https://dx.doi.org/10.22161/ijaers.4.8.13 *ISSN: 2349-6495(P) | 2456-1908(O)*

Block Transformation for Encrypted Image through RDH

Pavana K P[1], Mrs. Aritri D.Ghosh[2]

[1]Student M.Tech Digital electronics, Dept. of ECE, CMR Institute of technology, Bengaluru, India
[2]Assistent Professor Dept. of ECE, CMR Institute of technology, Bengaluru, India

Abstract*—For a greater amount of ubiquity of information outsourcing to cloud, it may be vital to preserve those security of information furthermore empower those cloud server should handle the information effortlessly toward same period. With accomplish such requirements, "Reversible Data hiding by Encrypted image (RDH EI)" makes enormous challenge for analysts. In this novel, proposed a framework for "Block transformation for EI through RDH". Contrasting with past Encryption based schemes, RDH EI based framework let the user to transmit the semantic of original image into semantic of target image with similar size. The transmitted picture or image looks similar as target image, which is utilized as Encrypted image (EI), and will outsource to Cloud server. Hence, Cloud server can embed the data into EI through RDH technique for Plain text image. Also image can retrieve back as original without any degradation. Data hiding will be done by least significant bit replacement, also RIT mainly includes block pairing and block transformation process which satisfies image quality.*

Keywords— Reversible image transformation (RIT), Encrypted image (EI), LSB, Reversible data hiding (RDH).

I. INTRODUCTION

These days outsourced capacity through cloud gets more mainstream service, particularly to media files such as images, videos, which have huge storage room. On deal with the outsourced images, those cloud server might implant A percentage extra information under the images, for example, picture classification Also documentation data and utilization such information should identify those ownership alternately check the integument from claiming pictures. Also reversible data hiding technology is needed, by which the original image can be losslessly restored after the embedded message is extracted. Data security basically means protection of data from illegal users and provides high security to check data medication. This area of data security has gained more attention over the recent period of time due to the huge increase in data transmission rate over the network. In order to recover the security types in data transfers over the internet, many techniques have been developed like: cryptography, steganography. Also cloud service for outsourced storage makes it interesting to protect the privacy of image contents. For instance, recently many private photos of actress leaked from cloud. For this RDH is helpful for managing the outsourced images, it cannot protect the image content, encryption is the most popular technique for protecting privacy. So it is fascinating to implement RDH in encrypted images but will not get any information about the image contents. Inspired by the needs of privacy protection, many methods have been presented to extend RDH methods to encryption domain. From the viewpoint of compression, these methods on RDH-EI belong to the frameworks [14] "vacating room after encryption (VRAE)" and "reserving room before encryption (RRBE)"

For both frameworks, VRAE and RRBE the image owner will send a cipher text formed image to the cloud. However the cipher texts with the special form of messy codes are easy to cause the attention of the cloud server who may try to dig out information on the encryption users. In fact the cloud server is assumed to be curious to collect information from the outsourced files [15], and obviously the encrypted images are more attractive to a curious cloud server. Therefore, the fact that the user is outsourcing encrypted images, itself is also a kind of privacy of the user, which should be protected.

II. LITERATURE REVIEW

There are many techniques available for reversible data hiding in encrypted image as follows Lai et al. [2] propose an image transformation technique, which selects a target image similar to the secret image, then replaces each block of the target image by a similar block of the secret image and embeds the map between secret blocks and target blocks; it forms an Encrypted image of the secret image. A greedy search method is used to find the most similar block. Although Lai et al.'s method is reversible, it is only suitable for a target image similar with the secret image, and the visual quality of encrypted image is not so good.

https://dx.doi.org/10.22161/ijaers.4.8.13 *ISSN: 2349-6495(P) | 2456-1908(O)*

In 2003 J Tian proposed the "reversible data embedding (RDE) utilizing of difference expansion" [7]. He presented a max-capacity with high-quality, RDE technique for digital-images. This technique can apply for both digital-audio & for digital-video also. He evaluates the dissimilarity between neighboring pixel-values. In this paper author considered only grayscale images. The author explored the redundancy in digital-images, which achieved a high embedding capacity, and remain the distortion law. This correspondence [3] proposed a lossless, reversible and data hiding schemes for public-key-encrypted images probabilistic and homomorphic properties of cryptosystems. With these schemes, the pixel reorganization is avoided and the encryption/decryption is performed on the cover pixels directly so that the amount of encrypted data and the computational complexity are lowered. Due to data embedding on encrypted domain may result in a little bit distortion in plaintext domain due to the homomorphic property, the embedded data can be extracted and the original content can be recovered from the directly decrypted image. With the combined technique, a receiver may extract a part of embedded data before decryption, and extract another part of embedded data and recover the original plaintext image after decryption This technique [5] Z Qian et al proposed a "Distributed Source coding (DSC) with RDH in EI". After Encryption of 0riginal image by content user, the Data Hider compress the elected bits series considered from encrypted image which makes the room for secret-data/message. From the receiver side, secret bit sequence can be withdraw if the receiver know unique embedding key. If receiver knows encryption-key then he can recuperate original image exactly with higher-quality by using image estimation algorithm. Finally if receiver knows "Embedded key" & "Encryption-key", then receiver can embed the secret message and perfectly recover the actual image by utilizing of "Distributed source decoding method". The aim of author is to enhance the embedding payload in encrypted-images. So he applied the separable RDH methodology for encrypted images through "Slepian-wolf source encoding" mechanism. He concludes that his work achieves the great embedding payload with good image recovery quality, and avoids the room reserving operations by the sender.

The reversibly embed the message into the host sequence by modifying its histogram with methods like histogram shifting [6]. Recently, Zhang et al. proposed the optimal histogram modification algorithm [8], for RDH by estimating the optimal modification probability. Zhang divided the encrypted image into several blocks. By flipping 3 LSBs (least significant bits) of the half of pixels in each block, room can be vacated for the embedded bit. The data extraction and image recovery proceed by finding which part has been flicked in one block. This process can be recognized with the help of spatial association in the decrypted image. The decoder side by further exploiting the spatial correlation using a dissimilar estimation equation and side match technique. For both methods in [10] and [11], decrypting image and extracting data must be jointly executed. Recently, Zhou et al. [12] proposed a novel RDH-EI method for joint decryption and extraction, in which the correlation of plaintexts is further exploited by distinguishing the encrypted and non-encrypted pixel blocks with a two-class SVM classifier. To separate the data extraction from image decryption, Zhang [13] emptied out space for data embedding by directly using the typical manner of cipher text compression that is, compressing the encrypted pixels in a lossless manner by using the syndromes of parity-check matrix of channel codes. Recently Weiming Zhang, Hui Wang, Dong dong Hou, and Nenghai Yu propose a novel context [1], for RDH-EI based on reversible image transformation (RIT). Dissimilar from all preceding encryption-based frameworks, in which the encryption texts may attract the notation of the curious cloud, RIT-based context allows the user to transform the contented of original image into the content of another cover image with the same size. The transformed image that looks similar as the cover image is used as the "encrypted image," Reversible data hiding in images is a technique that hides data in digital images for secret communication. It is a method to hide other missive into cover media with a revocable manner so that the innovative cover content can be perfectly restored after extraction of the hidden message. In this paper will be using the method as [1] for transformation where the concept of mosaic image for data security, dividing the image into blocks with respect to cover and will be doing data hiding using LSB replacement with less complexity also achieved exact recovery by extracting the hidden data.

III. PROPOSED SYSTEM

Here in this we proposed framework for RDH-EI by using reversible image transformation (RIT). RIT transforms the content of original image I into the content of another target image J, with equal size and the transformed image looks similar as target image or cover image which will be used as "encrypted image" and which will be outsourced to cloud. And cloud server can embed data into the encrypted image using RDH method that is least significant bit replacement with less complexity and gives high quality of image also original image can be retrieved back in lossless way through encryption key.

https://dx.doi.org/10.22161/ijaers.4.8.13 *ISSN: 2349-6495(P) | 2456-1908(O)*

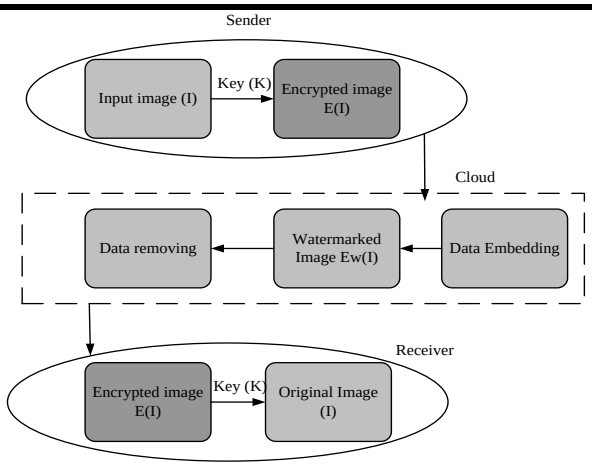


Fig.1: Proposed system

For color images, we transform the color channel R, G, and B respectively in the same manner. So we just take gray images (one channel) as an example to describe the method. For an original image I, we randomly select a target image J having the same size with I from an image database. Firstly, we divide the original image I and the target image J into N non-overlapping blocks respectively, and then pair the blocks of I and J as a sequence such that $(B_1,T_1),...,(B_N ,T_N)$, where B_i is an original block of I and T_i is the corresponding target block of J, $1 \leq i \leq N$. We will transform B_i toward T_i and generate a T_i' similar to T_i. After that, we replace each T_i with T_i' in the target image J to get the transformed image J'. Finally we embed some accessorial information (AI) into J' with an RDH method and generate the ultimate "encrypted image" E(I).These AI is necessary for recovering I from J'. Before being embedded, these AI will be compressed and encrypted with a key K shared with the receiver, so only a receiver having K can decrypt E(I). the proposed transformation process consists of three steps: block pairing, block transformation and AI embedding.

A. BLOCK PAIRING

To make the transformed image J' look like target image J, we hope, after transformation, each transformed block will have close mean and standard deviation (SD) using equation (1) and (2) with the target block. So we first compute the mean and SD of each block of I and J respectively. Let a block B be a set of pixels such that B = {p1, p2,..., pn}, and then the mean and SD of this block is calculated as follows:

$$u = \frac{1}{n}\sum_{i=1}^{n} p_i \qquad (1)$$

$$\sigma = \sqrt{\frac{1}{n}\sum_{i=1}^{n}(p_i - u)^2} \qquad (2)$$

When matching blocks between original image and target image, we hope two blocks with closest SDs to be a pair. In Lee et al.'s method, the blocks of original image and target image are sorted in ascending order according to their SDs respectively, and then each original block is paired up with a corresponding target tile in turn according to the order. To recover the original image from the transformed image, the positions of the original blocks should be recorded and embedded into the transformed image with an RDH method. If the image is divided into N blocks, N log N bits are needed to record block indexes. Obviously, the smaller the block size is, the better the quality of transformed image will be, but which will result in a large N. therefore, the amount of information used to record the index for each block may be so large that it will cause much distortion when embedding these information into the transformed image. In fact there may not exist enough redundant space to store these additional information. For instance, if we divide a 1024×1024 image into 4×4 blocks, 2^{16} ×16 bits are needed to record the positions of blocks. To compress the block indexes, we first classify the blocks according to their SD values before pairing up. In fact, we found that the SD values of most blocks concentrate in a small range close to zero and the frequency quickly drops down with the increase of the SD value from boss base image database. Therefore we divide the blocks into two classes with unequal proportions class 0 for blocks with smaller SD, and class 1 for blocks with larger SD and pair up the blocks belonging to the same class. By assigning the majority of blocks to the class 0, we can avoid the large deviation of SDs between a pair of blocks and efficiently compress the indexes at the same time. In this paper, we propose to divide both the original and target images into non-overlapping 4× 4 blocks and calculate the SDs of each block. We first divide the blocks of original image I into 2 classes according to the quantile of SDs. Denote that the %α quantile of SDs by N_α, We assign the blocks with SDs $\in$ [0, N_α] to "Class 0," and blocks with SDs $\in$ (N_α , N_{100}] to "Class 1." And then we will scan the blocks in the raster order, i.e., from left to right and from top to bottom, and assign a class label, 0 or 1, to each block. Next, we label the blocks of target image based on the classes' volumes of original image. Assuming that the i^{th} class in the original image includes n_i blocks for i= 0 or 1, we scan the target image in the raster order, and label the first n_0 blocks with the smallest SDs as Class 0, and the rest n_1 blocks as Class 1. As a result, each class in the target image includes the same number of blocks as the

https://dx.doi.org/10.22161/ijaers.4.8.13 *ISSN: 2349-6495(P) | 2456-1908(O)*

corresponding class in the original image. We pair the original block up with target block in the following manner. Scan the original image and target image in raster order respectively and pair the j^{th} block of the class *i* in the original image up with the j^{th} block of the class i in the target image for i = 0, 1 and j= 1, . . . , n_i. For each pair of blocks (B,T), as will see later section, the original block *B* will be transformed to target block *T* by mean shifting and block rotation, yielding T. By replacing each T with T' in the target image, the sender will generate the transformed image. Note that both operations of mean shifting and block rotation will not change the SD value, so T' has the same SD as B. Therefore, the SDs in transformed image is only a permutation of those in original image. When classifying the blocks of transformed image according to %α quantile of SDs, the receiver can get a CIT that is same with the CIT of target image. Therefore to restore the original image from the transformed image, the receiver only needs to know the CIT of the original image.

B. BLOCK TRANSFORMATION

Let the original block B = {p_1, p_2,⋯, p_n}, and the corresponding target block T = {p_1',p_2'….,p_n'}. And calculate the means of B and T and denote them by u_B and u_T respectively. The transformed block T'= {p_1", p_2",…..p_n"} is generated by the mean shifting as follows:

$$p_i" = p_i + u_T - u_B \quad (3)$$

Where ($u_T - u_B$) is the difference between the means of target block and original block. We want to shift each pixel value of original block by amplitude ($u_T - u_B$) and thus the transformed block has the same mean with the corresponding target block. However, because the pixel value p_i" should be an integer, to keep the transformation reversible, we round the difference to be the closest integer as

$$\Delta u = \text{round}\,(u_T - u_B) \quad (4)$$

And shift the pixel value by Δu, namely, each p_i" is gotten by

$$p_i" = p_i + \Delta u \quad (5)$$

Note that the pixel value p_i" should be an integer between 0 and 255, so the transformation may result in some overflow/underflow pixel values. To avoid such transformed blocks abstained by (5), we assume that the maximum overflow pixel value is OVmax for Δu ≥0 or the minimum underflow pixel value is UNmin for Δu<0. If overflow/underflow occurs in some blocks, we eliminate them by modifying Δu

$$\Delta u = \begin{cases} \Delta u + 255 - OV_{max}, & \text{if } \Delta u \geq 0 \\ \Delta u - UN_{min}, & \text{if } \Delta u < 0 \end{cases}$$

(6)

We use the modified Δu to shift the pixels of block B, and thus all the pixels' values are controlled into the range of [0,255]. However the range of Δu's value is still very large which cannot be efficiently compressed. Thus we further modify Δu as

$$\Delta u = \begin{cases} \lambda \times round(\frac{\Delta u}{\lambda}), & \text{if } \Delta u \geq 0 \\ \lambda \times floor(\frac{\Delta u}{\lambda}) + \frac{\lambda}{2}, & \text{if } \Delta u < 0 \end{cases}$$

(7)

In which the quantization step, λ, is an even parameter. Then it just needs to record Δu'=2 |Δu|/λ, by which it has the advantage of not to record the sign of Δu. Because when Δu' is an even number it means Δu ≥0 and when Δu' is an odd number it means Δu<0. Since when λ is large the amount of information recording Δu' will be small but the offset between the modified Δu and the original Δu will be large, a tradeoff must made by choosing λ. We set λ =8 in the following experiments. Finally, to maintain the similarity between the transformed image and target image as much as possible, we further rotate the shifted block into one of the four directions 0^0, 90^0, 180^0 or 270^0. The optimal direction is chosen for minimizing the root mean square error (MSE) between the rotated block and the target block. After shifting transformation and rotation, we get a new block T'. With these new blocks, we replace the corresponding blocks in the target image and generate the transformed image J'. The parameters, Δu' and rotation directions, will be compressed, encrypted and then embedded into the transformed image J' as AI to output the "encrypted image" E (I).

C. REVERSIBLE DATA HIDING

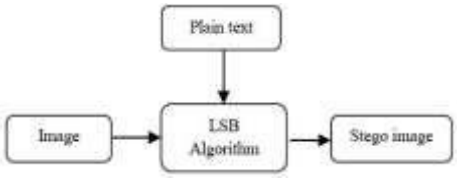


Fig.2. Embedding data

Fig.3. Reverse data hiding

Message encoding on an image can be divided in to two parts, one portion is data hiding other is reversible data hiding. In data hiding part there is a digital image in which we encode secret message by removing LSB of image pixel and add our secret message on corresponding LSB position, then the output image is called stego image. For retrieve the secret message program splits the image into its channels and applies the inverse lifting

https://dx.doi.org/10.22161/ijaers.4.8.13 *ISSN: 2349-6495(P) | 2456-1908(O)*

scheme to each channel to the level specified by the user. When the transformation is completed, the program retrieves the message out of the pixels of the cover image. Different streams of digital media can be used as a cover stream for a secret message. Stegnography is the art of writing secret message so that only the sender and the intended recipient are aware of the hidden message. A successful information hiding should result in the extraction of the hide data from the image with high degree of data integrity. Current trends favor using digital image files as the cover files to hide another digital file that contains the secret message or information.

IV. RESULT

The experimental result for the method block transformation, embedding the data, restoration achieved through MAT lab tool using GUI, MAT lab implements GUIs as figure windows containing various styles of control objects, there we must program each object to perform the intended action when activated by the user of the GUI, all of these tasks are simplified by GUIDE, The process of implementing a GUI involves two tasks that is

- Layout the GUI components
- Programming the GUI components

GUIDE primarily is a set of layout tool. Which generates an M-file that contains code to handle the initialization and launching GUI also this file provides a frame work for the implementation of the callbacks the functions that execute when users activate components in the GUI, and FIG- file contains a complete description of the GUI figure

Let us show complete result analysis, by taking original image as lenna image and target image or cover image as baboon image which is shown below of equal size as 1024x1024 and done reversible image transformation process as explained and data hiding will gives the following outputs,

(a) *(b)*

Fig.4. (a) Original image. (b) Cover image

Once we select with the images, will be doing block pairing step where can see the plots for SD value distribution as shown below

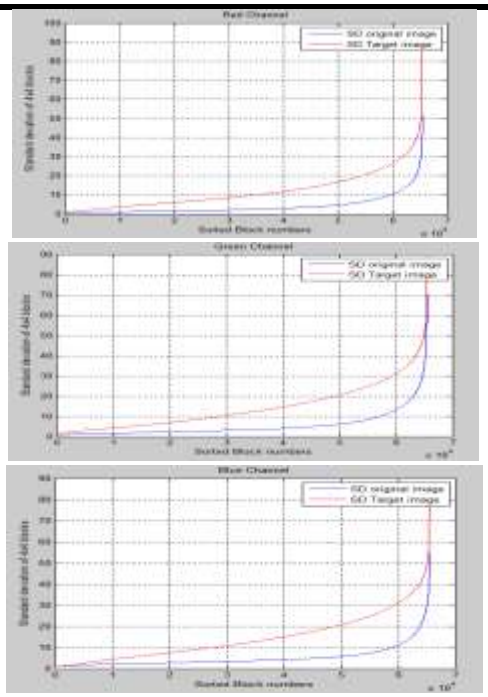
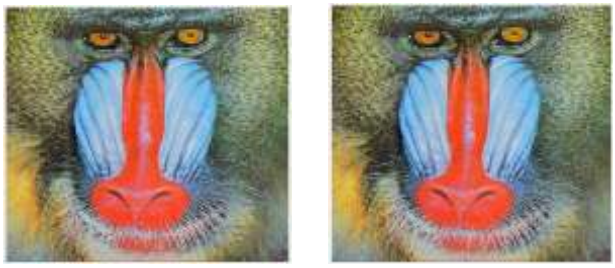


Fig.5. Plots of SD values for R G B channel

Later will do transformation step by considering several mathematical steps as explained above and embed the data into the transformed image using LSB replacement, corresponding transformed and embedded image will be shown below



(a) *(b)*

Fig.6. (a) Transformed image. (b) Embedded image

To recover image back, we need to extract the hidden data and do anti transformation gives the recover image which is as same as original that is called lossless recovery. Which will be shown in below figures

(a) *(b)*

Fig.7. Recover image. (a) Wright key. (b) Wrong key

https://dx.doi.org/10.22161/ijaers.4.8.13 *ISSN: 2349-6495(P) | 2456-1908(O)*

V. CONCLUSION

The proposed work formulates the novel for "RDH EI" which allows the secure block transmission for EI. "RIT" based "RDH - EI" changes the content of original image into content of another target image where secure the original image contents by transforming entire original to target and the outcome looks target image which is also the encrypted image. Since an EI contains plaintext image form, which neglect the annotation of cloud server. That will free from cloud server to select any conventional RDH method for plaintext image to implant watermark. Here the reversible image transmission based scheme will be used to restore as the original image in lossless fashion hence it achieves reversibility. From this technique, user can transmit the actual image to randomly selected cover image with equal size. Also the method fulfill the requirements on image quality with embedding capacity. Since the method works with key, gives back original image with maximum accuracy hence the method most helpful for all secured communication systems.

REFERENCES

[1] Weiming Zhang, Hui Wang, Dong dong Hou, and Nenghai Yu propose a novel framework for RDH-EI based on reversible image transformation IEEE Trans on Multimedia, vol.18, no.8, aug 2016.

[2] I.-J. Lai and W.-H. Tsai, "Secret-fragment-visible mosaic image–a new computer art and its application to information hiding," IEEE Trans. Information Forensics and Security, vol. 6, no. 3, pp. 936–945, 2011.

[3] Xinpeng Zhang, Jing Long, Zichi Wang, and Hang Cheng, "Lossless and Reversible Data Hiding in Encrypted Images with Public Key Cryptography," IEEE Trans. on Circuits and Systems for Video Technology, 2015.

[4] X. Hu, W. Zhang, X. Li, and N. Yu, "Minimum rate prediction and optimized histograms modification for reversible data hiding," IEEE Trans. Inf. Forensics Security, vol. 10, no. 3, 653–664, Mar. 2015.

[5] Z. Qian, and X. Zhang, "Reversible data hiding in encrypted image with distributed source encoding," IEEE Trans. on Circuits and Systems for Video Technology, vol. 26, no. 4, pp. 636-646, Apr. 2016.

[6] Z. Ni, Y .Shi, N. Ansari, and S. Wei, "Reversible data hiding," IEEE Trans. Circuits Syst. Video Technol., vol. 16, no. 3, pp. 354–362, Mar. 2006.

[7] J. Tian, "Reversible data embedding using a difference expansion," IEEE Trans. Circuits Syst. Video Technol., vol. 13, no. 8, pp. 890–896, Aug. 2003.

[8] W. Zhang, X. Hu, X. Li, and N. Yu, "Recursive histogram modification: Establishing equivalency between reversible data hiding and lossless data compression," IEEE Trans. Image Process., vol. 22, no.7,pp.2775–2785, Jul. 2013.

[9] X. Zhang, "Reversible data hiding in encrypted images," IEEE Signal Process. Lett., vol. 18, no. 4, pp. 255–258, Apr. 2011.

[10] W. Hong, T. Chen, and H. Wu, "An improved reversible data hiding in encrypted images using side match," IEEE Signal Process. Lett., vol. 19, no. 4, pp. 199–202, Apr. 2012.

[11] J. Zhou et al., "Secure reversible image data hiding over encrypted domain via key modulation," IEEE Trans. Circuits Syst. Video Technol., vol. 26, no. 3, pp. 441–452, Mar. 2016.

[12] X. Zhang, "Separable reversible data hiding in encrypted image," IEEE Trans. Inf. Forensics Security, vol. 7, no. 2, pp. 826–832, Apr. 2012.

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

[14] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable, and fine-grained data access control in cloud computing," in Proc. IEEE INFOCOM, Mar. 2010, pp. 1–9.