International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 05 Issue: 04 | Apr-2018 www.irjet.net p-ISSN: 2395-0072

CAMOUFLAGE OF IMAGE BY REVERSIBLE IMAGE TRANSFORMATION

Lija John[1], Vani V Prakash[2]

[1]M.Tech, Dept. of computer science & Engineering, Sree Buddha College of Engineering, Elavumthitta, Kerala, India, 689625
[2] Assistant Professor, Dept. of computer science & Engineering, Sree Buddha College of Engineering, Elavumthitta, Kerala, India, 689625

Abstract - *As the world progresses multimedia data become more and more valuable and thus security concern will increases. Multimedia data includes high percentage of images so its protection is very important to prevent unauthorized usage and data exchange. For that purpose a new RIT technique is proposed. From all existing encryption method, RIT technique let the user to transmute the original image into another target image with the same size. The appearance of transmuted image is similar to the target image which is used as the encrypted image and transmutation can be done between the micro blocks with small size, which enhance the quality of the encrypted image. For the recovery of original image the additional data is added into the encrypted image. For that purpose a novel RDH algorithm is proposed [1][2].*

Key Words: **Introduction, Image Encryption Techniques, Data Hiding Techniques, Camouflage of Image by RIT, RDH Algorithm.**

1. INTRODUCTION

Information transfer through the internet for various applications is limited due to various attacks. Areas like military, medical imaging, telecommunication etc., transfer different types of secret images and data through the internet. So, it is very important to protect these types of images from different security problems.

The two commonly used methods are data hiding and encryption, decryption methods. Information hiding methods are watermarking, anonymity, and steganography. In this method data or images are securely hided inside an image. So it is very difficult to identify the presence of other images or data. Image encryption and decryption method contains conventional encryption and chaotic encryption methods. Here secret images are encrypted by using secret key. Some disadvantages are occurred by data hiding and encryption, decryption method. So a new method called reversible image transformation is developed. Here two types of images are used. The secret image and target image are select with same size. These two images are divided into small pieces and then combine these small pieces to form a transformed image [1].

The small pieces of two images are combining based on mean, standard deviation, CIT, root mean square error. The accessorial information is needed to retrieve the original image from target image. The accessorial information is encrypted by using AES encryption algorithm.

2. RELATED WORKS

2.1 Image Encryption Technique

In [3], image can be protected through the internet by using the method called secret fragment visible mosaic images. Mosaic image are small component of materials like stone, glass, tile etc. In this method, two images are divided into small pieces. Each piece of two images is combined on the basics of color. One of the disadvantages of this method is, (1) tiles are random in position, (2) sometimes one can guess what the image is. Also tiles are composed of different color values, so there is a chance for loss of some of the information.

Lai et al [4], proposes an image transformation technique. In this method target image similar to the secret image. These two images are divided into equal blocks and then replace each block of target image by a similar block of secret image. The most related block is selected by, using the method called greedy search. This method is reversible. One of the disadvantage of this method is visual quality of encrypted image is not so good.

A new procedure for image encryption based on combination of chaotic maps [5]. It is focus on the chaotic digital encryption techniques. Symmetric key chaotic cryptography is used here. In this method, a typical coupled map was added with a one dimensional chaotic map. It provides high degree security image encryption. It is suitable for confidential information can be securely transmitted over the internet. This paper presents the combined mechanism of chaotic maps. It increases the key space and security of algorithm.

Another paper called a symmetric chaos based image cipher with an improved bit level permutation strategy. A symmetric chaos based image cipher with a 3D cat map based on spatial bit level permutation is used. Here bits are shuffled among different bit planes rather than within the same bit plane. This proposed scheme is excellent for online image encryption applications. One problem is that, during the decryption time exact image is not recovered.

1.2 Data Hiding Techniques

In [6] proposed a technique called separable RDHEI framework. Previously, Josephus traversal and a stream cipher was used to embed the additional data into cipher image. A BHS procedure using self-hidden peak pixels is

preferred to perform reversible data embedding. The embedded data can extract by using data hiding key and original image can be extracted by using decryption key. The additional data and original image are extracted if both keys are available. The advantage of this technique is better data embedding capacity, better quality decrypted image, and data can be recover in error free and accurate image reconstruction.

In [7] introduce the technique called RDH in encrypted images using Slepian - Wolf source encoding. Stream cipher is used to encrypt the secret image. After encryption, series of bits are selected and compress to make a room to accommodate the secret data. Here two different keys are used. So this method is separable. The hidden data encrypted by using the embedding key and the secret image can be recovered encryption key. The high quality secret image can be recovered.

In the framework VRAE [8] and [9], the image is encrypted by using the key K. The encrypted image is compressed and makes a space for embedding data. The original image is decrypted by using key K after removing the embedding data and decompression.

In the framework RRBE [10] [11], first reserve room from the image I and encrypted by using the key K. The additional data is embedded into this reserved room. The original image decrypted by using key K and also additional data is obtained.

The PWLC technique [12] uses XOR binary operation to embed the additional information in the original image. In this technique the original image is scan in raster scanning order. The sequences “000000” or “111111” are chosen to hide data. When a 0 bit is inserted the sequence "000000" becomes "001000”. When a bit 1 inserted the sequence "000000" becomes "001100". Also, order “11111" becomes"110111"and "110011" when bits 0 and 1 are inserted respectively.

One of the disadvantage of this technique is, the hidden data does not correctly extract and fails to recover the original image.

2. OVERVIEW

2.1 Proposed System

Camouflage of image by reversible image transformation project is used for secure transmission of images. Here two types of images are present, one is secret image and other is target image in which the secret images are embedding. Firstly secret image are selected. After a target image is selected at random, the given secret image and target are first divided into small pieces called tile images.

Each block of original image is transformed to be that of the corresponding block in the target image, according to a similarity based on standard deviation. The resulting transformed image which look like the target image. The proposed method can transform a secret image into a target image without compression. A novel RDH method is used to embed accessorial information into transformed image [1].

2.2 Ideas of Camouflage of Image by RIT [1]

The proposed transformation process involves three steps: block pairing, block transformation, accessorial information embedding. The third step can be done by any RDH method.

The same size of original image and target image are two images which are used in the proposed transformation technique. Firstly, the original image and target image are divided into equal blocks. The mean and standard deviation of each block of original and target image is calculated.

The mean and standard deviation of each block of two images are calculated as [1],

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

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

The standard deviation of each block close to the range value 0. The large numbers of block indexes are very difficult to compress. It will reduce the quality of encrypted image. So each block of original image and target image are split into two classes. The blocks with smaller standard deviation are undergoes class 0 and blocks with larger standard deviation are undergoes class 1. According to this classification class index table (CIT) is generated. The class index table is easy to compress and will not affect the quality of encrypted image. The block paring is based on CIT of original and target image. Blocks belonging to the same classes are pair up.

Each blocks of original image is transformed to the blocks of target image by mean shifting and block rotation. The mean shifting transformation and block rotation are reversible. In mean shifting transformation, mean of each block pair is calculated and takes the difference. The mean difference is added to the original block. The transformed block is obtained through the mean shifting. The transformed block has same mean with the corresponding target block [1].

In order to maintain the similarity between the transformed image and target image, rotate the shifted block into one of the four directions are 0^0, 90^0, 180^0, or 270^0. To minimize the RMSE between the rotated block and target block, the optimal direction is chosen. The transformed block is obtained through the mean shifting and block rotation. Each block of target image is replaced with the transformed block and transformed image is obtained [1].

The accessorial information such as SDs, CIT, mean, value of degree of rotation is embedded in to the transformed image.

This accessorial information is compress and encrypted by using AES procedure and embedded into the transformed image by using RDH procedure [1].

Finally an encrypted image is obtained. The accessorial information is important to recover the original image from the transformed image.

The original image obtained by following steps [1]:

1) The accessorial information is extracted and transformed image is obtained.

2) The accessorial information is decrypt by using AES procedure and decompresses the accessorial information such as standard deviation, CIT, mean, rotation value.

3) The transformed image is split into blocks. The standard deviation of each block is calculated and generates the CIT.

4) According to the CITs of original and transformed image, rearrange the blocks of transformed image. The transformed block is obtained.

5) Rotate the transformed block in anti-direction and subtract the mean difference from the transformed block.

Finally, the original image is obtained.

2.3 RDH Algorithm [2]

The accessorial information embedded into the transformed image by using RDH algorithm. It keeps the PSNR value of transformed image high. The proposed algorithm**,** elaborate the contrast of a transformed image to expand its visual quality. The largest two bins in the image histogram are chosen for data embedding. The proposed algorithms presently work in gray level images. But it can be easily extended to color images [2].

RDH embedding procedure [2]:

Input: Transformed image

Output: Final embedded image

(1) First, the operation are performed with pixels in the range of [0, L-1] and [256-L, 255], excluding the first 16 pixels in the bottom row. The location map is used to record the locations of pixels and compress it.

(2) Compute the histogram of image without calculating the first 16 pixels in the bottom row.

(3) The largest two peak value in the histogram is spilt for data hiding by using the Eq.,

$$i' = \begin{cases} i-1, & \text{for } i < I_S \\ I_s - b_k, & \text{for } i = I_S \\ i, & \text{for } I_S < i < I_R \\ I_R + b_k, & \text{for } i = I_R \\ i+1, & \text{for } i > I_R \end{cases}$$

(4) The embedding process continues until L pairs are spilt. The values L, compressed location map, are embedded in the last two peaks. The value of last two peak values are embedded in the LSB from the 16 omitted pixels.

(5) Finally marked image is obtained.

RDH Extraction and Recovery Procedure [2]:

Input: Final embedded image

Output: Transformed image

1) The LSBs of the 16 excluded pixels are retrieved so that the values of the last two split peaks are known.

2) The data embedded with the last two split peaks are recovered. The L value, the compacted location map, the LSBs of 16 excluded pixels, and all the splited peak values are extracted.

3) The process of extraction and recovery are continuing until all of the split peaks are recovered and the data embedded with them are extracted.

4) The transformed image is recovered by using the Eq. [2],

$$i = \begin{cases} i' + 1, & \text{for } i' = I_S - 1 \\ I_S, & \text{for } i' = I_S - 1 \text{ or } i' = I_S \\ I_R, & \text{for } i' = I_R \text{ or } i' = I_R + 1 \\ i' - 1, & \text{for } i' = I_R + 1 \end{cases}$$

3 EXPERIMENTAL ANALYSIS

In the proposed RIT method, both original and target image are divided into 4 × 4 blocks. Then SDs of each block is calculated. According to SDs, each block is classified into two classes. The blocks are assigning with SDs ∈ [0, N_α] to "class 0", and blocks with SDs ∈ (N_α, N_{100}] to "class 1". After labeling the class indexes, a class index table (CIT) is obtained from the original image and target image. CIT is helpful for understanding the processing of block pairing.

The transformation process from original image to secret image is shown in the figure 3.1,

(a) (b) (c)

Fig.3.1. (a)Original image. (b) Secret image. (c) Transformed image.

The RDH algorithm is used to embed the accessorial information. The AES procedure is used to encrypt the AI. The accessorial information such as SDs, CIT, mean are hide into the transformed image. This accessorial information is very necessary to restore the original image. For α in the range of [0.05, 0.95], the variation of AI payload seems to be not large. When α is 0.75, the AI payload reaches the valley value. So, in the experiment α is set 0.75. The appearances of encrypted images obtained by RIT look like similar to the target images. Both RIT and RDH algorithm are reversible.

By using RDH extraction and recovery procedure, the transformed image and AI is obtained from the final embedded image. The information about the original image obtained from decrypting AI. By using this AI information, the original image is loselessly recover from the transformed image.

The histogram of before and after data embedding in transformed image is shown in figure. 3.2.

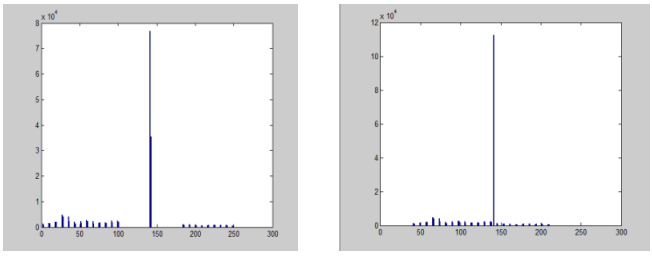

Fig.3.2. (a) Before data hiding in transformed image.(b) After data hiding in transformed image.

4 ANALYSIS

The quality of the encrypted image $E(I)$ is measured by the peak-signal-to-noise ratio (PSNR) defined as;

$$PSNR = 10 \times log_{10}\left(\frac{255^2}{MSE}\right) \quad (1)$$

Where the MSE for an $m \times n$ image is computed by formula;

$$MSE = \frac{1}{m \times n}\sum_{i=1}^{m}\sum_{j=1}^{n}(x_{ij} - y_{ij})^2 \quad (2)$$

Where x_{ij} and y_{ij} denote the pixel values of the target image J and encrypted image $E(I)$, respectively.

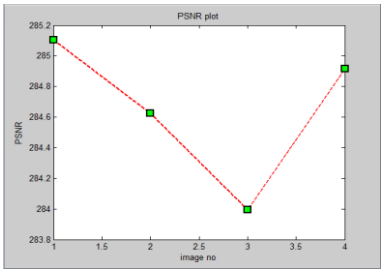

Fig.4.1. Different PSNR values for four input images.

5. CONCLUSION

Camouflage of Image by RIT, which can transform a original image to a selected target image for getting an encrypted image which is used as the encryption of original image with good visual quality, and the original image can be restored without any loss. It can protect the image content. The RDH is used to hide the AI into the transformed image and then form encrypted image. This accessorial information is very necessary to recover the original image. The RDH procedure is reversible. The further work includes improving the RIT, RDH methods and transmuting the two encrypted image (original image) into only one target image and extend idea to the video or audio [1][2].

REFERENCES

[1] Weiming Zhang, Hui Wang, Dongdong Hou, Nenghai Yu: "Reversible Data Hiding in Encrypted Images by Reversible Image Transformation," IEEE Transaction On Multimedia, Vol. 18, No. 8, August 2016.

[2] Hao - Tian Wu , Jean-Luc Dugelay, and Yun - Qing Shi "Reversible Image Data Hiding with Contrast Enhancement," IEEE Signal Processing Letters, Vol. 22, No. 1, January 2015.

[3] Y.-L. Lee and W.-H. Tsai, "A new secure image transmission technique via secret-fragment-visible mosaic images by nearly reversible color transformations," IEEE Trans. Circuits Syst. & Video Technol., vol. 24, no. 4, pp. 695–703, 2014.

[4] 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

[5] S.Behnia, A. Akhshani, H. Mahmodi, and A. Akhavan, "a novel algorithm for image encryption based on mixture of chaotic maps", Chaos Solit. Fract, vol. 35, no. 2, pp. 408419, 2008.

[6] Zhaoxia Yin, Andrew Abel, Xinpeng Zhan, Bin Luo "Reversible Data Hiding In Encrypted Image Based On Block Histogram Shifting," Acoustics, Speech and Signal Processing (ICASSP), 2016 IEEE International Conference on, DOI: 10.1109/ICASSP.2016.7472053, Pages: 2129-2133.

[7] 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.

[8] X. Zhang, "Reversible data hiding in encrypted images," IEEE Signal Processing Letters, vol. 18, no. 4, pp. 255-258, Apr. 2011.

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

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

[11] W. Zhang, K. Ma and N. Yu, "Reversibility improved data hiding in encrypted images," Signal Processing, vol. 94, pp. 118-127, Jan. 2014.

[12] Jaspreet Kaur, Er. Varinderjit Kaur, "A Review on Reversible Data Hiding Techniques" IJCSMC, Vol. 4, Issue. 7, July 2015, pg.334 – 340