and content owner’s privacy. Obviously, the cloud service provider has no right to introduce permanent distortion during data coloring into encrypted data. Thus, a reversible data embedding technique based on encrypted data is desired. Consider a medical image database is stored in a data center. The notations can be embedded into an encrypted version of a medical image through a RDH technique in the server’s data center. With these notations, the server can verifies and manages the integrity without having the knowledge of the original content, and consequently the patient’s privacy is protected. In contrast, a doctor who is having the cryptographic key can decrypt and restore the image in a reversible manner for the purpose of further diagnosing purpose.

In the proposed system, data can be embedded in the encrypted image by reserving room before encryption. Data embedding can be done by rearranging the position of LSB by reversibly embedding into the other part of LSB. This replacement can be done by shifting the Histogram using estimated error sequence of pixels. Initially the error sequence to be predicted by its neighbourhood pixels and then histogram can be dynamically shifted by using Extended dynamic histogram method. Then image can be encrypted and decrypted in the content owner side and receiver side by means of proposed encryption and decryption algorithm. Then data is embedded in the reserved space of the image. Finally the data can be extracted and image is recovered without any distortion by using the data hiding and encryption key.

II. RELATED WORK

In practical aspect, many RDH techniques have emerged in recent years. The following shows the few methods for data hiding and embedding tasks.

The method in [1] used vacating room after encryption technique. In this, a content owner encrypted the image using standard encryption algorithm with encryption key. In that encrypted image, content owner can hide data by losslessly vacating some room based on data hiding key. Then the receive who is said to be third party can extract data with the data hiding key and recover the original version of image from the encrypted image based on encryption key.

To perform this [1] compressed the encrypted LSBs of images to vacate room for additional data by searching the syndromes of a parity-check matrix. And the side information
is used at the receiver side which is moreover the spatial correlation of decrypted images. Thus these methods attempt to vacate room from the encrypted images directly.

In [2] a rate-distortion model for RDH is established. In that the rate-distortion bounds of RDH is proved for less covers of memory and suggested a recursive code construction in which does not approach the bounds.

In [3] a general outline for RDH is constructed. In this extracting compressible features of original cover are extracted and then compressing them without any loss. In this spare space can be excepted for embedding auxiliary data.

In [4], A more popular method is based on difference expansion is utilized in which the difference of each pixel group is expanded. Thus the least significant bits (LSBs) of the difference are all-zero and can be used for embedding messages.

In [5] Another strategy is used for RDH which is known as histogram shift (HS). In HS the space is saved for data embedding by shifting the gray value bins of histogram.

In [6][7] to embed data, the space is emptied out following the idea of compressing encrypted images. This separates out the data extraction from decrypted image.

In [8] the error rate is reduced while embedding data by exploiting the pixels in calculating the smoothness of each block and using side match vector. The extraction and recovery of blocks are accomplished based on the descending order of the absolute smoothness difference between the recovered blocks. This can be used to compute the smoothness of unrecovered blocks, which is referred to as side match vector.

III. PROPOSED SYSTEM

The proposed framework of reserving room prior to image encryption at content owner side uses the robust encryption and data hiding technique. The proposed framework consists of four stages:

1. Generation of Encrypted Image
2. Data hiding phase
3. Image decryption phase
4. Data Extraction and Image Recovery phase

A. GENERATION OF ENCRYPTED IMAGE

The encrypted image is generated by means of following three steps.

1. Image partition
2. Self-reversible embedding
3. Encryption

1) Image partition: Image partition step divides original image into two parts A and B; then, the LSBs of A are reversibly embedded into B with a proposed algorithm so that LSBs of A can be used for accommodating messages; at last, encrypt the rearranged image to generate its final version. The goal of image partition is to construct a smoother area B.

Consider the image I is an 8 bits gray-scale image with its size MxN and pixels I_{x,y} \in \{0,255\}. Initially, the content owner extracts from the original image, along the rows. Several overlapping blocks whose number is determined by the size of to-be-encoded messages, denoted by l. Every block consists of m rows, where m=[l/N], and the number of blocks can be computed through n=M+m+1.

For each block, define a function to measure its first-order smoothness

\[ F = \sum_{u=2}^{m} \sum_{v=1}^{N-1} \left| C_{u,v} - \frac{C_{u-1,v} + C_{u+1,v} + C_{u,v-1} + C_{u,v+1}}{4} \right| \]

Higher f relates to blocks which contain relatively more complex textures. The content owner, therefore, selects the particular block with the highest f to be A, and puts it to the front of the image concatenated by the rest part B with fewer textured areas.

2) Extended Dynamic histogram shifting (EDHS) for self-reversible embedding: The goal of self-reversible embedding is to embed the LSB-planes of into by employing message embedding method based on dynamic extracting histogram shifting method.

Pixels in the rest of image B are categorized into two sets: white pixels and Black pixels. White pixels has indices i and j by satisfying (i+j) mod2=0. And black pixels whose indices i and j meet (i+j) mod2=1. Then, each white pixel and black pixel is estimated by the interpolation value obtained with the four white and black pixels surrounding it separately as follows:

\[ B(w)_{ij}' = w_1B(w)_{i-1,j} + w_2B(w)_{i+1,j} + w_3B(w)_{i,j-1} + w_4B(w)_{i,j+1} \]

\[ B(b)_{ij}' = w_1B(b)_{i-1,j} + w_2B(b)_{i+1,j} + w_3B(b)_{i,j-1} + w_4B(b)_{i,j+1} \]

The predicted error for these pixels p(i,j) can be calculated based on prediction-error neighbourhood p(i,j)' is as follows

\[ p(w)_{ij} = \frac{w_1B(w)_{i-1,j} + w_2B(w)_{i+1,j} + w_3B(w)_{i,j-1} + w_4B(w)_{i,j+1}}{4} \]

\[ p(b)_{ij} = \frac{w_1B(b)_{i-1,j} + w_2B(b)_{i+1,j} + w_3B(b)_{i,j-1} + w_4B(b)_{i,j+1}}{4} \]

Consider the pixel block, the prediction-error of the pixel is given by Predicted error estimation:

\[ e_{i,j} = p(i,j) - p(i,j)' \]

Where p(i,j)' is the predicted value of p(i,j) derived as from its four nearest neighbour pixels of black and white. The message to be embedded can be done in carrier class Pixels which belong to the class of the histogram maxima). The carrier class can be defined as C. The pixels don’t belong to the carrier class are considered as non-carrier classes Nc. The carrier class in the range of [-Δ,Δ] where Δ is fixed magnitude to shift a histogram in order to create gap near the histogram maxima.

Prediction-errors that encode the message belong to the carrier-class C; other prediction-errors are non carriers. Moreover, because prediction acts as a low-pass filter, most prediction-error carriers are located within smooth image regions. Highly textured regions (i.e., Region of B in image) contain non carriers. The basic idea of our proposal is thus to
gain carriers in such a region by adapting the carrier-class depending on the prediction-error to be embedded with messages. We propose a Extended Dynamic histogram shifting modulation to achieve this goal.

Steps
1. Estimate underflow and overflow pixels
2. Classify the embedding pixels

EDHS results in adding/subtracting Δto pk(Ij) in order to modulate its prediction-error. Hence, some pixels may lead to an underflow/overflow if message is embedded. To distinguish such embeddable pixels (or blocks), i.e., pixels that do not introduce overflow or underflow is modified, we propose a second classification process also based on the reference image Γ, or more precisely on the reference block B(k)'.

In order to build up this classification process we propose to characterize one pixel p(i,j) through some characteristics extracted from its reference block B(k)'. The objective is to discriminate embeddable pixels (or blocks) from the others with these characteristics. Herein, two characteristics are used. They are defined as B'(k)(min) and B'(k)(max) correspond to the minimum and maximum values of B(k)'. These overflow and underflow pixels can be categorized by setting two thresholds T(min) and T(max)

\[ T_{\text{min}} = \min_n \{ F_{B_{\text{min}}}^n \} \quad (6) \]
\[ T_{\text{max}} = \max_n \{ F_{B_{\text{max}}}^n \} \quad (7) \]

The block B(k) of pixel p(Ij) is embeddable only satisfying the following condition

\[ B(k') > T(\text{min}) \quad \text{and} \quad B(k') > T(\text{max}) \]

The extractor can identify threshold values and Tr(min) and Tr(max) different from T(min) and T(max) and computed at the embedding stage.

At the end of this process, the embedder builds the message overhead (flags concatenated with the values of Tmin and Tmax in case Tr(\text{min}) ≠ T(\text{min}) and Tr(\text{max}) ≠ T(\text{max})).

3) Image Encryption: After self-embedding image X, the image can be encrypted to build the encrypted image, denoted by E. For example, a gray value ranging from 0 to 255 can be represented by 8 bits, Xij(0)……Xij(7), such that Xij(k)=X[i,j]/2^k mod 2 where k=0,1,……7

The encrypted bits can be calculated through the proposed robust encryption method

The proposed encryption algorithm is described as follows:
Step 1: Consider original message bit Xi,j(k) and secret message bit Ri,j(k)
Step 2: Take secret key and split it into two parts

\[ R_{i,j}(k) \rightarrow r1_{i,j}(k) \oplus r2_{i,j}(k) \]
Step 3: Take first part of secret key, r1_{i,j}(k)
Step 4: EXOR the Original bit with the first part of secret key

\[ E(i,j)(k) \leftarrow X(i,j)(k) \oplus r1(i,j)(k) \]
Step 5: From the result of EXOR, perform circular transform

\[ E_{c}(i,j)(k) \leftarrow \text{circular shift}(E(i,j)(k)) \]
Step 6: Then take another part of secret key, r2_{i,j}(k)
Step 7: Perform EXOR on second part of secret bit with the circular shift result

\[ E(i,j)(k) \leftarrow E(i,j)(k) \oplus r2(i,j)(k) \]
Step 8: The obtained resultant cipher text is Ei,j(k).

B. DATA HIDING IN ENCRYPTED IMAGE

In this phase, data hider can embed the data in the encrypted image E. The embedding process is done on the first prat A of image E is denoted as A_E. Since A_E has been rearranged to the top of E, it is simple for the data hider to read 10 bits information in LSBs of first 10 encrypted pixels in A_E. Then the data hider can adopt LSB replacement to substitute the bit-planes with additional data by knowing the modifiable bit-planes and pixel rows. Finally, label can be set by the data hider following m to point out the end position of embedding process. Further m can be encrypted based on data hiding key to formulate marked encrypted image denoted by E'. The data cannot be extracted unless possessing the data hiding key.

C. IMAGE DECRYPTION

The Image can be decrypted by means of following steps:
1. Consider cipher text Ei,j(k) and second part of secret key r2i,j(k).
2. EXOR cipher text with second part

\[ E(i,j)(k) \leftarrow E(i,j)(k) \oplus r2(i,j)(k) \]
3. Perform circular shift on the resultant cipher.

\[ E_{c}(i,j)(k) \leftarrow \text{circular shift}(E(i,j)(k)) \]
4. EXOR circular shift cipher and First part of secret key.

\[ X(i,j)(k) \leftarrow E_{c}(i,j)(k) \oplus r1(i,j)(k) \]
5. Obtain the original message Xi,j(k)

D. DATA EXTRACTION AND IMAGE RECOVERY

After generating the decrypted image D', the content owner extracts the data and original image can be recovered.

Step 1: Consider the histogram amplitude parameter Δ.
Step 2: Retrieve the values of Tmin, Tmax, Tr(\text{min}) and Tr(\text{max}).

Based on the above two step the embedded data can be extracted.

IV. EXPERIMENTAL RESULT

The proposed approach is has been evaluated on publicly available standard images that includes “Barbara”, “Lena” etc. The size of images is in 512 X 512 X 8. The main objective criterion of the proposed method is PSNR which is employed to estimate the quality of marked decrypted image.

To quantify achieved performance, the following criteria’s have been considered.

The embedding rate expressed in bpp (bit of message per pixel of image).

The Peak Signal to Noise Ratio (PSNR) to measure the distortion between an image and its embedded version.
Where d is depth of an image and M are the image dimensions.

The following comparison table 1 shows the PSNR value for the existing and proposed methods:

<table>
<thead>
<tr>
<th>Embedding rate: Bits per pixel(bpp)</th>
<th>Existing system</th>
<th>Proposed system</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lena</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0.005</td>
<td>67.16</td>
<td>69.01</td>
</tr>
<tr>
<td>0.01</td>
<td>63.44</td>
<td>66.05</td>
</tr>
<tr>
<td>0.05</td>
<td>55.46</td>
<td>58.40</td>
</tr>
<tr>
<td>0.1</td>
<td>52.33</td>
<td>55.30</td>
</tr>
<tr>
<td>0.2</td>
<td>49.07</td>
<td>52.02</td>
</tr>
<tr>
<td>0.3</td>
<td>45.00</td>
<td>48.01</td>
</tr>
<tr>
<td>0.4</td>
<td>40.65</td>
<td>43.61</td>
</tr>
<tr>
<td>0.5</td>
<td>35.84</td>
<td>38.00</td>
</tr>
</tbody>
</table>

The above graph in figure 1 shows the proposed system achieves highest PSNR value when compare with the existing system.

V. CONCLUSION

In this paper Reversible data hiding in encrypted images using Extended dynamic histogram shifting modulation (EDHS) and novel encryption method has been discussed. It uses reserving room before encryption scheme for embedding data in an image. An Extended dynamic histogram shifting modulation (EDHS) shifts the pixels in histogram based on predictive error of the pixels and its neighbourhood values. After reserving space by using EDHS method, content owner encrypts the image by using novel encryption algorithm. The proposed method achieves excellent performance without any loss of secrecy and takes benefit when comparing with compare with conventional data hiding methods.

Reference


