ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor & UGC Approved Journal)

Website: www.ijirset.com

Vol. 6, Issue 8, August 2017

Recovery of an Enhanced RGB Image in an Encrypted Image Using Reversible Data Hiding Technique

B.Kamala[1], K.Suseela[2]

M.Tech Scholar (DECS), Dept of ECE,School of Engg.& Technology,Sri Padmavathi Mahila Viswavidyalam,Tirupati, India[1]

Asst. Professor, Dept. of ECE, School of Engg.& Technology, Sri Padmavathi Mahila Viswavidyalam, Tirupati, India[2]

ABSTRACT: This paper proposes a method of reversible data hiding in encrypted images (RDH-EI) based on progressive recovery and recovery of an enhanced rgb image in proposed manner. Three parties are involved in the framework, including the content owner, the data-hider, and the recipient. The content owner encrypts the original image using a stream cipher algorithm and uploads ciphertext to the server. The data-hider on the server divides the encrypted image into three channels and respectively embeds different amount of additional bits into each one to generate a marked encrypted image. On the recipient side, additional message can be extracted from the marked encrypted image, and the original image can be recovered without any errors. While most of the traditional methods use one criterion to recover the whole image, we propose to do the recovery by a progressive mechanism. Rate-distortion of the proposed method outperforms state-of-the-art RDH-EI methods.

KEYWORDS*:* Reversible data hiding, information hiding, encrypted image

I.INTRODUCTION

Idea of reversible data hiding in encrypted images (RDH-EI) originates from reversible data hiding (RDH) in plaintext images [1][2]. It is feasible in the applications like cloud storage and medical systems. In cloud storage, a content owner can encrypt an image to preserve his/her privacy, and upload the encrypted data onto cloud [3][4]. On the cloud side, when managing huge amount of encrypted images, an administrator can embed additional messages (e.g., labels, time stamps, category information, etc.) into the ciphertext. This embedding not only saves the storage overhead, but also provides a convenient way of searching encrypted images. On the recipient side, when a user downloads the encrypted data containing additional messages from the server, he/she can losslessly recover the original images after decryption. Some attempts on RDH-EI have been made. In [5], a content owner encrypts the original image using stream enciphering, and a data-hider embeds additional bits into ciphertext blocks by flipping three least significant bits (LSB) of half the pixels in each block. On recipient side, the ciphertext image is decrypted
and two candidates for each block are generated by flipping again. As the original block is smoother than the interfered, embedded bits can be extracted and original image can be losslessly recovered. This method was improved in [6] by exploiting spatial correlation between neighboring blocks to achieve a better embedding rate, which was further improved in [7] using a full embedding strategy to achieve larger embedding rate. Secure RDH EI can be ensured by public key modulation [8]. RDH-EI can also be realized in encrypted JPEG bitstreams by slightly modifying the encrypted data [9]. One problem in [5]-[9] is that data extraction can only be done after image decryption. Separable RDH-EI was proposed to resolve this problem, allowing one to extract hidden data directly from the encrypted image. In [10], the data-hider permutes and divides the encrypted pixels into segments, and compresses some LSB layers of each segment to fewer bits using a predefined matrix. The recipient extracts additional message from the marked encrypted image. After decryption, the original LSBs are recovered by comparing the estimated bits with the compressed. If higher bitplanes are used [11-13], better embedding rate can be achieved. Some RDH-EI methods were

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor & UGC Approved Journal)

Website: www.ijirset.com

Vol. 6, Issue 8, August 2017

also proposed to enlarge embedding rates by vacating embedding room before encryption, e.g., [14] and [15]. Rate-distortion is important in RDH-EI. Rate stands for the embedding rate while Distortion the difference between the original image and the decrypted marked image. Users with only the decryption key always need to view the image content by decrypting the marked encrypted image directly. We limit the distortion to three LBS-layers in encrypted images, as [5]-[7] and [10], to preserve the decrypted image with good quality. Subjecting to this condition, we propose a progressive recovery based separable RDH-EI to achieve a better capability, which is an extension to our work in [10]. We divide the embedding procedure into three rounds to hide additional messages. Different from the traditional recovery using only one criterion, the progressively recovery uses three criterions. Guaranteed by the progressive mechanism, larger payloads can be achieved.

II.PROPOSED SYSTEM

The proposed system is illustrated in Fig. 1, including three parties: the content owner, the data-hider, and the recipient. The content owner encrypts the original image and uploads the encrypted image onto a remote server. The data-hider divides the encrypted image into three sets and embeds message into each set to generate a marked encrypted image. The recipient extracts message using an extraction key. Approximate image with good quality can be obtained by decryption if the receiver has decryption key. When both keys are available, the original image can be losslessly recovered by progressive recovery.

A. Image Encryption

When the content owner enciphers a grayscale image **X** sized M×N, the conventional stream cipher algorithm is used, such as the RC4, AES in the CTR mode (AES-CTR).

With an encryption key KENC, the key stream **K** with 8MN bits can be generated, and the ciphertext image is generated by $\mathbf{J} = \mathrm{Enc}(\mathbf{X},\mathbf{K}) = \mathbf{X} \oplus \mathbf{K}$ (1)

where Enc(·) and "⊕" represent the encipher algorithm and the XOR operation respectively. Conversely, the plaintext image can be recovered by $\mathbf{X} = \mathrm{Dec}(\mathbf{J},\mathbf{K}) = J \oplus K$

B. Data Embedding

On the server side, the data-hider embeds additional message into the ciphertext image. The pixels of the ciphertext image are divided into three sets: the Square, the Triangle, and the Circle. Hence, there are MN/4 pixels in the Square set, MN/4 pixels in the Triangle set, and MN/2 pixels in the Circle set.

Denote the pixels in the Square set, the Triangle set and the Circle set as S_1 , S_2 , S_3 respectively. With an embedding keyK_{EMB}, the data-hider pseudo-randomly permutes the encrypted pixels within each set. The data-hider divides each permuted set S_i into segments, each of which contains L_i pixels (i=1,2,3). Generally, we have $L_1 > L_2$and $L_1 > L_3$. Collect the bits of three LSB-layers in each segment, and denote these bits of each segment as the group B_i (B_i)=[B_i k_i, 1), B_i (k_i, 2), …, B_i(k_i, $3L_i$)]T, where $k_i \epsilon [1, R_i]$ is the group index, R_1=[MN/(4L_1)] for S_1, R_2=[MN/(4L_2)] for **S**2, and R_3=[MN/(2L_3)] for S_3.

C. Message Extraction and Progressive Recovery

On the recipient side, additional messages can be extracted if the receiver has the key K_{EMB} . The marked encrypted mage is separated to the Square set, the Triangle set and the Circle set again. With the embedding key, the recipient permutes pixels in each set independently, and divides the permuted sets into segments, each of which contains L_i (i=1,2,3) pixels. Collect the bits of three LSB-layers in each segment and reconstruct the groups $B'_i(k_i)$=[c_i (k_i, 1), C_i (k_i, 2), …, C_i (k_i, $3L_i$–P), A_i (k_i, 1), A_i (k_i, 2), …, A_i(k_i, P)]T ($k_i \epsilon [1, R_i]$). From each group, the additional bits $[A_i(k_i,2), \ldots, A_i(k_i,P)]^T$ are extracted.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor & UGC Approved Journal)

Website: www.ijirset.com

Vol. 6, Issue 8, August 2017

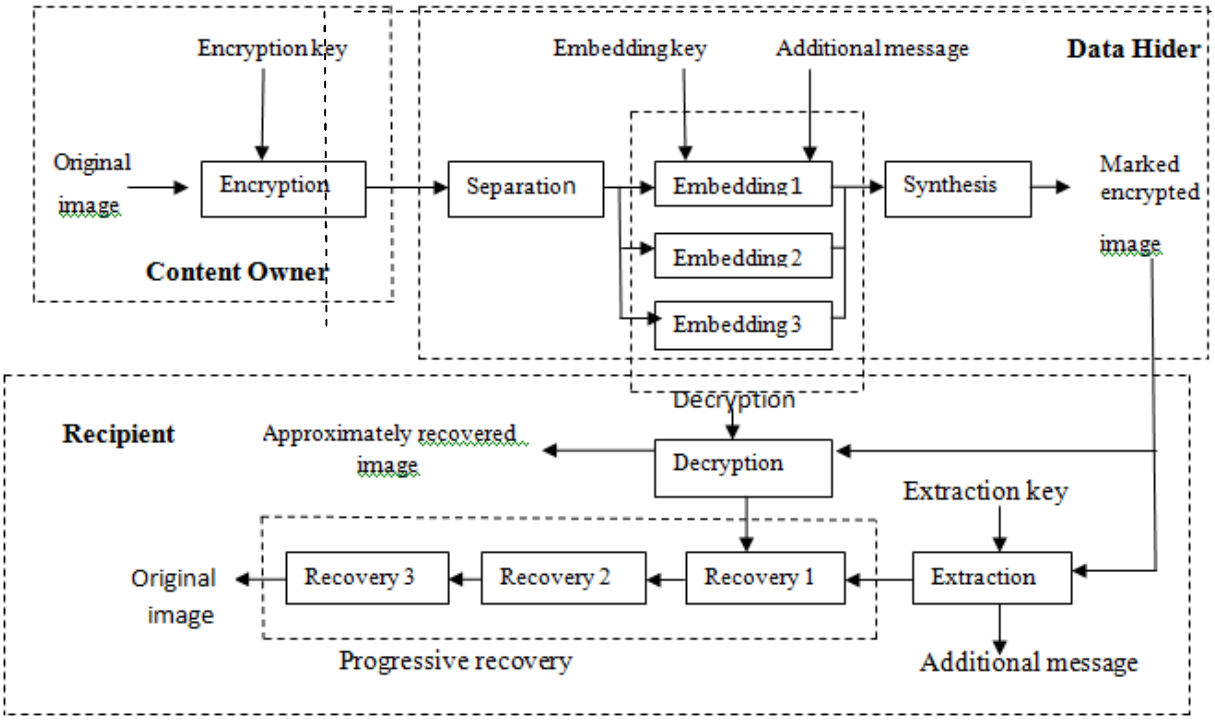


Fig 1. Block diagram of progressive recovery of an RDH-EI

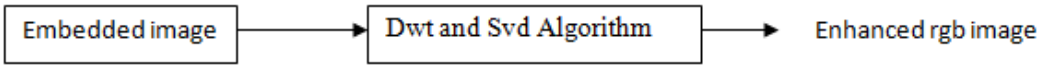


Fig 2.frame work of proposed method

III.EXTENSION TO THE PRPOSED SYSTEM

A. Discrete Wavelet Transform (DWT)

In numerical analysis and functional analysis, a **discrete wavelet transform** (**DWT**) is any wavelet transform for which the wavelets are discretely sampled. As with other wavelet transforms, a key advantage it has over Fourier transforms is temporal resolution: it captures both frequency and location information (location in time).

HAAR WAVELET TRANSFORM

The first DWT was invented by Hungarian mathematician Alfréd Haar. For an input represented by a list of 2^n numbers, the Haar wavelet transform may be considered to pair up input values, storing the difference and passing the sum. This process is repeated recursively, pairing up the sums to prove the next scale, which leads to 2^n-1 differences and a final sum.

$$\Psi(t) = \begin{cases} 1, & 0 \le t \le \frac{1}{2}, \\ -1, & \frac{1}{2} \le t < 1, \\ 0 & otherwise. \end{cases}$$

$$\varphi(t) = f(x) = \begin{cases} 1, & 0 \le t < 1, \\ 0, & otherwise \end{cases}$$

For every pair n, k of integers in **Z**, the **Haar function** $\psi_{n,k}$ is defined on the real line **R** by the formula

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor & UGC Approved Journal)

Website: www.ijirset.com

Vol. 6, Issue 8, August 2017

$\Psi_{n,k}(t)=2^{n/2}\ \Psi(2^n t - k),\ t \in R.$

$\int_R \Psi_{n,k}(t)\, d = 0, \quad \|\Psi_{n,k}\|^2_{L^2(R)} = \int_R \Psi_{n,k}(t)^2 dt = 1$

The Haar functions are pairwise orthogonal,

$\int_R \Psi_{n1,k1}(t)\Psi_{n2,k2}(t)dt = \delta_{n1,n2}\ \delta_{k1,k2}$

where $\delta_{i,j}$ represents the Kronecker delta. Here is the reason for orthogonality: when the two supporting intervals $I_{n1,k1}$ and $I_{n2,k2}$ are not equal, then they are either disjoint, or else, the smaller of the two supports, say $I_{n1,k1}$, is contained in the lower or in the upper half of the other interval, on which the function $\Psi_{n2,k2}$ remains constant. It follows in this case that the product of these two Haar functions is a multiple of the first Haar function, hence the product has integral 0.

The **Haar system** on the real line is the set of functions

$\{\Psi_{n,k}(t); n \in Z, k \in Z\}$.

B. Singular Value Decomposition

In linear algebra, the **singular value decomposition** (**SVD**) is a factorization of a real or complex matrix. It is the generalization of the Eigen_decomposition of a positive semi_definite normal_matrix (for example, a symmetric matrix with positive Eigen values) to any m x n matrix via an extension of the polar decomposition. It has many useful applications in signal processing and statistics.

Formally, the singular value decomposition of an m x n real or complex matrix M is a factorization of the form $U\Sigma V^*$, where U is an m x m real or complex unitary matrix, Σ is a m x n rectangular diagonal_matrix with non-negative real numbers on the diagonal, and V is an n x n real or complex unitary matrix. The diagonal entries σ_i of Σ are know as singular values of M

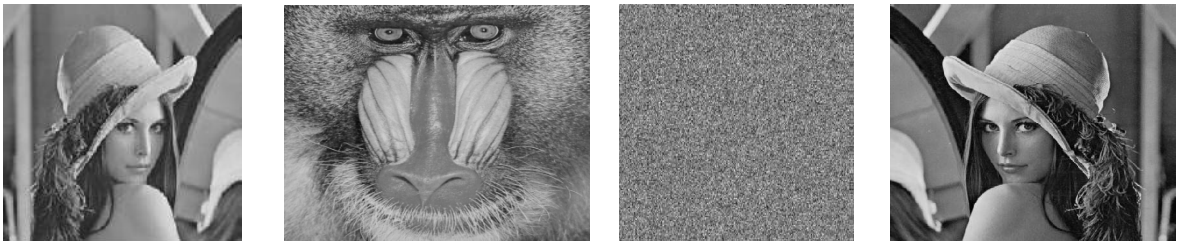
The columns of U and the columns of V are called the **left-singular vectors** and **right-singular vectors** of M, respectively.

The singular value decomposition can be computed using the following observations:

- The left-singular vectors of **M** are a set of orthonormal eigenvectors of $\mathbf{MM}^*$.
- The right-singular vectors of **M** are a set of orthonormal eigenvectors of $\mathbf{M}^*\mathbf{M}$.
- The non-zero singular values of **M** (found on the diagonal entries of $\mathbf{\Sigma}$) are the square roots of the non-zero eigenvalues of both $\mathbf{M}^*\mathbf{M}$ and $\mathbf{MM}^*$.

Applications that employ the SVD include computing the pseudo_inverse, least squares fitting of data, multivariable control, matrix approximation, and determining the rank, range and null space of a matrix.

IV .EXPERIMENTAL RESULTS



A)Original Image B)Secret Image C)Marked Encrypted Image D)Losslessly Recovered Image

Fig 1.Output Of Existing System

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor & UGC Approved Journal)

Website: www.ijirset.com

Vol. 6, Issue 8, August 2017

A)Original Image B) Secret Image C) Embedded Image D)Recovered Image

Fig 2. Output of proposed system

The proposed method is compared with the separable RDH-EI method in [10]. Both methods embed message into three LSB-layers of the encrypted image. Maximal embedding rates Re of the different images are shown in Table I, where Re stands for the embedding rate (bit-per-pixel, bpp). We use a parameter P=5 in the proposed method, equaling to S=5 in [10]. The parameter L used in [10] means the segment length. Other parameters also are listed in Table I. The results show that the proposed method achieves a better embedding rate. We also compare the average of maximal embedding rates in the proposed method with other methods. Algorithms in [5]~[7] and [10] are implemented in 50 natural images sized 512×512 with various features. When calculating maximal embedding rates, we use P=5 and ensure the lossless recovery. All methods use three LSB-layers of the encrypted image for data hiding.

The previous reversible data hiding in encrypted image based on progressive recovery only for gray scale image , the rgb image recovery is not possible .So the proposed extension system provides the recovery of an rgb image with enhanced image format by using DWT and SVD algorithm .Here in this the image is segmented and compared nonlinearly and all the pixels are compared with LL,LH,HL,HH process to segment each pixel and count the 3 valued real numbers of LL,LH,HL for recovery of an original encrypted image without any loss.

The LSBs of three layers is counted and stored in host by embedding process and final image recovery completed by progressive recovery.

V .CONCLUSION

Based on our previous work, a new RDH-EI protocol for three parties is proposed in this paper. Main improvement is extending the traditional recovery to the progressive based recovery. The progressive recovery based RDH-EI provides a better prediction way for estimating the LSB-layers of the original image using three rounds, which outperforms state-of-the-art RDH-EI methods. Since RDH-EI is equivalent to a rate-distortion problem, capability of the method should be evaluated by both the distortion and the embedding rate. For a fair comparison, this paper limits the distortion to three LSB-layers, and accordingly improves the embedding rate.

REFERENCES

[1] X. Hu, W. Zhang, X. Li, and N. Yu, Minimum Rate Prediction and Optimized Histograms Modification for Reversible Data Hiding, IEEE Transactions on Information Forensics and Security, 10(3): 653-664, 2015
[2] X. Li, W. Zhang, B. Ou, and B. Yang. A brief review on reversible data hiding: current techniques and future prospects, IEEE China Summit & International Conference on Signal and Information Processing (ChinaSIP), 426-430, 2014
[3] H. Wang, W. Zhang, and N. Yu, Protecting Patient Confidential Information based on ECG Reversible data hiding, Multimedia Tools and Applications, doi:10.1007/s11042-015-2706-2,2015
[4] Z. Fu, X. Sun, Q. Liu, et al. Achieving efficient cloud search services: Multi-keyword ranked search over encrypted cloud data supporting parallel computing, IEICE Transactions on Communications, 98(1): 190-200, 2015
[5] X. Zhang, Reversible data hiding in encrypted images, IEEE Signal Processing Letters, 18(4): 255–258, 2011 [6] W. Hong, T. Chen, and H. Wu, An improved reversible data hiding in encrypted images using side match, IEEE Signal Processing Letters, 19(4): 199–202, 2012
[7] M. Li, D. Xiao, A. Kulsoom, and Y. Zhang, Improved reversible data hiding for encrypted images using full embedding strategy, Electronic Letters, 51(9): 690-691, 2015 [8] J. Zhou, W. Sun, L. Dong, et al. Secure reversible image data hiding over encrypted domain via key modulation, IEEE Transactions on Circuits and Systems for Video Technology, 26(3): 441-452, 2016
[9] Z. Qian, X. Zhang, and S. Wang, Reversible data hiding in encrypted JPEG bitstream, IEEE Transactions on Multimedia, 16(5): 1486-1491, 2014
[10] X. Zhang, Separable reversible data hiding in encrypted image, IEEE Transactions Information Forensics and Security, 7(2): 826–832, 2012

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor & UGC Approved Journal)

Website: www.ijirset.com

Vol. 6, Issue 8, August 2017

[11] Wu X, Sun W. High-capacity reversible data hiding in encrypted images by prediction error, Signal processing, 104: 387-400, 2014
[12] Z. Qian, and X. Zhang, Reversible data hiding in encrypted image by distributed encoding, IEEE Transactions on Circuits and Systems for Video Technology, 26(4): 636-646, 2016
[13] X. Zhang, Z. Qian, G. Feng and Y. Ren, Efficient reversible data hiding in encrypted images, Journal of Visual Communication and Image Representation, 25(2): 322-328, 2014
[14] K. Ma, W. Zhang, et al. Reversible data hiding in encrypted images by reserving room before encryption, IEEE Transactions Information Forensics and Security, 8(3): 553-562, 2013
[15] X. Cao, L. Du, X. Wei, et al. High capacity reversible data hiding in encrypted images by patch-level sparse representation, IEEE Transactions on Cybernetics, 46(5): 1132-1143, 2016.
[16] Gogovi, Gideon Kwadzo," Digital Image Processing Via Singular Value Decomposition".
[17]H. Andrews; C. Patterson" Singular value decompositions and digital image processing" IEEE Transactions on Acoustics ,Speech, and Signal Processing (Volume: 24, Issue:1, Feb 1976)
[18] P. Srilakshmi; Ch. Himabindu Image watermarking with path based selection using DWT & SVD "10.1109/ICCIC.2016.7919658,