ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 8, August 2017

Reversible Data hiding by Reversible image Transformation Algorithm for Encrypted Images

[1] Bharati S Pochal,[2] Gayatri Prasanna
[1] Assistant Professor
[1][2] Department of Computer Applications
[1][2] VTU PG Centre Kalaburgi, Karnataka, India

***Abstract*— The outsourcing data to the cloud is very important to defend privacy of the information and it will allow the cloud server to easily manage the information at the same time. And reversible data hiding in encrypted images (RDH-EI), it will attracts the more and more researchers interest and also we are introduced a framework for RDH-EI based on Reversible Image Transformation that is [RIT]. This one is the unique framework from all other frameworks, in which framework the cipher text may be attract the notation of the interested cloud. This framework permits the client to convert the original image content in to target image content with a similar size, and the transformed image seems like a target image and it is used as an encrypted image and it is outsourced to the cloud. For this the cloud server embeds the data in to encrypted image so easily, by using any RDH techniques for the plain text pictures. Like that we realized that client free scheme for RDH-EI, and this is data embedding process and it will be implemented by the cloud server is unrelated with the both encryption and decryption process, to embed the watermark in the encrypted image we need two RDH techniques, including unified embedding, scrambling scheme and traditional RDH scheme, it can assure different requirements on picture quality and huge embedding capacity.**

***Index Terms*— reversible data hiding, reversible image transformation, privacy protection, outsoured storage in cloud, image encryption.**

1. INTRODUCTION

The current system the outsourced storage by cloud grow to be more and more popular service, especially for multimedia files, like videos or images, these need huge memory space. For managing the outsourced pictures the cloud server may insert some extra data in to the images, like notation information and image category for this we data we are going to identify the ownership or it is going to verify the integrity of images. Apparently, the cloud server has no right to establish permanent alteration during the data inserting into the outsourced pictures. For that we are using Reversible Data Hiding (RDH) technique, by it we can be recovered the original image after the embedded message is extracted. This method is also broadly used in military imagery, law forensics and medical imagery where no distortion of the original cover is allowed.

II. RELATED WORK

[1]In this work they are using analytical strategy combining fractal geometry and grey level co occurrence matrix method or keywords, we are using this paper in our project because our project transformed the original image in to target image and then it will transformed white and black image in to grey color image.

[2] This one is also one of the important paper, it is also very helpful to this project because it uses texture analysis methods, that is it stores the second or higher order statics on the relation between pixel grey level values in matrix form, in this they are used class distance and class difference matrices to achieve the low dimensional adaptive feature vectors for texture classification.

[3] This is also very important for this project it will has several researches one is the introduction of a set of textural measures that capture the particular parameters of cervical textures as professed by human and another one is generalized texture analysis technique it is based on the combination of conventional statistical and structural textural analysis. At last the experimental study of original pictures established the feasibility of the proposed approach in between cervical texture patterns of different phases of cervical lesions.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 8, August 2017

[4] In this paper the author describes the KNN classifier, it is a flexible multivariate statistical classification method, and in this the author included most recently developed wavelet energy parameters. This will also describe the texture in an objective and quantitative means it will combined the set of texture parameters with the relationship of such parameter to the cell properties, and it is also useful to both reduction of the inherently coupled to visual observation and another one is accurate prognosis.

[5] The author of this paper describes the reversible data hiding algorithm, this algorithm is used to recover the original picture without any distortion from the watermarked picture after the hidden data has been extracted, this RDH algorithm uses the zero or the minimum points of the histogram of an image and it is faintly modifies the pixel greyscale points to embed data in to the image, it can also embed the more information than many of current reversible data hiding algorithms, in this paper the lower bound of peak signal to noise ratio is more higher than the reversible data hiding methods are included.

[6] This paper described the Inverse Discrete Wavelet Transform and it is applied to the stego object and this paper also describes the strong verification method based on semantic segmentation, encryption and data hiding and it uses the qualified significant wavelet trees to provide both significant resistance and invisibility against compression and transmission. This paper is useful for the project because the above used methods are also used in the project.

[7] In this paper the author considered logo as watermark and that logo is rooted in to the original input picture to form the watermarked image using Discrete Wavelet Transform algorithm and using Inverse Discrete Wavelet Transform the watermark can be decrypted, for this type the digital watermarking is done.

[8] This one is very important paper that is very helpful for the project because it uses a CLAHE Discrete Wavelet Transform technique, this will has three major steps they are first one, it is decomposed the original image in to high frequency and low frequency components by discrete wavelet transform.

[9] The author of this paper propose a scheme that is compressing the encrypted images with secondary data and this paper is also used in the data compression and image reconstruction, and the image can be reconstructed at recipient side using secret key.

[10] The author of this paper mainly described the strong digital watermarking scheme. It is useful for copyright protection of digital pictures based on sub sampling, and the author used a chaotic map in watermarked picture. For that the output image of watermark is good and strong to attack, this also have problems they are the image quality is low and the watermark is done only in binary picture.

The present system the Reversible Data Hiding techniques on pictures has been proposed, all these methods can be seemed as a procedure of semantic lossless compression, the semantic compression means is that the compressed picture can be close to the original picture, for this we can got a marked picture with fine optical feature.

III. SYSTEM DESIGN

A. Proposed System

Because The proposed system, it can advice a framework that is RDH EI, and also using a reversible image transformation (RIT), it transfers the semantic of the original picture I in to the semantic of another picture J and the reversibility means I can be restored from the transformed picture. Next we are intriguing the original picture as I and the target image as J and then we are going to divide the both unique image and the intention figure in to non extend beyonding obstructs correspondingly and next it will pair the blocks I and J as a sequence like as a (B1, T1) and (BN, TN) where Bi is taken as original block and Ti is taken as the target image block, using key K we can compressed and embedded the information, and the only recipient having this secret key, using this the receiver can decrypt the image. Finally the anticipated transformation progression restrains three varieties of renovation they are block transformation, information embedding and block pairing.

B. Objectives

The main objective of the project is to transforming the Original image in to transformed target image using the reversible data hiding technique.It will transform the RGB image into gray color image using some encryption and decryption AES techniques.

C. Methodology

AES Algorithm: Advanced Encryption standard is a symmetric block cipher. It state that, it will make use of the similar key for mutually Encryption and Decryption. Nevertheless AES is different to a certain extent from DES in a number of manners. And the Rijindael algorithm gives permission to assortment of key and block dimension and not

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 8, August 2017

immediately the size of DES blocks like 64 and 56 bits. The amount of advanced encryption standard factors is dependent on the length of the key.

The algorithms Rijindael have the subsequent qualities:

- In Opposition to all well known attacks.
- Code and speed compression on extensive range of proposals.
- Straight forwardness of design.

D. System Architecture

System design is the process of defining the architecture, components, modules, interfaces and data for a system to satisfy satisfied requirements. System design also considered as the application of system theory which is used to develop the product.

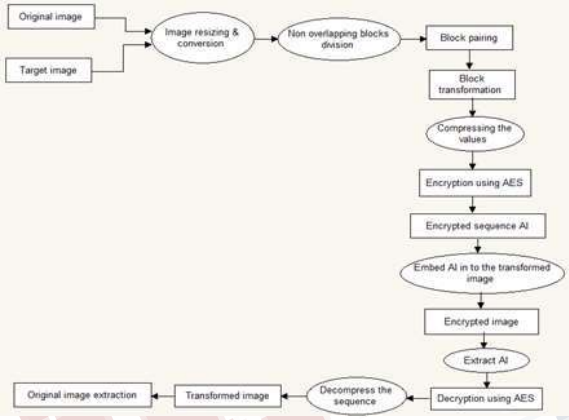

Fig 1: Architecture diagram

IV. IMPLEMENTATION

The Module description

Module Names

- Rescaling And RGB To Gray Conversion
- Non-Overlapping Block Separation
- Computation Of Mean And Standard Deviation
- B lock Pairing
- CIT Table Generation
- Block Transformation
- AES Encryption
- Encrypted Image Generation
- AES Decryption
- Block Anti-Transformation / Reconstruction
- Performance Measurements

Image Rescaling And Color Channel Conversion

The size of the input image and the target image was rescaled to a square matrix. We can convert the RGB image into three channels. The input is the RGB (24bits/pixel) image. The RGB image is converted to grayscale image using RGB to gray conversion process. The output is the grayscale image (8 bits/pixel).

Nonoverlapping Block Generation

Divide both I and J into several non-overlapping 4×4 blocks. Assuming that each image consists of N blocks. 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 (B1, T1) and (BN, TN), where Bi is an original block of I and Ti is the corresponding target block of J, $1 \le i \le N$.

Mean And Standard Deviation Computation

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) 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. while and indicate the local window mean and standard deviation which are defined as:

$$\mu_w = \frac{1}{N^2} \sum_{(i,j)\in(k,l)} p(i,j)$$

$$'_w = \sqrt{\frac{1}{N^2} \sum_{(i,j)\in(k,l)} (p(i,j) - \mu_w)^2}$$

Block Pairing

When matching blocks between original image and target image, we hope two blocks with closest SDs to be a pair. 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.

Cit Table Generation

To compress the block indexes, we first classify the blocks according to their SD values before pairing them 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 Therefore, we divide the blocks into two classes with unequal proportions.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 8, August 2017

Block Transformation

For each pair of blocks (B, T), 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.

AES Encryption

Encrypt the compressed sequence and the parameter by a standard encryption scheme such as AES with the key.

Encrypted Image Generration

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′. Decryption

1) Extract AI and restore the transformed image J′ from E(I) with the RDH scheme.

2) Decrypt AI by AES scheme with the key K, and then decompress the sequence to obtain CIT of I.

3) Divide J′ into non-overlapping N blocks with size of 4 × 4. Calculate the SDs of blocks, and then generate the CIT of J′ according to the % a quantile of SDs. Block

Anti-Transformation/Reconstruction

1) According to the CITs of J′ and I, rearrange the blocks of J′.
2) For each block T ′ i of J′ for 1 ≤ i ≤ N, rotate T ′ i in the antidirection of _i, and then subtract del-ui from each pixel of T ′ i , and finally output the original image I.

PERFORMANCE MEASUREMENTS

PSNR: Peak Signal to Noise Ratio (PSNR) is generally used to analyze quality of image, sound and video files in dB (decibels). PSNR calculation of two images, one original and an altered image, describes how far two images are equal.

$$\mathbf{PSNR(dB) = 10 * \log\left(\frac{255^2}{MSE}\right)}$$

$$\mathbf{MSE = \sum_{i=1}^{x}\sum_{j=1}^{y}\frac{(|A_{ij} - B_{ij}|)^2}{x * y}}$$

2 Algorithm

AES Algorithm

Algorithm 1 Procedure of Transformation
Input: An original image I and a secret key K.
Output: The encrypted image E(I).

1) Select a target image J having the same size as I from an image database.
2) Divide both I and J into several non-overlapping 4×4 blocks. Assuming that each image consists of N blocks, calculate the mean and SD of each block.
3) Classify the blocks with %_ quantile of SDs and generate CITs for I and J respectively. Pair up blocks of I with blocks of J according the CITs as described in subsection III-A.
4) For each block pair (Bi, Ti) (1 ≤ i ≤ N), compute the mean difference _ui. Add _ui to each pixel of Bi 4 and then rotate the block into the optimal direction _i (_i ∈ {0o, 90o, 180o 270o}, which yields a transformed block T ′i .
5) In the target image J, replace each block Ti with the corresponding transformed block T ′i for 1 ≤ i ≤ N and generate the transformed image J′.
6) Collect _ui's and _i's for all block pairs, and compress them together with the CIT of I. Encrypt the compressed sequence and the parameter _ by a standard encryption scheme such as AES with the key K.
7) Take the encrypted sequence as accessorial information (AI), and embed AI into the transformed image J′ with an RDH method such as the one in [7], and output the encrypted image E(I).

Algorithm 2 Procedure of Anti-transformation
Input: The encrypted image E(I) and the key K.
Output: The original image I.
1) Extract AI and restore the transformed image J′ from E(I) with the RDH scheme in [7].
2) Decrypt AI by AES scheme with the key K, and then decompress the sequence to obtain CIT of I, _ui, _i (1 ≤ i ≤ N) and _.
3) Divide J′ into non-overlapping N blocks with size of 4 × 4. Calculate the SDs of blocks, and then generate the CIT of J′ according to the %_ quantile of SDs.
4) According to the CITs of J′ and I, rearrange the blocks of J′ as described in Subsection III-A.
5) For each block T ′i of J′ for 1 ≤ i ≤ N, rotate T ′i in the anti-direction of _i, and then subtract _ui from each pixel of T ′i , and finally output the original image I.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 8, August 2017

V. PERFORMANCE ANALYSIS

The Tool and Technology

Tools: Image Processing Tool Box

This tool box permits to carrying out picture enrichment, diminishing of echo, characteristic credentials, arithmetical amendment, image segmentation, registration of image, as well as deblurring of picture. In this tool box there are two methods they are

1. Fundamental import and export:

Fundamental export and import methods consent to pictures achieved by means of image accomplishment plans for Ex, medical imaging devices, digital cameras such as microscopes, satellite, telescopes, MRI and CT, airborne sensors and other scientific rudiments.

2. Display Function:

This function is used to demonstrate the pictures that are read by means of the import reason. This allows towards making exhibit by means of graphics and wording pictures within a specific display and window for example, histogram, outline plot and so on.

Technologies

1. Mean, standard Deviation

Standard deviation is considered that it facilitates to compute the measure of differentiation or variation of set of data standards, and it is symbolize with sigma sign that is a Greek letter. And a low standard variation signifies that the data points are close to mean of the set. And high standard deviation increase out the number of variety values.

2. Quantile measurement

The quantile structure is accurate method of shaping the level of success in arithmetic of the students and structure has two faces of the similar coin one is for assessing the student's success and one more is for concepts and skills compute, the student assessment state that how much the student has the capacity to understand the skills and idea of mathematical command.

3. Reversible image transformation (RIT)

Reversible data hiding has most necessary transformation technique that is RIT Reversible Image Transformation, it will used for transferring the original picture in to target image allowing for as encrypted image, and it is outsourced to the cloud. For that reason the cloud server insert the data in to encrypted image by naturally.

4. Advanced Encrypted standard (AES)

The highly developed encrypted standard [AES] one of the algorithm of symmetric encryption, it is developed by two persons those are planned for keep the hardware and software as able one, and it wires block length of 128 bits and key lengths of 128, 192 and 256 bits.

RESULTS AND DISCUSSION

1. Original Input Image

Fig 2: Original Input Image

The original image from the Bossbase database is given as the input.

2. Original Input Image-Grayscale

Fig 3: Original Input Image-Grayscale

The RGB Original image is divided into grayscale image.

3. Target Image

Fig 4: Target Image

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 8, August 2017

The target image from the Bossbase database is given as the output.

4. Target Image-Grayscale

Fig 5: Target Image-Grayscale

The RGB target image is divided into grayscale image.

5. Histogram of Original Image

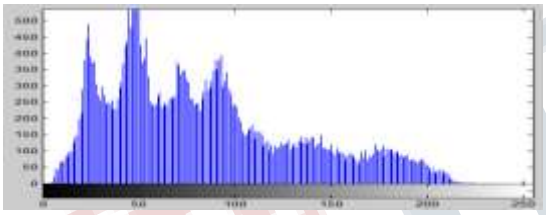

Fig 6: Histogram of Original Image

6. Histogram of Target Image

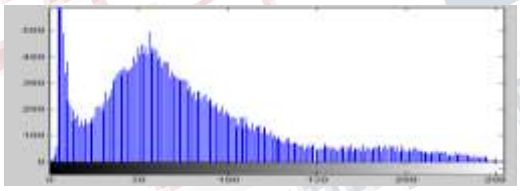

Fig 7: Histogram of Target Image

7. Encryptyed Image

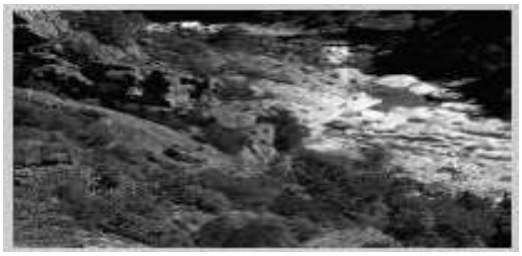

Fig 8: Encryptyed Image

Take the encrypted sequence as accessorial information (AI), and embed AI into the transformed image j' with an RDH method and output the encrypted image.

8. Decrypted Image

Fig 9: Decrypted Image

Decrypt AI by AES scheme with the key K, and then decompress the sequence to obtain CIT of I.

9. Performance Measures

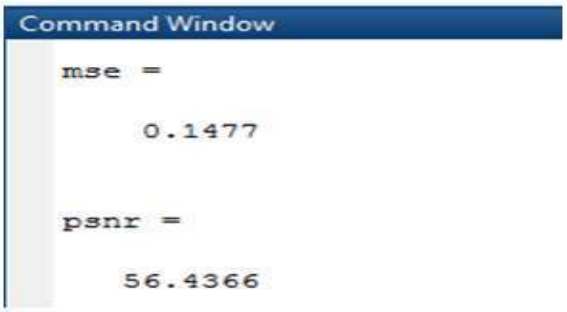

Fig 10: Performance Measures

Performance evaluation measures such as PSNR and MSR is calculated.

CONCLUSION

A In this system we are going anticipated a noble agenda for Reversible Data Hiding in Encrypted image that is (RDHEI) found on the Reversible Image Transformation (RIT). In earlier days the frameworks do encrypt the plaintext picture in to a cipher text form, using RDH EI and RIT based shift we can protect the privacy of the original image, it will swings the semantic of the innovative picture to the semantic of further picture and hence we are protecting the seclusion of the inventive picture. However the encrypted figure is in the appearance of plaintext picture, therefore we can choose any one of the Reversible Data hiding techniques to

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 8, August 2017

plaintext images to insert a watermark, and then we are using a RIT based technique to improve the transformation of image method to be reversible. Using Reversible image transformation (RIT) we are going to renovate the imaginative picture to a certain objective icon with the similar volume and then it will restore the original picture from the encrypted image. This system can take several interesting problems in the future, it will include how to perk up the eminence of the encrypted picture and it will also improve hoe to extend idea of Reversible Image Transformation to video and audio. In the system it will proposed an approach of combining the innovative picture in to objective image and formed encrypted image and then we need to decrypt the original image from the encrypted image. We show that the generated watermarks with the projected algorithms are the quality of encrypted picture and the improved the images and also invisible. Next it will compared the proposed methods with the present reversible data hiding techniques, using statistical factors like as mean square error [MSE] and peak signal to noise ratio [PSNR].

REFERENCES

[1] A. W. Zhang, X. Hu, N. Yu, et al. "Recursive histogram modification: establishing equivalency between reversible data hiding and lossless data compression," IEEE Trans. on Image Processing, vol. 22, no. 7, pp. 2775-2785, Jul. 2013.

[2] V. Sachnev, H. J. Kim, J. Nam, S. Suresh, and Y. Q. Shi, "Reversible watermarking algorithm using sorting and prediction," IEEE Trans. on Circuits and Systems for Video Technology, vol.19, no.7, pp. 989-999, Jul. 2009.

[3] B.ou, X. Li, Y. Zhao, R. Ni, Y. Shi, "Pairwise prediction-error expansion for efficient reversible data hiding," IEEE Trans. On Image Processing, vol. 22, no.12, pp. 5010-5021, Dec. 2013.

[4] Ioan-Catalin Dragoi, Dinu Coltuc, "Local-prediction-based difference expansion reversible watermarking," IEEE Trans. on Image Processing, vol. 23, no. 4, pp. 1779-1790, Apr. 2014.

[5] Z. Ni, Y. Shi, N. Ansari, and S. Wei, "Reversible data hiding," IEEE Trans. on Circuits and Systems for Video Technology, vol. 16, no. 3, pp. 354-362, Mar. 2006.

[6] Klimis Ntalianis and Nicolas Tsapatsoulis, "Remote Authentication via Biometrics: A Robust Video-Object Steganographic Mechanism Over Wireless Networks," in IEEE Transactions on Emerging Topics In Computing, Jan. 2015.

[7] Mehran Andalibi and Damon M. Chandler,, "Digital Image watermarking via adaptive logo texturization," in IEEE Transactions on Image processing, Dec. 2015.

[8] Huang Lidong, Zhao Wei, Wang Jun and Sun Zebin, "Combination of contrast limited adaptive histogram equalization and discrete wavelet transform for image enhancement," in IET Transactions on Image processing, 2015, Vol. 9, Issue no. 10, pp. 908–915

[9] Xinpeng Zhang, Member, IEEE, Yanli Ren, Liquan Shen, Zhenxing Qian, and Guorui Feng, "Compressing Encrypted Images with Auxiliary information," IEEE Transactions on Image processing, vol. 16, no. 5, pp. 1327–1336, Aug 2014.

[10] W. Hong and M. Hang, "Robust Digital Watermarking Scheme for Copy Right Protection",IEEE Trans.Signal process,Vo.12, pp.1-8-2006