IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 7, July 2017

Multilevel Security for Template Protection using RLE-RSA Algorithm

Gagandeep Kaur Bassi[1], Jatinder Pal Singh Raina[2]

Student, ECE Department, BBSBEC Fatehgarh Sahib, India[1]

Assistant Professor, ECE Department, BBSBEC Fatehgarh Sahib, India[2]

Abstract: The behavioral characteristics are used to identify the person in biometric recognition systems. Every person has different traits which are used to authenticate their identity. Similarly, In the IRIS recognition system, the human eye is used to identify the identity of the individual. But these systems are suffering from the problems of security which is a big concern in recognition. Several mechanisms have been developed by different researchers in last few years that provide protection to the IRIS template. Likewise, a new method has proposed in this thesis, which is acquired by combining the RLE and RSA algorithm together. The RLE provides compression of data and RSA provides encryption of images for security. The proposed method provides high level of security by compressing the template, encrypting the template with RSA and then acquired template is hiding under another cover image. With the application of the proposed technique, template becomes more protected and secure. In order to conclude the efficiency of the proposed approach, experimental analysis has done in terms of different performance parameters such as SSIM, PSNR, MSE, BER and correlation coefficient. The approach has been compared with the traditional LSB technique over 10 different images. From the results analysis, it has been concluded that the proposed RLE-RSA algorithm outperforms the traditional approach regarding efficiency, proficiency and security.

Keywords: Template Protection, RLE algorithm, RSA algorithm, Correlation Coefficient, PSNR.

I. INTRODUCTION

Circular shaped area around the eye pupil is called as Iris. It is unique in all individuals and hence used as a parameter for biometrics recognition system and this type of biometrics recognition is called as Iris recognition system. It is highly advance and recently developed biometrics system [1]. It is highly reliable as well. Due to the fine pattern of iris structure the authentication is easier and simple [2]. In ordinary iris recognition criteria, the iris features are directly matched with the data set of the images stored in database of computer system.
IRIS recognition is a process in which different stages are involved which are listed above [3]:

a) Image Acquisition
b) Localization or Segmentation
c) Normalization
d) Feature Extraction.
e) Pattern Matching

A. Image Acquisition

Firstly in iris identification process, image of iris is acquired. For acquiring iris image, an image capturing equipment is required like camera, scanner etc. For image acquisition various sensors are implemented that can automatically scan the iris [3][4][5]. It is very necessary and critical stage in iris identification system. As we know that the good quality of iris image should be maintained. It is required to maintain good quality because this stored image is further used for comparison and identification purpose. Therefore the stored image in data base can affect the performance of whole system.

B. Localization/Segmentation

Now after image acquisition the second step is localization. This step is also highly important. The image acquired in previous step contain whole eye region [6]. Now, it is required to measure. Different types of localization or segmentation methodologies are implemented to locate the boundaries. In this step the inner as well as outer boundaries are located from the raw image scanned and captured in the previous step.

C. Normalization

This is third step after localization or segmentation. In Normalization step, the variation obtained in the pixel intensity value [7][8]. The main aim focus of normalization is to form a region where all variables have same dimensions in

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 7, July 2017

order to maintain the different images of same iris in different situations, exhibits the identical features. There are different normalization techniques which can be implemented in this stage.

D. Feature Extraction

Extraction of features is fourth step in the process in iris identification process. In this stage the distinctive characteristics from the captured iris image of an individual have been saved separately [9]. With the help of these distinctive features the authenticity of an individual can be recognized. Extraction of characteristics also referred as reduction of dimensions. Different types of algorithms can be used for extraction of distinctive characteristics.

E. Pattern Matching

Last and fifth stage is matching of pattern in iris identification process. In this stage the characteristics of a person whose authenticity is to be identified are compared with data saved n the system database [10][11]. Now if the result has shown the matched characteristics then the person is identified and authorized. On the other hand if result has shown that no feature is matched then the person is not authorized. Templates are used for matching and identification purpose.

II. BACKGROUND

Iris recognition is most reliable and accurate biometric recognition process. On the basis of the iris recognition, in this process the iris pattern of the human eye is captured then this captured image is converted into the frame using the image processing that will convert it into the coded digit that is called as iris code. One of the weaknesses of biometrics is that once a biometric data or template is stolen, it is stolen forever and cannot be reissued, or discarded. Therefore a new algorithm is to propose that will consider all these problems of iris recognition system.

III. PROPOSED WORK

The process of iris recognition is the process in which the iris pattern is used for the recognition process. By studying the literature a new method of the iris recognition is proposed in which the problem of the traditional method is considered. As the biometric authentication systems are gaining more popularity, the security of database templates are becoming important. Thus, template security has become very critical in biometric recognition systems. Proposed technique provides the security of the iris template using the RLE and RSA algorithm. In such process iris template has been hidden under the cover image. As a result security is enhanced because it compress the template, encrypt it and then hide it under different cover images so it will become difficult to decrypt, decompress and extract the template from it. In the proposed work, two different techniques are combining together such as RLE and RSA. The algorithm for individual is mentioned as:

A. RSA algorithm

The RSA algorithm was developed by the Rivest, Shamir and Adleman in the year of 1977. This algorithm is used to encrypt the message and then forward it to the destination for the enhancement in security. The algorithm is totally based on the mathematics explained below: Basically in the algorithm three steps are involved such as Key generation, Encryption and Decryption. Both encryption and decryption is done based upon the generated key.

Key generation

Select any two prime number p and q

Evaluate $n = p * q$

Calculate $\emptyset(n) = (p-1)(q-1)$

Select an integer e

Where

$e < \emptyset(n)$ And prime with $\emptyset(n)$

Evaluate d

$d = e - |\emptyset(n)|$

Public Key KU= {e,n}

Private Key KR= {d,n}

Encryption

$$C = M^c |n|$$

Decryption

$$M = C^d |n| = (M^e)^d |n| = M^{ed} |n|$$

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 7, July 2017

M= block of plain text
C=Cipher text
e, d = any numbers, only receiver knows the value of d whereas sender has knowledge of e and n.

B. RLE Algorithm

The Run length encoding algorithm is considered as a lossless compression technique which is used to compress the data by taking identical sequences of input data. In such technique, the repetition of data is considered to be as a single count. Consequently, multiple existences for the same data will be reduced to a single existence. Thus this type of compression can reduce the actual size of the data. The generalized algorithm for the RLE is listed below:

```
Loop: count = 0
      REPEAT
        Get next symbol
        Count = count + 1
      UNTIL (symbol unequal to next one)
                  Output symbol
      IF count > 1
        Output count
      GOTO Loop
```

In the above algorithm, firstly, the value of count is 0 and then process has started by reaching one symbol. If the symbol is already contained then the value of count will be incremented to the 1. The whole process will be repeated to the total number of symbols or data. In case count is greater than, show the count and continues the loop.

IV. METHODOLOGY

The methodology of the proposed work has shown below which represents the primary steps followed to achieve the projected work.

1. Initially, selects an iris image from the dataset of test images to perform further operation.
2. After selecting an image, perform segmentation over the selected iris image.
3. Extract the template from the selected image to secure it by applying several encryption algorithms.
4. Firstly, apply Run Length Encoding technique over the template to compress it and easily accessible for encryption.
5. Secondly, apply RSA encryption algorithm to provide high level of security to the template.
6. At last, the encrypted template will be hidden under the cover image. For the simulation, 10 different cover images have taken and the encrypted template is hidden under these variant images.
7. Last of all, the encrypted images termed as stego image will be acquired.

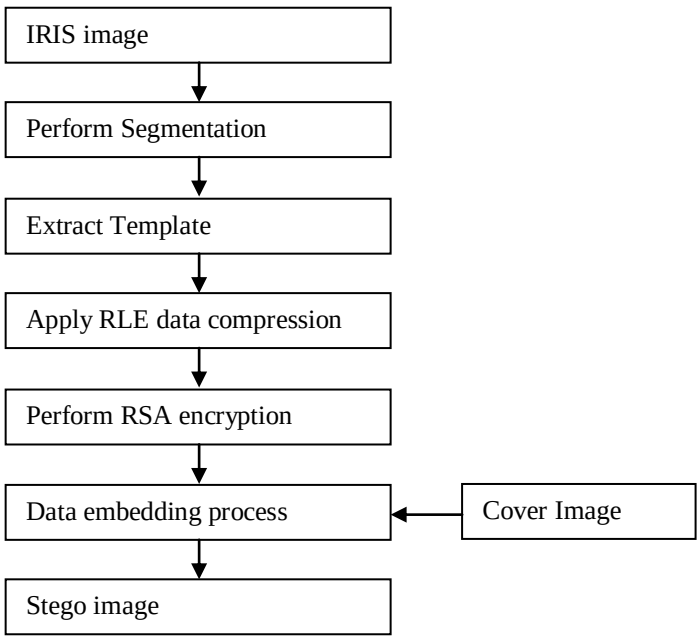

Figure 1 Framework of the proposed model

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 7, July 2017

V. RESULTS AND DISCUSSION

The performance parameters which are used to evaluate the efficiency of the proposed work are listed below:

A. PSNR

It is used to evaluate the noise in the image. The PSNR defines the ratio between the data and noise. The equation used to calculate PSNR is as follows:

$$\text{PSNR} = 10.\log_{10}\left(\frac{\text{MAX}_1^2}{\text{MSE}}\right)$$
$$= 20.\log_{10}\left(\frac{\text{MAX}_1}{\sqrt{\text{MSE}}}\right)$$
$$= 20.\log_{10}(\text{MAX}_1) - 10.\log_{10}(\text{MSE}) \ldots\ldots\ldots\ldots (1)$$

In the above equation, Max shows the maximum possible value of the image and MSE represents the sum over all squared value differences which is divided by the size of an image.

B. MSE

It is the performance parameter which is used to define the average error of an image. The efficiency lies in non-negative and closer to zero value. The equation used to calculate is as:

$$\text{MSE} = \frac{1}{\text{mn}}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j) - K(i,j)]^2 \ldots\ldots\ldots\ldots\ldots\ldots (2)$$

C. BER (Bit Error Rate)

The bit error rate is referred as the number of bits errors with respect to per unit time. It can be calculated as the number of bit errors divided by the transferred bits. The performance measurement has done in terms of percentage. The equation followed to acquire the BER is as follows:

$$\text{BER} = \frac{\text{Eb}}{\text{N0}} \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (3)$$

The equation 3 defines the energy per bit to noise power spectral density ratio.

D. Correlation

Correlation in the images defined the mutual relationship between two different images. In the proposed method, two different images have compared to each other and conclude the efficiency of the proposed technique in terms of how far they are similar to one another. The range varies from -1.00 to 1.00. The equation used to find the correlation coefficient of the proposed technique is as follows:

$$R = \frac{N\sum XY - (\sum X)(\sum Y)}{\sqrt{[N\sum X^2 - (\sum X^2)][N\sum Y^2 - (\sum Y^2)]}} \ldots\ldots\ldots (4)$$

The above equation finds out the relation between two different variables such as X and Y.

E. SSIM (Structural Similarity Index)

This performance parameter is used to measure the similarity between two different images. This parameter can generate efficient results. This parameter is based on the perception

$$\text{SSIM}(x,y) = \frac{(2\mu_x\mu_y + C_1)(2\sigma_{xy} + C_2)}{(\mu_x^2 + \mu_y^2 + C_1)(\sigma_x^2 + \sigma_y^2 + C_2)} \ldots\ldots\ldots\ldots\ldots\ldots\ldots (5)$$

Where in the equation 8, μ_x represents the average of x.

μ_y Is the average of y.

σ_x^2 is treated as a variance of x.

σ_y^2 is treated as a variance of y.

$\boldsymbol{\sigma_{xy}}$ is the covariance of x and y.

The performance parameter satisfies the similarity between two images with the condition of symmetry such as: SSIM(x, y) = SSIM (y, x)

1. Experimental Analysis

The proposed work has been analyzed under different performance parameters to check their performance with traditional work. The traditional technique considered is the LSB approach whereas the proposed technique is the hybridization of RLE and RSA algorithm. The figure 2 describes the proposed and traditional technique in terms of

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 7, July 2017

MSE i.e. Mean Square error. From the figure it has been clearly shown that the traditional technique provides high number of mean square error whereas in the propose technique the rate of MSE has reduced at 0.03

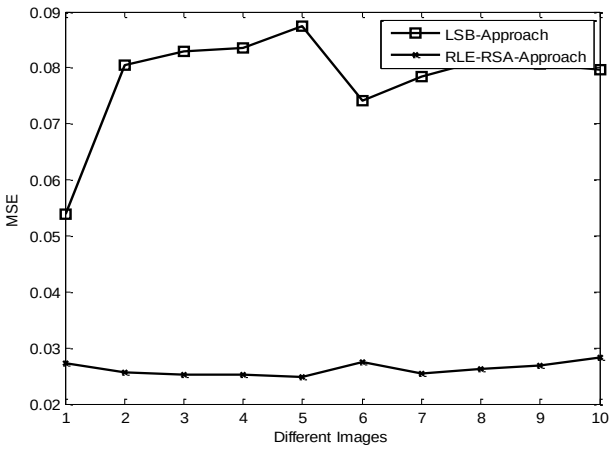

Figure 2 Comparison between different approaches in terms of MSE

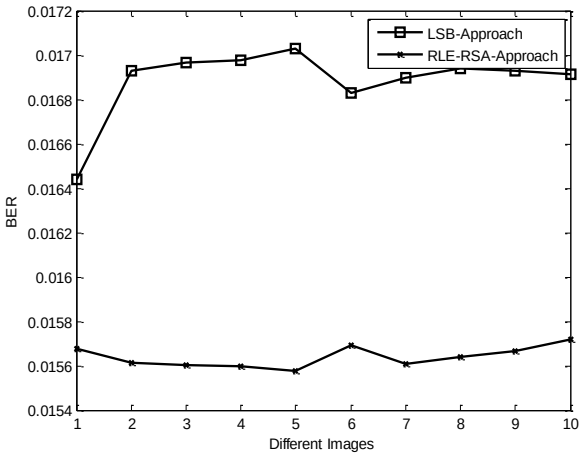

Figure 3 Comparison between different approaches in terms of BER

The BER shows the number of bit error per unit. For the experimental analysis, BER has used to represent the efficiency of the techniques. It has been clearly shown from the figure is that there are total 10cover images have taken and on each image a particular technique has applied. There is high number of variations depending on the image type in case of traditional technique. Alternatively, consider the proposed technique where there is less number of variations with respect to different images which shows the stability and effectiveness of the projected work.

The figure 4 represents the Peak signal to noise ratio of different approaches. The PSNR shows the amount of noise in the image after application of a particular technique. The figure clearly shown the fact that initially, the amount of noise in the image 1 in case of traditional approach was quite low i.e. around 60. Similarly, it degrades with different types of images. On the flip side, initial PSNR in the image 1 was around 64 which is higher than the traditional approach so it can be concluded that the proposed approach is efficient in terms of PSNR.

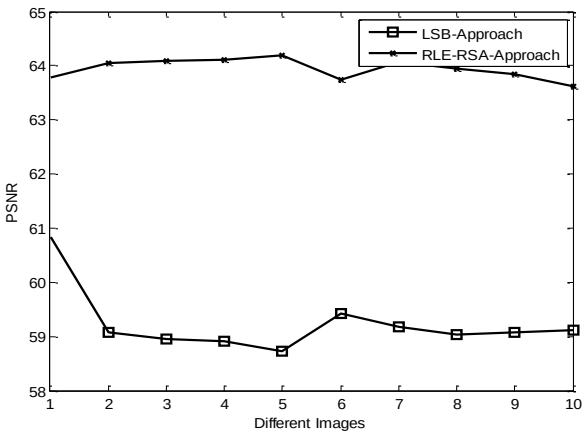

Figure 4 Comparison between different approaches in term of PSNR

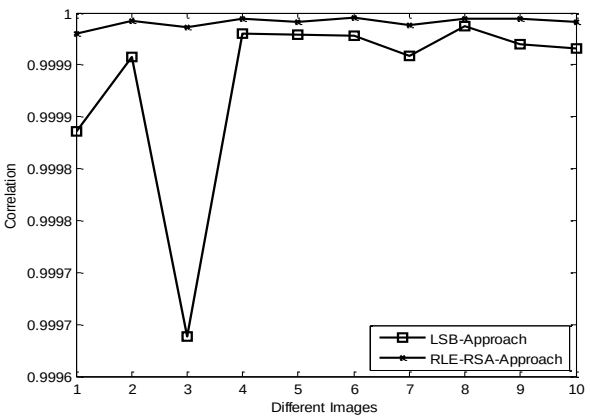

Figure 5 Comparison between different approaches in terms of correlatin

The Correlation between two different images identifies that how mutually they are related with each other. The higher amount of correlation coefficient ensures the efficiency of the proposed approach. In the below figure, the LSB approach provides less relationship with different images whereas the combination of RLE and RSA algorithms shows high level of efficiency in all types of images.

The last performance parameter considered for the evaluation is SSIM which shows the similarity between two different images after performing data embedding to the original image. The comparison has done between the traditional and the proposed approach. The LSB shows the high SSIM in the second image only and varies with different images. On the contrary side, SSIM of all images are high with respect to different images in the RSA-RLE approach.

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 7, July 2017

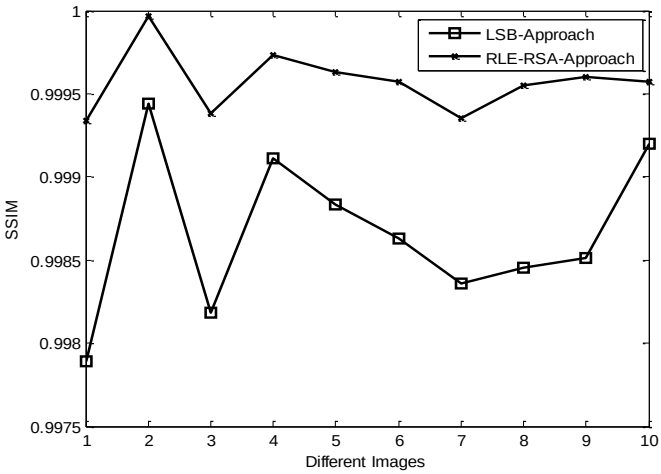

Figure 6 Comparison between different approaches in terms of SSIM

VI. CONCLUSION AND FUTURESCOPE

The work has done in this paper is to secure the IRIS template from being modified. Thus, a new algorithm has proposed in this work termed as RLE-RSA algorithm. RLE algorithm is used to compress in order to reduce the overall size of the data and RSA algorithm is used to encrypt the template and then perform hiding of data under different cover images. For the experimental analysis, LSB traditional approach has taken for the comparison with the proposed RLE-RSA algorithm. The simulation analysis has done using five performance parameters such as MSE, BER, PSNR, Correlation coefficient and SSIM. From the simulation analysis, it has been concluded that proposed technique outperforms under different scenarios with respect to traditional approach. Each approach has been carried out over 10 different cover images and at each individual image, proposed approach produces effective results. On the whole, PSNR of proposed approach is high, BER and MSE is less, SSIM and correlation coefficient is also high.
The proposed work is relied upon the combination of two different approaches such as RLE and RSA whereas in future it can be expanded up to dual watermarking Steganography for security. In this approach stego image can be hidden again with another cover image.

REFERENCES

[1] S.E. Baker et al, Empirical evidence for correct iris match score degradation with increased time-lapse between gallery and probe matches, SPRINGER, vol. 5558, pp. 1170–1179,2009.
[2] S.E. Baker et al.,” Degradation of iris recognition performance due to non-cosmetic prescription contact lenses.”, Computer vision and image understanding, Vol. 114, No. 9, Pp 1030–1044, June 2010.
[3] K. Bowyer et al, “Trial Somaliland voting register de-duplication using iris recognition” IEEE Automatic Face and Gesture Recognition Conference Workshops (2015)
[4] A. Czajka, “Influence of iris template ageing on recognition reliability”, CCIS, Vol 452, Pp 284–299, November 2014
[5] J. Daugman,” New methods in iris recognition.”, IEEE, Vol. 37, No. 5, Pp 1167–1175, October 2007
[6] J. Daugman, I. Malhas, “Iris recognition border-crossing system in the UAE. Biometrics”, No. 2, 2004.
[7] J. Doyle, K. Bowyer, “Robust detection of textured contact lenses in iris recognition using BSIF”, IEEE Access 3, Pp. 1672–1683, August 2015.
[8] S.P. Fenker, “Experimental evidence of a template aging effect in iris biometrics” (2011).
[9] J. Galbally et al., “Iris image reconstruction from binary templates: An efficient probabilistic approach based on genetic algorithms”, ELSEVIER, Vol. 117, Pp. 1512–1525, 2013
[10] K. Hollingsworth et al, “Pupil dilation degrades iris biometric performance.”, ELSEVIER, Vol. 113, No. 1, Pp150–157, January 2009.
[11] A.W.K. Kong, D. Zhang, M.S. Kamel, ”An analysis of Iris Code”, IEEE , Vol.19, No. 2, Pp 522–532, October 2009.
[12] James R. Matey et al, “Iris on the Move: Acquisition of Images for Iris Recognition in Less Constrained Environments”, IEEE, Vol. 94, No. 11, Pp. 1936-1947, November 2006.
[13] Jonas Nyasuslu, “Literature Study of Iris Biometric Recognition”, IDA, Pp 1-5, 2008
[14] Simranjeet Kaur et al. “Survey of Different Approaches in Biometric Iris Recognition System”, IJARCSSE, Vol 4, Issue 7, Pp 768-771, 2014
[15] Khattab M. Ali Alheeti, “Biometric Iris Recognition Based on Hybrid Technique”, IJSC, Vol 2, Issue 4, Pp 1-9, 2011.
[16] A. Malikarjuna et al. “Biometric Security Techniques For Iris Recognition System”, IJRCTT, Vol 2, Issue 8, 2013
[17] S V Sheela et al. “Iris Recognition Methods- Survey”, IJCA, Vol 3, Issue 5, Pp 19-25, 2010
[18] Upasana Tiwari et al. “Study of Different Iris Recognition Methods”, IJCTEE, Vol 2, Issue 1, Pp 76-81, 2012
[19] Donald M. Monro et al. “DCT based Iris Recognition”, IEEE, Vol 29, Issue 4, 2007
[20] Li Ma et al. “Local Intensity Variations Analysis For Iris Recognition”, ELSEVIER, Vol 37, Issue 6, Pp 1287-1298, 2004
[21] Richard P. Wildes, “Iris Recognition: An Emerging Biometric Technology”, IEEE, Vol 85, Issue 8, Pp 1-16, 1997.
[22] Richard P. Wildes et al. “A Machine Visison System for iris recognition”, SPRINGER, Vol 9, Issue 1, Pp 1-8, 1996.
[23] J.C. Asumith et al. “A System for Automated Iris Recognition”, IEEE, 2002
[24] Kresimir Delac et al. “A Survey of Biometric Recognition Methods”, ISEM, Pp 184-193, 2004.