www.ijecs.in
International Journal Of Engineering And Computer Science ISSN: 2319-7242
Volume 5 Issue 11 Nov. 2016, Page No. 19149-19154

Image Encryption using RSA Algorithm with Biometric Recognition

R.Saranya[1], S.Prabhu[2]
[1]Department of ECE, KPR Institute of Engineering & Technology, Tamilnadu
Email: *saranyamec@gmail.com*
[2]Department of Mechanical Engineering, Excel College of Engineering & Technology, Tamilnadu
Email: *prabhu.kpm@gmail.com*

Abstract: — *In the fast evolution of digital data exchange, security of any information becomes much important in data storage and transmission. Due to the increasing use of images in various fields, it is essential to protect the confidential image data from unauthorized access. Biometric identification is an actively growing area of research and is widely used in application fields like E-commerce, E-banking, E-passports, E-licences and security applications. In recent years, Face recognition becomes one of the popular biometric identification systems used in identifying or verifying individuals and matching it against library of known faces. Also it finds its application in wide variety of areas like criminal identification, human - computer interaction, security systems, credit- card verification, teleconference, image and film processing. This paper suggests a secure encryption of medical images along with an automated face recognition system based on extracting the features from the input face image. For encryption process, RSA algorithm is used. Feature extraction process in the face image is performed by locating the position of eyes, nostrils and mouth and determining the distances between those regions. From the extracted features, a database is created for known individuals. A virtual neural network is created based on Extreme Learning Machine (ELM). This network verifies whether the individual is a known user or an intruder.*

Keywords: Image encryption, RSA algorithm, Biometric identification, Face recognition, Feature extraction, ELM, FAR, FRR.

1. Introduction

Cryptography is the study of hiding information using secret keys and sent via wireless channel. Information may be text, number, image, audio or video. Various types of cryptography includes i) Public key cryptography (RSA, McEliece), ii) Secret key cryptography (DES, AES) and iii) Hash functions. Image and video encryption have applications in various fields including internet communication, multimedia systems, medical imaging, Tele-medicine and military communication. Public key cryptosystem or asymmetric key cryptography that uses two keys - public and private keys. Private key cryptosystem is otherwise known as symmetric/secret/single key cryptography that uses one key that is shared by both sender and receiver. If this key is disclosed, communications are compromised and insecure. Hash functions uses single key and used for encryption.

1.1. RSA ALGORITHM

RSA cryptosystem is used for encrypting the images. It was developed by Rivest, Shamir & Adleman of MIT in 1977. It is best known & widely used public-key scheme. It is based on integers modulo of a prime numbers. It uses large integers and easy operation. It provides better security due to cost of factoring large numbers. The steps in RSA algorithm are,

1. Key generation
2. Encryption of plain text to produce Cipher text using public key (to lock)
3. Decryption of cipher text to obtain plain text using private key (to open)

1.2. BIOMETRICS

Biometrics is a measurable physiological or behavioral characteristic of an individual used in personal identification and verification. It includes fingerprint, iris, face, voice, palm symmetry, hand geometry and so on. Biometric identification has significant advantages over other authentication techniques because biometrics characteristics are not easily modifiable and are unique.

1.3. FINGERPRINT AND IRIS RECOGNITION

Fingerprint recognition has been widely used because it is cost affordable and best utilized in small-scale verification systems. This recognition method finds applications in mobile phones, computers, Employees identification scheme, etc. But this method encounters problems like some fingerprints are unsuitable for use due to cuts or other defects. Also artificial finger straps are readily available in the market makes the recognition process difficult or identifying the wrong

individual. To overcome the difficulties in fingerprint recognition, some other methods are suggested.

Iris recognition has evolved in recent years which eliminate the problem in fingerprint mechanism. The accuracy and speed of iris systems allows this technique implementing in a large scale system. The iris of each person is distinctive and even identical twins have different patterns. Since it is extremely difficult to alter the texture of the iris through surgery, it would be difficult for someone to provide wrong identifications. Also it is relatively easy for the system to detect when an artificial iris specially made by contact lens, is being used to gain identification. But iris recognition also encounters some difficulties in the verification applications. To overcome such difficulties in iris recognition techniques, Face recognition comes into existence in the modern world of artificial intelligent systems.

1.4. FACE RECOGNITION

Face recognition field has achieved a significant growth over the past few years. It is the popular area of research for more than 3 decades in computer vision and the most successful applications of image analysis. Several companies offer face recognition software that can produce high-accuracy results with a large database. Recent research involves developing approaches that accounts for changes in lighting, expression, and aging, for a given person. Also, researches under this field include dealing with glasses, facial hair, and makeup. Face recognition is commonly used in two ways, Face identification and Face verification [8]. First refers one to many matches and next refers one to one matching. The automated methods of facial recognition work very well, but it do not recognize persons effectively as a human brain. The modules present in the recognition process are Detection, Alignment, Feature extraction and Matching. Regarding face recognition problems, it also encounters the combined variations in illumination, pose, expression, spectacles, and optimization of training databases and also needs the real-time requirements.

1.5. EXTREME LEARNING MACHINE (ELM)

ELM is one of the virtual neural networks, provides less training time and high accuracy. It is a sequential learning algorithm where the training observations are sequentially used as single data block or data with varying or fixed length in the learning algorithm. At any time, only the new observations are seen and learned. The training data are discarded as soon as the learning procedure for that particular data is completed as in [4]. In this paper, ELM network is used for training and testing databases of the face images. For recognition purpose, 35 images are taken into consideration. 9 images are used for training process and the remaining for testing process. Number of hidden nodes is manually entered. Input weights and bias are randomly assigned based on the inputs and hidden neurons. The created face database is trained using ELM network and matching is performed with test images. ELM works well even for small set of database. As the number of hidden neurons gets increased, high accuracy is achieved.

2. LITERATURE SURVEY

Atefe Assadi and Alireza Behrad [1] proposed a method for Face recognition using Texture and depth information. This method provided a 3D approach for recognizing faces under pose variation and different illumination conditions. Scale-invariant feature transform (SIFT) descriptors are used to extract the facial feature points and compared with the database. They also calculated the matching points using SIFT feature vector. Input face image with maximum matching points is recognized as known face. This method provided 88.96% recognition rate.

Deo Brat Ojha et al [2] proposed an authenticated transmission of medical images over a noisy channel using codebase cryptography. For secure transmission, McEliece key cryptography was used for encryption. Then Sequitter compression was used for efficient use of bandwidth of the channel. Decryption was done at the receiver's side to get the image. This method was used to provide a fast encryption and decryption algorithm. But the keys sizes were larger in size, would make it as complex method.

Guang-Bin Huang et al [4] developed an online sequential learning algorithm for single hidden layer feed forward networks (SLFNs) with additive or radial basis function (RBF) hidden nodes. Here the training time got reduced results in high accuracy. This algorithm could be effectively used with small database and data could be included when needed. the input weights and biases were randomly generated and based on this the output weights were analytically determined. Other sequential learning algorithms needed many control parameters

to be tuned but OS-ELM needed only the number of hidden nodes to be specified.

Ramesha K et al [5] proposed a Feature Extraction based Face Recognition, Gender and Age Classification (FEBFRGAC) algorithm. In this paper, recognition process was performed based on the geometric features based on the symmetry of human faces and the variation of gray levels, the positions of eyes, nose and mouth were extracted and located by applying the Canny edge operator. The gender was classified based on posteriori class probability and age was classified based on the shape and texture information using Artificial Neural Network. This algorithm provided face matching ratio is 100%, gender classification is 95%, and age classification is 90%.

Shermina J [6.a] proposed a face recognition system based on Multi linear principal component analysis (MPCA) and Locality preservation projection (LPP). In this paper, after face image preprocessing, dimensionality reduction is performed using MPCA. Features were extracted using LPP which provided nearest neighbor search in the low dimensional space. Recognition was performed by using L2 similarity distance measure, computed between the database image and the query image. High recognition rate was achieved by combining both the MPCA and LPP.

Shermina J [6.b] proposed a Face recognition system based on Discrete Cosine Transform (DCT) and PCA. In this research paper, low frequency DCT components are used to normalize the illuminated image. 64 illumination conditions are taken into account. This paper provided with accuracy of 94.2% and concluded that combination of DCT with any other recognition methods provided significant illumination invariant recognition accuracy.

Thamizharasi A [8] proposed a survey paper of Analysis on Face recognition by combining multi scale techniques and Homomorphic filter using Fuzzy k nearest neighbor classifier. In this paper, DCT and Discrete wavelet transform (DWT) were the two multi scale techniques used. Homomorphic filters were used for normalization of illumination. K means clustering algorithm was applied to group the pixels in the preprocessed image based on gray-scale threshold values. Fuzzy k nearest neighbor classifier was used to classify image in the test database by calculating the Euclidean distance matrix within the train database.

2D Haar DWT at level 1 was performed on the preprocessed image for choosing the approximate coefficients at level 1. Then the clustering algorithm and classifier were used for finding the face recognition rate. High recognition rate was achieved by combining all these multiscale techniques even though they could be used individually. DCT yielded 89.5% recognition rate while DWT yielded 90% rate with Homomorphic filter, K means clustering and Fuzzy k nearest neighbor classifier. The system became more complex because of more no. of techniques and computation time would be more.

2. PROPOSED METHOD

This paper proposed a method for feature extraction based face recognition using ELM network. The face recognition process will be used for end user security in many other authentication systems. Medical images are confidentially transmitted via wireless channel with higher level of security using various types of encryption/decryption algorithms. These algorithms avoid hacking of medical images while transmission across internet. But there is no security at the end user or receiver's side and thus anyone can receive the encrypted message. If the cryptographic algorithm will be private means the intruder can easily decrypts the message and gets the medical image. Hence it is necessary to provide authentication while transferring via internet. Face recognition algorithm is included at the end users side. Once the user gains the authority, he/she can transfer the images in a secured manner. The flowchart describes the proposed model will be shown in the figure1.

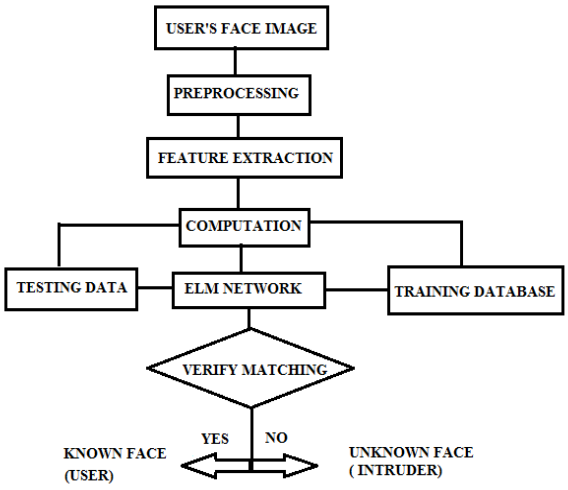
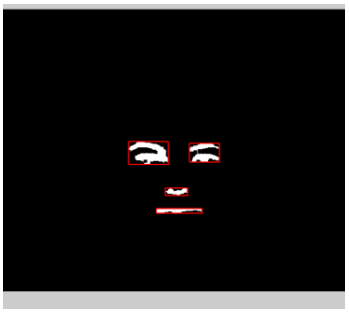


Fig.1 Face recognition model

Initially an RGB colour image of the user is captured using a web camera or high resolution video camera. The size of the face image is 640x480. It is represented as an array of mxnx3 color pixels corresponding to the red, green and blue components of an RGB image. Three dimensional RGB is converted into two dimensional binary image based on threshold values .The input face image is transformed into binary face image for retaining the important features. Background changes, illuminations are adjusted and concentrating on the face region alone. This process referred as Preprocessing for improving the quality of the image shown in the figure 2(a).

(a)



(b)

Fig.2 (a) RGB image of user1 and (b) Detected Regions with bounding boxes

Feature extraction is performed after preprocessing the input face image. The regions of two eyes, nostrils and mouth are located in the face image and Blob measurement properties are used in estimating the connected components in the face image. Thus the eyes, nostrils and mouth regions are located in the binary image. Then the regions are represented within the bounding boxes and filled the disconnected pixels are shown in the figure 2(b).

From the extracted regions, the following distances are measured in the face image. The distances are calculated by calculating centroid values of each bounding boxes.

Inter-Ocular Distance - The distance between the right eye and the left eye pixels.

Eye to Nose Distance - The distance between the midpoints of the line joining the eyes and the nose tip pixels.

Eye to Mouth Distance - The distance between the midpoint of the line joining the eyes and the center point of the mouth.

Nose to Mouth Distance - The distance between the nose tip and the center point of the mouth.

The above said distances are calculated from the face image and the ratios are calculated. These computed ratios are referred as features of the face image which are taken into account for recognition.

The ratios are mentioned as follows,

1. EENR is Eye to Eye and to Nose Ratio and is the ratio between the Inter-ocular distance and the Eye to Nose distance.
2. EEMR is Eye to Eye and to Mouth Ratio and is the ratio between the Inter-ocular distance and the Eye to mouth distance.
3. EENMR is Eye to Eye and Nose to Mouth Ratio and is the ratio between the Inter-ocular distance and Nose to mouth distance.
4. ENEMR is Eye to Nose and Eye to Mouth Ratio and is the ratio between the Eye to Nose distance and Eye to mouth distance.

For the user 1, the corresponding distances and ratios are calculated as.

Inter ocular distance = 99.2 mm

Eyes to nose distance = 85.5 mm

Eyes to mouth distance =10.9 mm

Nose to mouth distance= 25.4 mm

EENR = Inter-ocular distance/Eye to Nose distance

= 99.2/85.5 = 1.1602

EEMR = Inter-ocular distance/Eye to Mouth distance

= 99.2/110.9 = 0.8944

EENMR = Inter-ocular distance/Nose to Mouth distance

= 99.2/25.4= 3.9055

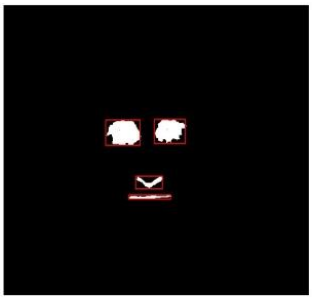
ENEMR = Eye to Nose distance/Eye to mouth distance

= 85.5/110.9 = 0.7683

Similarly these ratios are computed for legitimate users and created as database. Figure 3(a) and 3(b) shows the intruder's face image and its detected regions.

DOI: 10.18535/ijecs/v5i11.78

(a)



(b)

Fig. 3(a) RGB image of intruder and (b) Detected Regions with bounding boxes

The computed features from the face image are given as inputs to an extreme learning machine network. Number of hidden layer neurons alone is entered manually or it will be the sum of input neurons and output neurons. Input weights and biases are assigned randomly and from that output weights are calculated. The features are trained within the network for the given database. The query image is verified for matching purpose. If matching exists, the result shown as *KNOWN FACE* otherwise the result will be *UNKNOWN FACE*. Thus User verification is performed once the extracted features are matched with the database otherwise user cannot access the authority to use the resources. Figure 4 shows the simple architecture of ELM network.

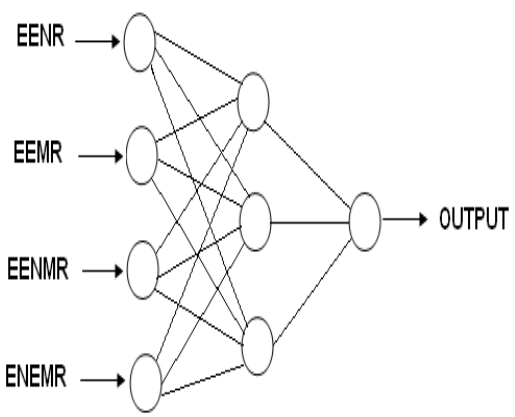


Fig.4 A simple ELM network

The table 1 shows that the extracted features of the sample database images used in the recognition process.

In this proposed method, 35 face images of different users are used for recognition purpose. Out of these 35 images, 9 images are taken as training data and remaining 26 images are taken for testing data. The accuracy or performance metrics of the biometric identification depends on two parameters i.e. FAR and FRR.

False Acception Rate or False Match Rate (FAR or FMR) is the probability that the system incorrectly matches the input pattern to a non-matching template in the database. It measures the percent of invalid inputs which are incorrectly accepted.

TABLE.1 DATABASE FOR DIFFERENT FACE IMAGES

Face image	EENR	EEMR	EENMR	ENEMR
06-1m	1.1895	0.6548	1.4571	0.5505
11-1m	1.1602	0.8944	3.9055	0.7709
14-1f	1.4506	0.8730	2.1926	0.6018
15-1f	1.3810	0.9320	2.8666	0.6748

False Reject Rate or False Non-Match Rate (FRR or FNMR) is the probability that the system fails to detect a match between the input pattern and a matching template in the database. It measures the percent of valid inputs which are incorrectly rejected.

3.1. KEY GENERATION IN RSA ALGORITHM

Each user generates a public/private key pair by selecting two large primes at random p, q then computing their system modulus N=p*q note that ø(N)=(p-1)(q-1). select at random the encryption key e where 1<e<ø(N), gcd (e ,ø(N))=1 and to find decryption key d using e.d=1 mod ø(N) and 0≤d≤N.

- Public encryption key: KU={e,N}
- Secret private decryption key: KR={d,p,q}

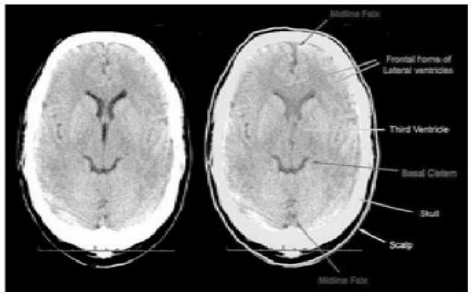
3.2. ENCRYPTION & DECRYPTION

To encrypt a message M the sender:

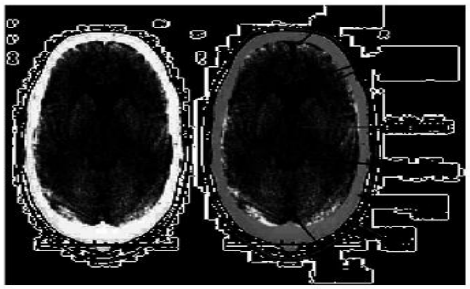
- obtains public key of recipient KU={e,N}
- computes: $C=M^e \bmod N$, where $0 \le M < N$

To decrypt the cipher text C the recipient:

- uses their private key KR={d,p,q}
- computes: $M=C^d \bmod N$



(a)



(b)

Fig. 5 (a) Original Medical image and (b) Encrypted image using RSA algorithm

4. RESULTS AND CONCLUSION

The proposed face recognition method yields the best authentication system. This method is simple and efficient. It deals with pixel information rather than texture information hence the accuracy will be more. The use of ELM network for training and testing the database provides fast and accurate authentication system. The measured FAR is 3.85% and FRR is 0% hence the proposed face recognition system yields a better biometric identification system using ELM network. The proposed face recognition technique is implemented in secure transmission of medical images at the end user's side. RSA encryption algorithm is widely used since it provides keys based on integer and modulo arithmetic. It also provides better security to images.

REFERENCES

[1] Atefe Assadi and Alireza Behrad "A new method for human face recognition using texture and depth information", *IEEE transactions on Neural Network Applications in Electrical Engineering (NEUREL)*, pp. 201-205, 2010.

[2] Deo Brat Ojha, Ajay Sharma, Abhishek Dwivedi, Nitin Pandey, Amit Kumar, "An Authenticated Transmission of Medical Image with Codebase Cryptosystem over Noisy Channel", *International Journal on Advanced Networking and Applications* ,vol. 02, Issue: 05, pp. 841-845,2011.

[3] Deo Brat Ojha et al, "An Authenticated two-tier security on transmission of medical image using codebase cryptosystem over teeming channel", *International Journal of Computer applications*, vol.12-no.9, pp. 22-26,2011.

[4] Nan-Ying Liang, Guang-Bin Huang, P.Saratchandran, and N. Sundararajan , "A fast and accurate online sequential learning algorithm for feed forward networks", *IEEE transactions on neural networks*, vol. 17, no. 6,2006.

[5] Ramesha K et al, "Feature Extraction based Face Recognition, Gender and Age Classification", *International Journal on Computer Science and Engineering (IJCSE)*, vol. 02, no.01S, pp.14-23, 2010.

[6] Sunanda Mulik, "Face recognition for biometric identification: A review", *International Journal of Intelligent Information Processing*, vol.4, pp. 89-92, 2010.

[7] Thamizharasi A, "Performance Analysis on Face recognition by combining multi scale techniques and Homomorphic filter using Fuzzy k nearest neighbor classifier", *IEEE International Conference on Communication Control and Computing Technologies (ICCCCT)*,pp. 643-650,2010.

[8] M.Turk and Pentland, "Face recognition using Eigen faces", IEEE International conference on Computer vision and pattern recognition, 1991.

[9] Face images databases from www.cs.cmu.edu/~cil/v-images/html and www.face-reg.org/databases/html.

[10] Medical images from brain images: mr-tip.com

DOI: 10.18535/ijecs/v5i11.78