ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

*Volume 3, Special Issue 3, March 2014*

2014 International Conference on Innovations in Engineering and Technology (ICIET'14)

On 21st & 22nd March Organized by

K.L.N. College of Engineering, Madurai, Tamil Nadu, India

# IRIS Authentication Based On AES Algorithm

R. Jubiya[1], M. Keirthi,[2] M. Anupriya,[3] A. Muthukumar[4]

Dept of ECE Kalasalingam university, Tamilnadu, India.

Dept of ECE Kalasalingam university, Tamilnadu, India

Dept of ECE Kalasalingam university, Tamilnadu, India

Dept of ECE Kalasalingam university, Tamilnadu, India

**ABSTRACT**—Cryptosystem is widely used in many information security application were the identification and verification are done by passwords, pin number etc which is easily cracked by others. So biometric cryptosystem is a powerful unique tool based on the anatomical and behavioral characteristics of the human beings in order to proof the authentication. Iris is used for generation of 128 bit binary key in order to prove the legitimate user who entering into the biometric system. This paper proposes extracting the multiple iris features from local iris image based on Independent Component Analysis (ICA) to reduce the dimensionality and to get accurate iris feature vector. It is clustered and its centroid value is converted into 128 bits iris key using K-Means clustering. The clustering is used to minimize the intra variation on the extracted iris feature vector. This paper also proposes biometric cryptosystem based on AES encryption and decryption to protect the confidential information by using iris as a biometric key. CRC is used to check whether there is no modification in the original data.

**KEYWORDS —** ICA, K-Means clustering, CRC, AES encryption and decryption**.**

## I.INTRODUCTION

Cryptographic techniques are being widely used for ensuring the secrecy and authenticity of information. The security relies on the assumption that the cryptographic keys are known only to the legitimate user. Maintaining the secrecy of keys is one of the main challenges in practical cryptosystems. Passwords can be easily lost, stolen, forgotten, or guessed using social engineering and dictionary attacks. Limitations of password-based authentication can be alleviated by using stronger authentication schemes, such as biometrics is shown in Fig. 1. Biometric systems establish the identity of a person based on his or her anatomical or behavioral traits, such as face, fingerprint, iris, voice, etc. Biometric authentication is more reliable than password-based authentication because biometric traits cannot be lost or forgotten and it is difficult to share or forge these traits [3].

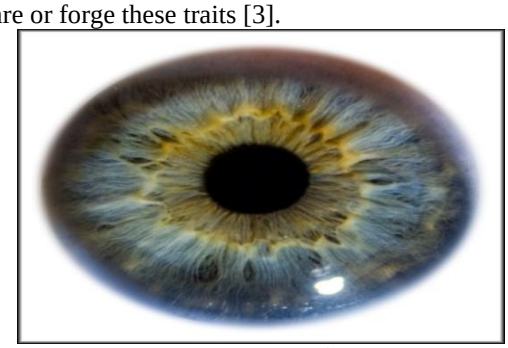

Fig. 1. An image of iris

This paper proposes Independent component analysis (ICA) method. ICA is a method for finding underlying factors or components from multivariate (multi-dimensional) statistical data. What distinguishes ICA from other methods is that it looks for components that are both statistically independent and non Gaussian. In this paper it

is used to reduce dimension and computational effort and iris recognition is also feasible based on ICA.By extracting multiple iris features from multiple local regions in a given iris image, and the exact value of the unordered set is then produced by using the clustering method. The main concept to use K-Means clustering is to approach every object in the database and must contain a minimum of one object. Each cluster is to find a mean vector, according to this approach, it comes under the category of centroid value. From this centroid value we get 128 bit key. Cyclic Redundancy Check (CRC) is used as a error detecting code and commonly used in digital network and storage device to detect accidental changes to raw data.CRC is popular because they are simple to implement in binary hardware, easy to analyze mathematically and particularly good at detecting common errors. So CRC is used in biometric cryptosystem. Advanced Encryption Standard (AES) which is accepted as a symmetric cryptography standard for transferring block of the data securely. The available AES algorithm is used for text data and it is also suitable for iris image encryption and decryption to protect the confidential iris image data from an unauthorized access. This paper proposes a method in which the iris image data is a key to AES encryption and to obtain the encrypted value, and the encrypted value is the input to AES decryption to get the original secret value. In this paper, generation of 128 bit key is used for AES encryption and decryption [5].

The remainder of this paper is organized as follows. Section II describes iris encryption phase. Section III describes iris decryption phase. Section IV describes experimental results and conclusion is explained in section V.

## II. IRIS ENCRYPTION PHASE

In this paper, biometric character itself acts as a key for a system. In symmetric cryptography, a single key is used for both the encryption and decryption purpose. According to this methodology, a key must be similar to both encrypting and decrypting process. In this paper, iris is acting as a biometric key for the crypto systems. For encryption and its reverse process, this paper uses the Advanced Encryption Standard (AES) algorithm. In this paper, biometric key is generated from the iris biometrics. The overview of the proposed iris encryption phase is shown in Fig. 2

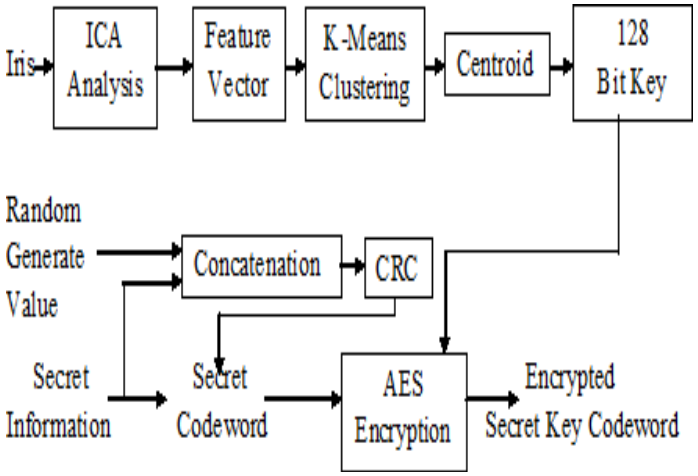


Fig. 2. Iris encryption phase

The input is x which is known as secret information and iris as a biometric key where it is acting as a 128 bit biometric key. Iris is not identical for every person, so this paper is using iris as a biometric key. In encryption phase, there are two steps. First step explains about iris feature extraction in biometrics and the second phase explains the encryption [9].

### *A. Independent Component Analysis*

Independent component analysis (ICA) is a method for finding underlying factors or components from multivariate (multi-dimensional) statistical data. What distinguishes ICA from other methods is that it looks for components that are both statistically independent and non Gaussian. Then feature extraction is done by Capturing eye image from interior and exterior boundary [6]. The left and right regions of the normalized iris image as region of interest (ROIs) for extracting iris feature [10] are selected. The *n* ICA bases that are able to represent iris texture signals are created. The first step is to find the optimal number of ICA bases with which the minimum rate of iris recognition is obtained. Second step is removing the vector the greatest variance of intra class distributions [1]. In this section, generally iris recognition system use string of 128 bits extracted from an entire iris region is shown in Fig. 2. Binary bit itself cannot be used as an element of unordered set. So, several bits are grouped into a feature vector. Even by grouping feature vector it shows a great variation. So that extracting multiple iris feature from multiple local images based on Independent Component Analysis.

*B. K- Means Clustering*

Clustering is the process of grouping a non-linear set of objects. This approach can assign the database of *n*-objects into *k*-number of clusters ($k < n$). The main concept of this K-Means approach is every object in the database must contain in any of the clusters or group, then every cluster must contain a minimum of one object. Then each cluster can be used to find a mean vector; according to this approach, it comes under the category of the centroid model.

In this paper, K-Means clustering is used to find the set of genuine key points, which is converted into binary bits and stored in the database in encryption phase. The process of iris K-Means clustering. Consider the key points are given as the input data vectors' M = (m1, …, mn). K-Means algorithm starts by initializing the first co- ordinates values as the centroid and defined the numbers of clusters to be spilt. According to our problem, this paper proposes the eight number of clusters to be defined, and to these objects are assigned to an each cluster initially. Then according to the initial centroid value, calculate distance between centroid and minutiae points Euclidean distance Equation (1). The minimum distance is retained in the updated distance matrix.

$$\|c_i\text{-}m_k\|^2 = \sum_{j=1}^{r} (c_i(j) - m_k(j)^2) \quad + \sum_{j=r+1}^{r} (c_i(j) - m_k(j)^2 \quad \text{---(1)}$$

The key points were grouped into new clusters until an optimum cluster reached. The optimum cluster value is reached, there after there are no possible movements for the minutiae points to move on the next cluster. At optimum level, centroid value is also calculated. The Centroid and key point binary value is calculated from the key points using AES algorithm [2].

*C. Cyclic Redundancy Check*

In this step it is to concatenate the original secret information (I/P) with CRC secret information to generate codeword. The CRC done for the secret information and random generate value. CRC is used to detect and correct the error. The secret code word of 128 bit message is generated from the secret information (I /P) x. Then this 128 bit message is encrypted by AES with 128 bit key.

*D. Advanced Encryption Standard*

Advanced Encryption Standard is a symmetric block cipher published by the National Institute of Standard and Tehnology (NIST) in December 2001.AES is non feistel cipher that encrypts and decrypts a data block of 128 bits. The key size can be of 128, 192 and 256 bit depends on the number of rounds. In this paper AES is used because it is simple to implement by using cheap processor and minimum amount of memory. It has better resistance against existing attacks and increases security with less power and high throughput.AES uses four types of transformations, they are substitution, permutation, mixing and key adding [7].

- AES, like DES, uses substitution. However, the mechanism is different. First, the substitution is done for each byte. Second, only one table is used for transformation of every byte, which means that if two bytes are the same, the transformation is also the same.
- Another process found in a round is shifting. Shifting transformation in the AES is done at the byte level: the order of the bits in the byte is not changed [8].
- In the encryption, the transformation is called Shift Rows and the shifting is to the left. The number of shifts depends on the row number (0, 1, 2, or 3) of the state matrix. This means the row 0 is not shifted at all and the last row is shifted three bytes.
- The mixing transformation changes the contents of each byte by taking four bytes at a time and combining them to recreate four new bytes.
- The operation in the Add Round Key is matrix addition. Since addition and subtraction in this field are the same, the Add Round Key transformation is the inverse of itself.

## III. IRIS DECRYPTION PHASE

In the iris decryption phase, the reverse process of encryption phase is done. The decryption phase also consists of two steps which are shown in Fig. 3. The first step is same as what was discussed in the encryption phase. The next steps, explains the decryption phase which is the reverse process of the encryption phase. The encrypted secret data is decrypted by AES with 128 bit key.

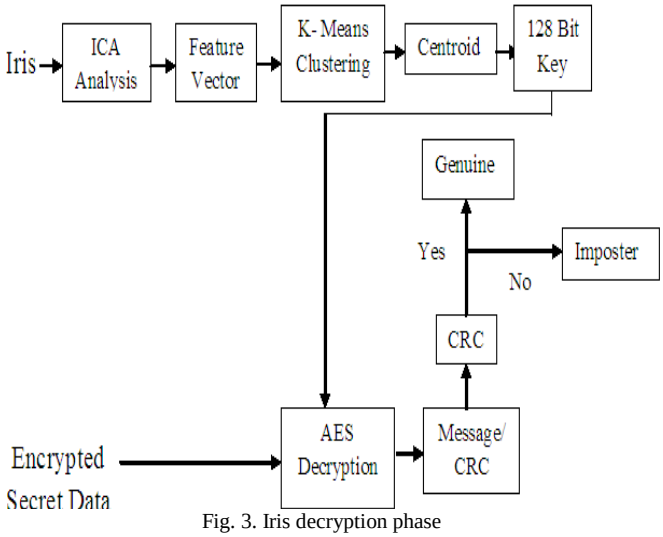


Fig. 3. Iris decryption phase

After decrypting we get a message. The message is checked with CRC to detect error and correct the error. If there is any modification in the message checked by CRC then it is an imposter. And if there is no modification or any other is not included I the original encrypted value then it is a genuine user. AES Decryption transformations are the inverse of the iris encryption phase [4]. From these processes the authentication as well as confidentiality is proven.

## IV. EXPERIMENTAL RESULTS

Experiments in this paper are conducted using the CASIA database. This database contains iris images with 249 sub databases; they contain left iris and right iris. Each sub database consists of 10 iris images each. Totally, database consists of 498 folders of 4980 FKP images. The images are taken randomly from the database and processed as explained in section II and III. The feature vectors are obtained from ICA process are shown in Fig. 5 and 6. The mean of the input image planes and the difference between each pixel with the mean value is shown in the Fig. 5. Then the covariance matrix and the Eigen values of the image are shown in Fig. 6.

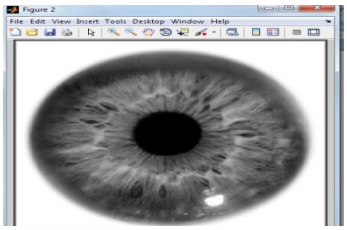

Fig. 4. Input iris image

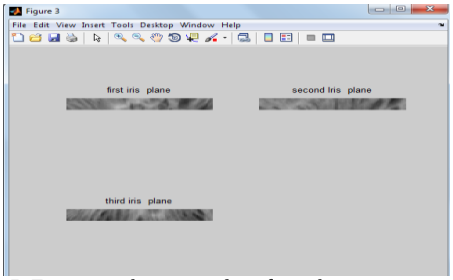


Fig. 5. Extracting the image plane from the input iris image

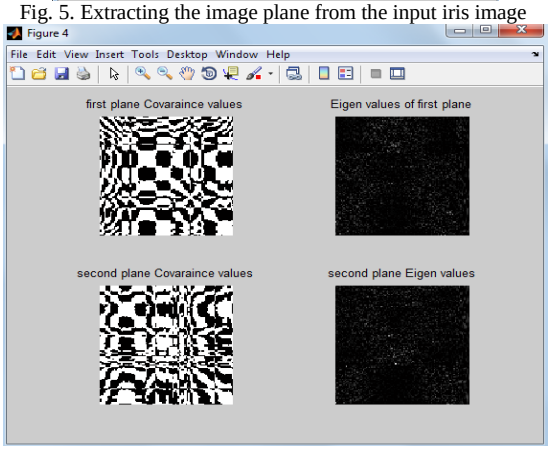


Fig. 6. ICA analysis results

The feature vectors of iris are extracted from ICA processes are grouped into eight clusters, and its centroid value obtained, which is converted into 128 binary bits. The 128 binary bits of iris obtained from above process is used as biometric key for Bio-encryption and decryption phase using AES algorithm.

## V. CONCLUSION

In this paper, ICA had reduced the dimensionality leaving those features that are critical for iris authentication. K-Means clustering had found that the same classification of different set in whole data. K-Means is made cluster tighter if the centroid found properly. AES was discussed so that in AES algorithm is very difficult to crack and is well suitable to security application and it has better resistance. AES is so simple and it had implemented easily.CRC had checked the message and give a genuine and imposter

## REFERENCES

[1] Youn Joo Lee, Kang Ryoung Park, Sung Joo Lee, Kwanghyuk Bae, and Jaihie Kim, "A New Method for Generating an Invariant Iris Private Key Based on the Fuzzy Vault System", *IEEE Transaction on Man and Cybernetics-Part B:Cybernetics*, vol. 38, No. 5, pp.1302-1313, Oct 2008.

[2] Muthu Kumar A., Kannan S., "Finger Knuckle Print Recognition with Sift and K-Means Algorithm*", ICTACT Journal Image and Video Processing*, vol. 3, No. 3, pp. 583-588, Feb 2013.

[3] Kshamaraj Gulmire, Sanjay Ganorkar, "Iris Recognition:An Emerging Biometric Technology", *IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)*, pp. 12-18.
[4] Mayank Vatsa, Richa Singh, et. al, "Improving Iris Recognition Performance Using Segmentation, Quality Enhancement, Match Score Fusion, and Indexing", *IEEE Trans. Systems. Man. And cybernetics-Part B: Cybernetics*, Vol. 38, No. 4, pp. 1021-1035, Aug 2008.
[5] John Daugman, "How Iris Recognition Works", *IEEE Trans. Circuit and Systems for Video Technology*, vol. 14, No. 1, pp. 21-30, Jan 2004.
[6] Boles W.W. and Boashash B., "A Human Identification Technique Using Images of the Iris and Wavelet Transform", *IEEE Trans. Signal Processing*, vol. 46, No. 4, pp. 1185-1188, Apr 1998.
[7] Behrouz A. Forouzan, "Cryptography and Network Security", *Tata McGraw-Hill*, 2007.
[8] Ramya M., MuthuKumar A., Kannan S., "Multibiometric Based Authentication Using Feature Level Fusion", *IEEE-International Conference On Advances In Engineering, Science And Management (ICAESM -2012)*, pp. 203-207, Mar 30, 31, 2012.
[9] Muthu Kumar A., Kannan S., "A Fingerprint based Biometric Authentication using Secured Hash and DES Algorithm" , *ICCIC 2011*, Dec. 2011.
[10] Kshamaraj Gulmire, Sanjay Ganorkar, "Iris Recognition using Independent Component Analysis", *International Journal of Emerging Technology and Advanced Engineering*, vol. 2, No. 7, pp. 2250-2459, July 2012.