Irisbased Authentication Scheme in WLAN Using Logistic Map with MAC

Sanjay Kumar[#1],D K Shaw[*2], Surjit Paul[#3]
[#1,3]Department of Computer Science and Engineering,
National Institute of Technology, Jamshedpur, Jharkhand, India
[1]sanjay.cse@nitjsr.ac.in
[3]paul.surjit55@gmail.com
[*]Department of Computer Applications,
National Institute of Technology, Jamshedpur, Jharkhand, India
[2]dkshaw.dca@nitjsr.ac.in

Abstract—**Shift from a wired network to a wireless network is rampant day by day due to the rapid development in information and wireless communications technology. But the wireless networks are insecure and more vulnerable to security threats and attacks. Biometric can play an important role in authentication and identification in WLAN. The image of iris varies from person to person; it could possibly be applied as a tool for biometric recognition and authentication used in WLAN. This paper attempts to introduce an iris based biometric authentication in WLAN using Logistic Map of cryptography and MAC. The encryption system utilizes an irisscanner to collect imagesof the iris of a person and applies an intelligent algorithm based on Chaos theory to generate initial keys for the Logistic Map. After applying Logistic Map, the randomness of irisimage results in a widely expanded key space which would be an ideal key generator for data encryption and decryption. Further to improve the security,We have introduced Message authentication Code (MAC) Scheme to match the hashed value of the decrypted templates from the encrypted templatesstored in the template database during enrollment with the MAC of current input iris image provided by the user for authentication.**

Keyword-Bio-cryptography, Logistic Map, Wireless LAN, Security, Iris, MAC.

I. INTRODUCTION

To ensure security initially password based authentication scheme was used, but later on two-factors of authentication procedure (“something known” and “something possess”) was introduced for authentication to enhance security. Further, to ensure more security third factor: “something inherent” is augmented along with the two-factors. Biometric traits are considered to be the third factor which may be physiological or behavioral characteristics of a person like face, iris, palm, fingerprint, retina, voice,handwritten signature, keystroke dynamics, gait, etc. which are unique, unalterable, universal and can be measured.

Biometric systems work by capturing a sample of the feature, such as recording a digital sound signal for voice recognition, or taking a digital scanned iris image for iris recognition. The sample is then transformed using some sort of mathematical function into a biometric template. The biometric template will provide a normalized, efficient and highly discriminating representation of the feature, which can then be objectively compared with other templates in order to determine identity. Most biometric systems allow two modes of operation. An enrollment mode for adding templates to a database, and an identification mode, where a template is created for an individual and then a match is searched for in the database of pre-enrolled templates. A good biometric is characterized by use of a feature that is; highly unique – so that the chance of any two people having the same characteristic will be minimal, stable- so that the feature does not change over time, and be easily captured – in order to provide convenience to the user, and prevent misrepresentation of the feature.

Fig1 showsthe block diagram of a biometric system which consists of two step process i.e enrollment and authentication. In the enrollment phase the sensor acquires the necessary data to be processed and represents the interface between the real-world and the biometric system. Afterwards, the pre-processing block is used to remove artifacts and noise from the data using advanced image processing techniques that enhance the acquired information at the input of the system. Once the data are cleaned, the feature extractor creates feature vectors designed to be unique to each individual.These features are used for the authentication. Using these features, a template vector or template is then created for further processing.At the enrollment phase, the encrypted templates using Logistic Mapare stored in the template database.In the authentication phase, MAC of the extracted feature vectors is of a particular user is compared to the MAC of the decrypted templates generated from an existing encrypted templatesof a particular user stored in the template database. If matching is found, then the user is authenticated and grants access to the user otherwise access is denied for the user.

DOI: 10.21817/ijet/2017/v9i1/170902309

Rest of the paper is organized as follows: Section II deals with related work, Section III deals with Proposed authentication scheme; Section IV presents experimental results and security analysis. Finally, we conclude the paper with conclusion and future work discussed in Section V.

II. RELATED WORK

HaojiangGao, Yisheng Zhang et. al.Proposed a new chaotic algorithm for image encryption. In this paper they presented a new nonlinear chaotic algorithm (NCA) which uses the power function and tangent function instead of linear function [1]. The experimental results demonstrated in this paper for the image encryption algorithm based on NCA shows advantages of large key space and high-level security, while maintaining acceptable efficiency. A novel chaotic fingerprint image encryption scheme is proposed combining with shuttle operation and nonlinear dynamic chaos system [2] was proposedby Song Zhao,Hengjian Li, and Xu Yan.Thechaos systemshows that the image encryption scheme provides an efficient and secure way for iris images encryption and storage. Muhammad Khurram Khan and Jiashu Zhang proposedan efficient and practical fingerprint-based remote user authentication scheme using smart cards, which is based on one-way collision free hash functions[3]. Experimental results derived in this paper show that the security, performance and accuracy of the presented system are encouraging for the practical implementation in real environment. A new image encryption technique was introduced by TiegangGao and Zengqiang Chen [4]. In their paper based on the image total shuffling matrix to shuffle the position of the image pixels and then uses a hyper chaotic function to complex the relationship between the plain image and the cipher image. The suggested image encryption algorithm has the advantage of large key space and high security. Moreover a coupled nonlinearchaotic map and a novel chaos-based image encryption technique were used to encrypt the color images by Sahar Mazloom and Amir MasudEftekhari-Moghadam[5]. In this paper they used the chaotic cryptography technique which is basically a symmetric key cryptography with a stream cipher structure. They used the 240 bit long secret key to generate the initial condition and to increase the security of the proposed system.

The schemes are especially useful for encryption of large amounts of data, such as digital images or electronic databases. The compound Chaos algorithm combines the Lorenz Chaotic system and Logistics map to generate the pseudo-random sequences. Then the pseudo-random sequences are used to produce the permutation matrix to encrypt the digital image [6]. A novel Chaos based Biocryptic Security aware packet scheduling algorithm (CBSPS) to strengthen the security levels in the WLAN [7] was proposed.

III. PROPOSED SCHEME

In this section, we have provided a brief introduction of Logistic Map, Preprocessing, Segmentation and Encryption and Decryption process.

The block diagram of the proposed authentication system is shown in the Fig 1.

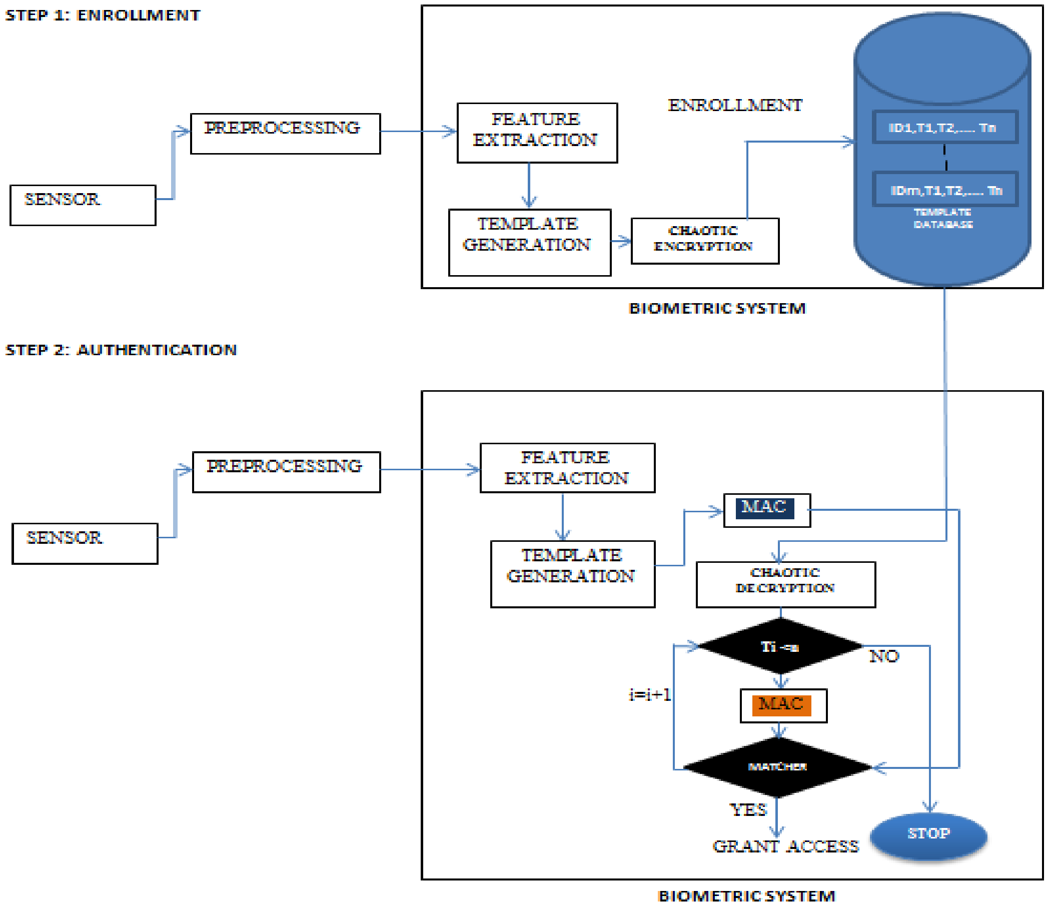


Fig. 1.Block diagram of proposed biometric system

Logistic Map: The Logistic Map is a polynomial of degree 2 dynamic model, which isexpressed as follows.

$$X_{n+1} = rX_n(1-X_n)$$

Where $X_n$is a system variable and r is the system parameter.

When X_n is the number between zero and one that represents the ratio of existing population to the maximum possible population. The values of the system parameter r are those in the interval [0, 4], but the interval of r [3.5699,4.00] gives a highly chaotic behavior with initial condition i.e $X_0 \in [0,1]$.

Preprocessing:In this technique, our goal is to enhance the visual appearance of biometric images and improve the manipulation of the dataset. Image resampling, gray scale contrast enhancement, noise removal, mathematical operations and manual correlation are required in this technique.

In image resampling, the no of pixels of the dataset are increased or reduced. Further the dataset is brightened to improve the visualization as shown in the below Fig2 and Fig3.

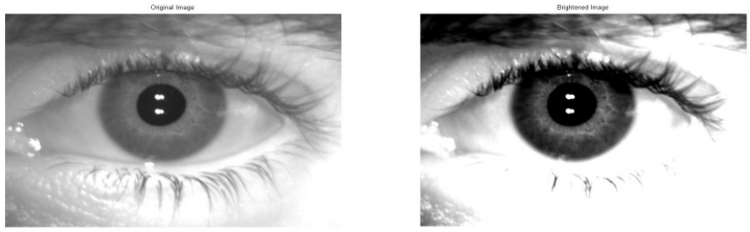


Fig. 2. Original image and corresponding brightened image

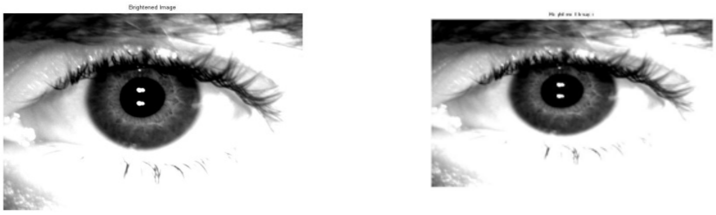


Fig. 3. Brightened image and its corresponding gray image

Noise removal: For removing the noise from the image dataset, several techniques like i) low pass, high pass, band pass spatial filtering, ii) mean filtering, iii) median filtering etc. can be used. Low pass filtering replaces all pixels of intensity higher than the specified value.Mean filtering and median filtering work on a (n x n) sub region of the image, generally usually 3 or 5.High pass filtering replaces all pixels of intensity lower than the specified value. Band pass filter replaces all pixels of intensity lower than the specified value and higher than another one. Low, High and Bandpass special filtering are efficient only in specific cases.Fig 4 shows the noisy image and its corronsponding median filtered image.

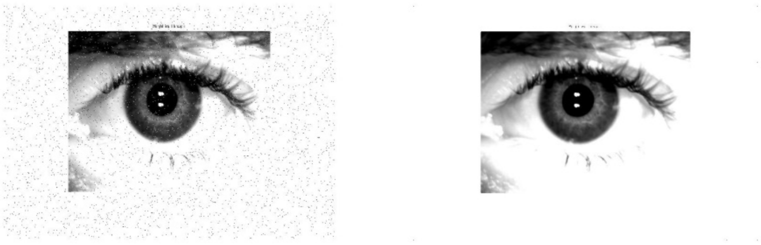


Fig. 4. Noisy image and its corresponding median filtered image

Dilation and Erosion:The most basic morphological operations used in image are dilation and erosion. Dilation adds pixels to the boundaries of objects in an image, while erosion removes pixels on object boundaries. The number of pixels added or removed from the objects in an image depends on the size and shape of the structuringelement used to process the image.

$$\text{Dilation-D(A,B)} = A \oplus B = \underset{\beta \in B}{\cup} (A + \beta)$$

$$\text{Erosion- E(A,B)} = A \ominus (-B) = \underset{\beta \in B}{\cap} (A - \beta)$$

Where, –B={-β|β ∈B}

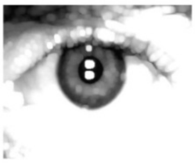


Fig. 5.Dilation with rolling ball element

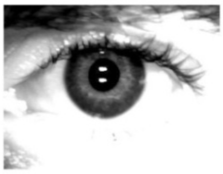


Fig.6. Erosion with line structure element

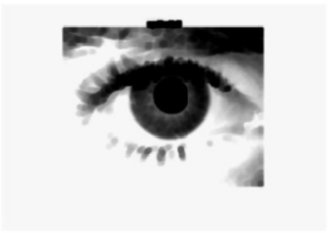


Fig. 7.Erosion with rolling ball element

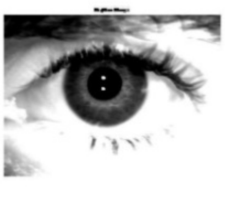
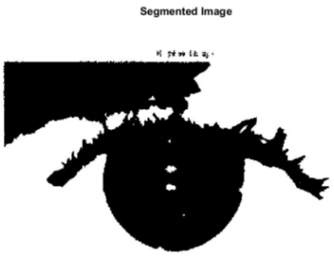


Fig. 8. Erosion with line structure element

Segmentation: It is the process of partitioning of an image into distinct (usually) non overlapping region in a meaningful way. It can also be thought of as a labelling operation, i.e a label corresponding to iris/anatomical structure is assigned to each pixel or voxel in the image.It identifies separate objects within an image and find a region of connected pixels with similar properties. It also finds boundaries between regions and remove unwanted regions.



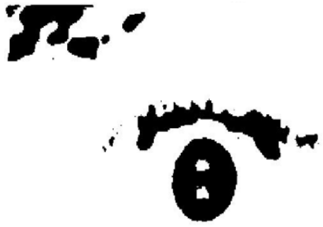


Fig.9. Segmented ImageFig. 10. Segmented Image usingactive contour

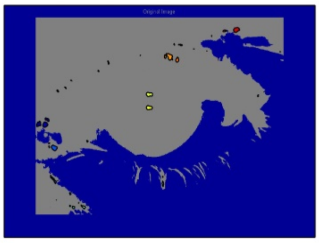
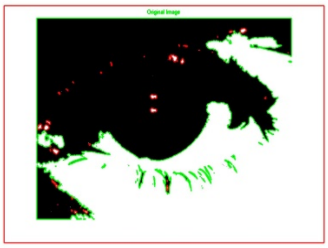


Fig. 11. Segmented image with image boundary



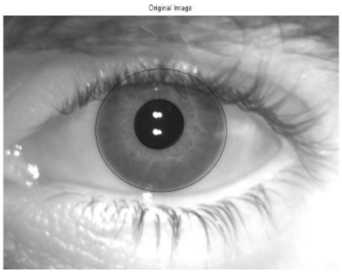


Fig.12. Segmented Image with complete boundary Fig.13. Circular boundary of pupil and iris

There are two types of image segmentation domain.

i) Image domain

ii) Feature domain

Image domain segmentation can be of the following types i) manual ii) thresholding iii) region growing iv) hierarchical.

Manual: Manual segmentation outlines the studied structure in each slice and is applied only on the contour or on the whole object. For segmentation, lines and splines can be used. It is usually a time consuming process.

Thresholding: It relies on intensity differences between structures in an image. It can be extended to multiple threshold levels; It is simple to implement but it is a low tolerance to intensity rescaling; difficult to set threshold and can use little of spatial information.

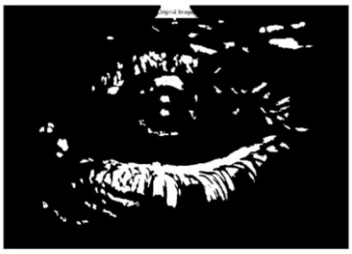


Fig.14. Threshold Iris Image

Region growing: It relies on intensity differences, but include the notion of spatial proximity of pixels and a seed point for the region.

Hierarchical: In this segmentation, pixels of the image are clustered into regions of similar intensity to create an intensity hierarchy. Wheninitial seed is merged to the desired structure ofthe hierarchy, then it iteratively separates the inside and outside of the hierarchical structure. This type of segmentation is fast and easy to implement, but have medium tolerance to intensity rescaling and needs human interaction for defining seed forms.

Feature domain segmentation: In this type of segmentation, each pixel is mapped to N pixels in the pixel space. It is powerful and tremendously flexible, but increase computations (because each pixel is mapped to N pixels). Also, large space requires a lot of data (for automated learning) or training examples (for supervised learning). Two types of feature domain segmentation are used, i.e supervised and unsupervised. In supervised segmentation a set of learning data is given, a learning algorithm uses this to determine a classification rule for new data, whereas in an unsupervised algorithm attempt is to discover clusters (or group of data points) in the feature space.

Encryption Process:In the proposed authentication scheme first capture an iris image and extract its features and generate a binary pattern from the given iris image. The binary pattern is further divided into small blocks of binary data to make the process simplified, because it is very difficult to encrypt the binary pattern of hundreds of thousands of bits at once. We made each block of 128 bits to make it simpler and to encrypt each block easily. A random block is then selected to create the initial condition for the secret key. The random selection of the block is preferred because of the attackers, so that no one can easily understand that which block is selected for the initial condition. At the transmission time of the image the bits of this randomly selected block are encrypted by using Logistic Map.

Fig15 presents the flow chart of the proposed chaotic algorithm. The steps of the algorithm are as follows.

1. Initial Condition X0 is generated by obtaining a random value between 0 and 255.
2. Using the initial condition obtains the series

   $$X_{n+1} = r.X_n\,(256-X_n) \bmod 256$$

   Where, n=1, 2, 3… is the map iteration index

   r= value in the interval [0,4] for logistic map.
3. The biometric key is obtained by selecting a random number between 1 and 2000, say i. For every Pixel (x, y), KEY [x, y] = Xi

   Where,iis a random number between 1 to 2000.
4. Ciphered Image is obtained by XORing the KEY with Input Image.
   Ciphered Image= P [x, y] XOR KEY [x, y]
   MAC of Image = SHA256 (P[x,y]||KEY[x,y])

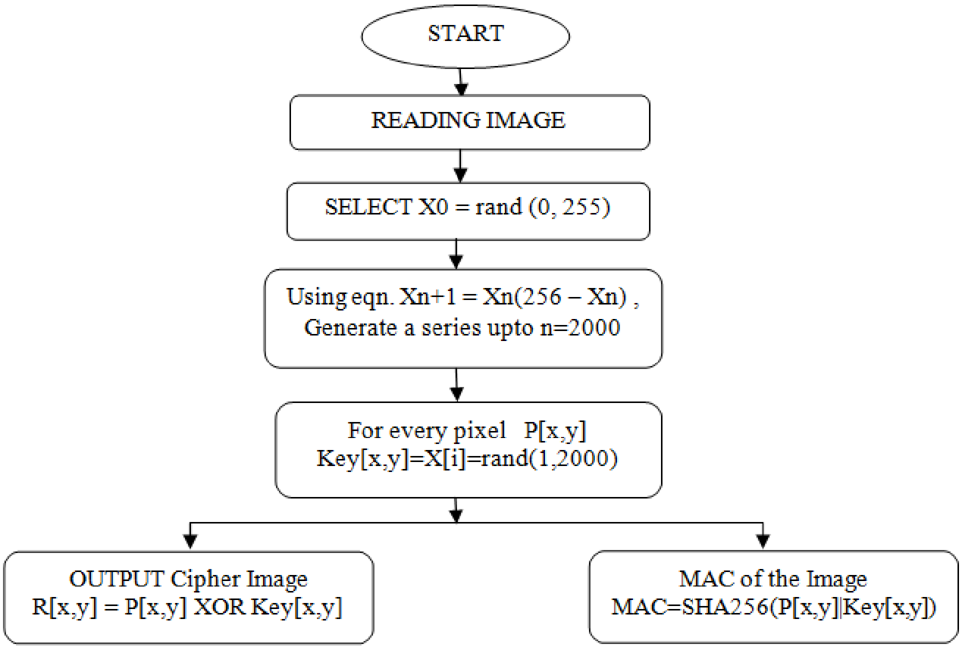

START
READING IMAGE
SELECT X0 = rand (0, 255)
Using eqn. Xn+1 = Xn(256 – Xn) ,
Generate a series upto n=2000
For every pixel P[x,y]
Key[x,y]=X[i]=rand(1,2000)
OUTPUT Cipher Image
R[x,y] = P[x,y] XOR Key[x,y]
MAC of the Image
MAC=SHA256(P[x,y]|Key[x,y])

Fig. 15. Flow Chart of Chaotic Algorithm

Decryption Process: In this process, decryption is done byXORing of the encrypted templates of a particular user stored in the template database with the same key used in the encryption process.

Plain Image= Encrypted Image⊕Key

Where,⊕ indicates Exclusive OR operation.

Authentication: In the authentication process, the MAC of the current captured iris image of a particular user is compared with the MAC of decrypted iris images from the encrypted iris templates of a particular user stored in the template database. If the match is found,thenthe user is authenticated and granted access to the system otherwise the system denied to the particular user to access the system.

IV. EXPERIMENTAL RESULTS

In order to evaluate and check the performance of the proposed algorithm, the database contains a lot of iris images taken from different people eyes. In our case, we have created the dataset of iris images of 80 people in our biometric lab, Department of CSE, NIT Jamshedpur and is used to carry out the experiment. These iris imagesare encrypted using logistic map for different value of r, where r is any real value between 0 and 1. The histogram image of the corresponding iris image is generated using Matlab are shown as given below. By observing the maps carefully it’s clear that even changing in a small part of the value the whole map become different and are more invisible. The different encrypted templates of iris images of a person is stored in the template database. During Authentication,MAC of the decrypted iris template stored in the template database is matched with the MAC of theiris images captured during authentication.If match is found then the claimant is authenticated and granted access to the system. For each case i.e. encryption, decryption and MAC generation using SHA256 the corresponding histogram are generated and is shown in the Fig. 19 .

A. Security Analysis

1. *Key space Analysis:* In our proposed biometric authentication scheme, we are using 128 bit symmatric key for encryption and decryption. The key space of this symmatric key is 2^{128} , which is enough to resists from all kind of brute-force attack. The key can be 256 bit which will provide larger key space, but it will take loger time for encryption, decryption as well as authentication process, which is not suitable for WLAN biometric authentication.
2. *Key Sensitive Analysis:*In the proposed scheme based on logistic map exhibits chaotic behavior with the value of r ranges from [0 4]. From r=3.57 upto r=4.0, it exhibits significant chaotic behavior. A small change in the key will generate a large chage in ciphered image, from which it is difficult to get the corresponding correct image. It fulfills the principle of avalanche effect.
3. *Analysis of corelationof adjacentpixel:*To test correlation between two vertically, horizontally and diagonally image pixels of original and ciphered image, we randomly select 25 adjacent pixelsof original gray image and encrypted gray image. Then we calculated the correlation coefficient of two adjacent pixels using standard correlation equaltion and plotted the correlation matrix.

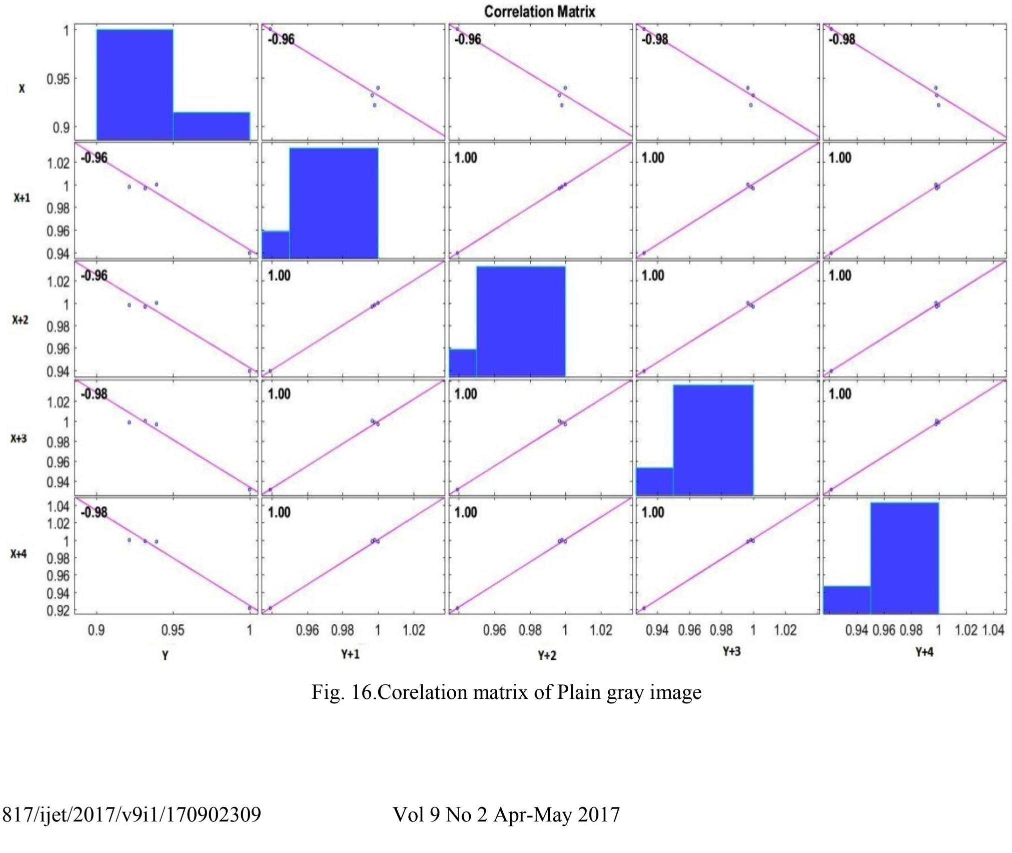


Fig. 16.Corelation matrix of Plain gray image

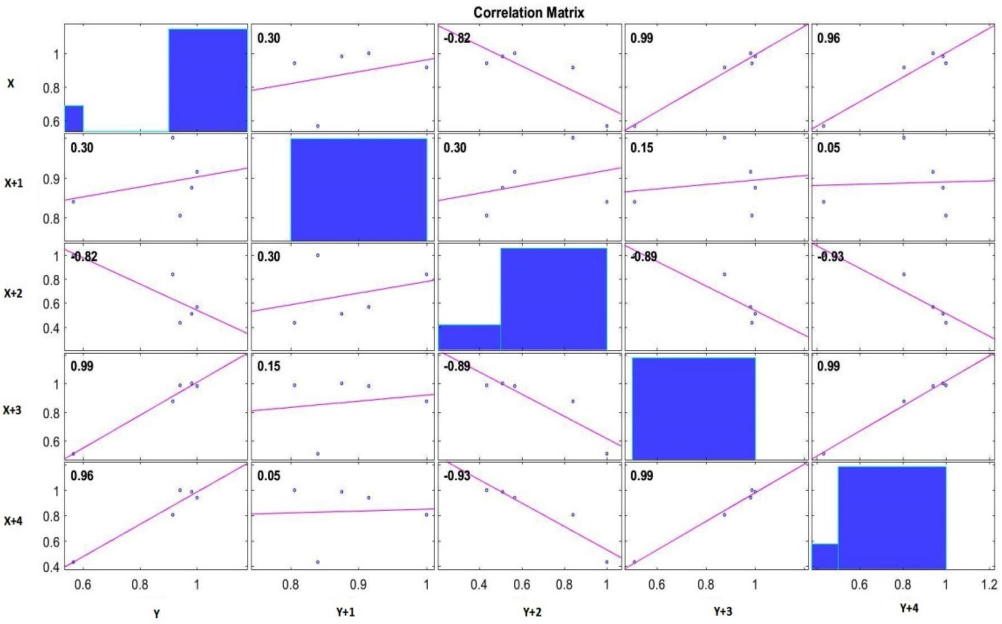


Fig. 17.Corelation matrix of encrypted gray image

From the above two correlation matrix, it is clear that there is a less correlation between two adjacent pixels of the encrypted image. However, the two adjacent pixels of the original image are highly correlated.

B. Entropy Analysis

For the proposed biometric authentication scheme based on logistic map the encrypted image is influenced by the value of r. The logistic map chaotic behavior can be visualized with the value of r ranges from [0,4].There is a abrupt chaotic behavior is visualized when r lies between [3.57, 4.0]. From the test run, the entropy of the britened gray image of iris is found to be 2.7977. At this enropy the image is brightened and easily visualized. After applying the logistic map for encryption the entropy of encrypted image must be greater than 2.7977. From the test run it is found that the entropy of the encrypted image is based on the value of r of logistic map and found to be maximum at 3.89 which is 5.7002. It ensures the security of the encrypted image. For r ≥3.57 and r ≤4.0 there is a sharp change in entropy, which is shown in the below Fig. 18.

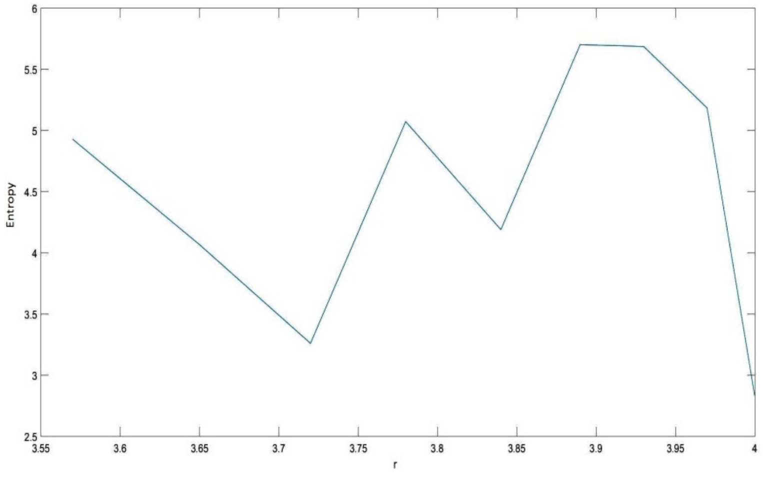
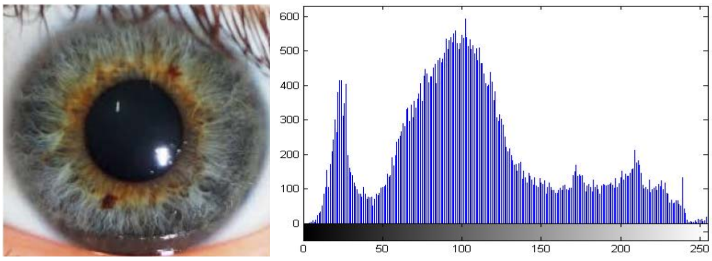


Fig. 18. Entropy of encrypted gray image with respect to r

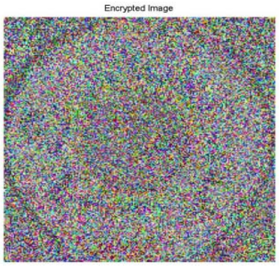
C. Histogram Analysis

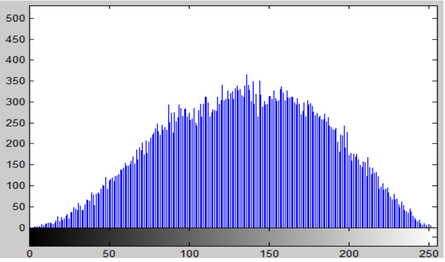
It is usuallyused for statistical analysisattack. The image histogram illustrates the distribution ofimage pixels by graphing a no. of pixel at each color intensity.In the Fig. 19, we have shown the histograms of original iris image, its encrypted image for the different value of r of the logistic map. From the below Fig. 19., it is clear that the histogram of the encrypted image is completely different than the original image and hence does not provide any clue to the attackers for employing stastistical attack on the proposed image encryption technique.



Original RGB ImageHistogram of Original Image

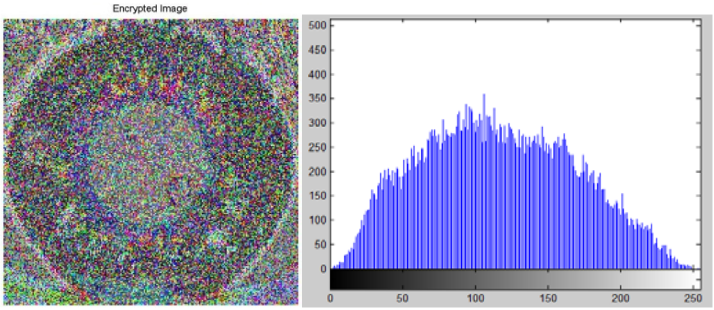
For r=3.97





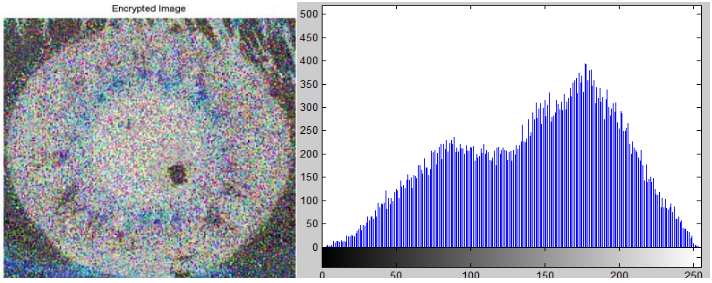
Encrypted Image Histogram of Encrypted Image

For r=3.89

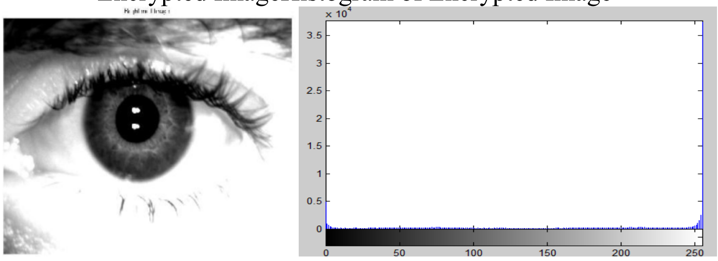


Encrypted ImageHistogram of Encrypted Image

For r=3.57

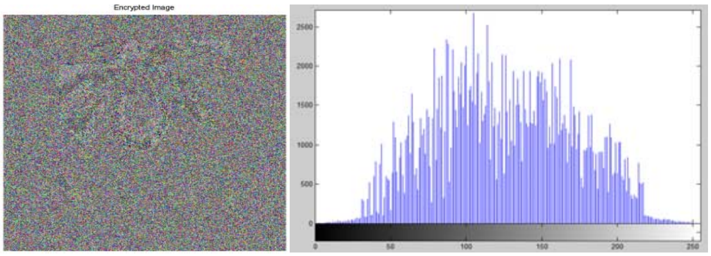


Encrypted ImageHistogram of Encrypted Image



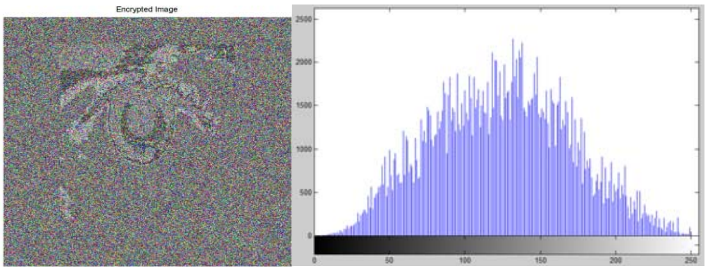
Original Gray ImageHistogram of OriginalGray Image

For r=3.97



Encrypted Gray ImageHistogram of Encrypted GrayImage

For r=3.89



Encrypted Gray ImageHistogram of Encrypted GrayImage

Fig. 19. Histogram analysis of RGB and gray image of Iris

V. CONCLUSION

This paper presents aniris based authentication scheme in WLAN using Logistic Map and MAC. The proposed algorithm takes an iris image and convert it into the binary bits pattern and divide them into small blocks of 128 bits long to simplify the process. Then a random block is selected from all these blocks to create the initial condition. This initial condition is then passed from the LFSR to generate the secret key. A secret key of 128 bits is generated from the result of the LFSR. This secret key is then used for the encryption of the iris image. The same procedure is then used at the receiver end to decrypt the iris image. Chaotic function is used to make the algorithm more secure and make the process of the encryption and decryption more complex. Experimental results and security analysis of the algorithm shows that the algorithm is stronger and more secure and can be used for the practical implementation of the iris base authentication scheme in WLAN.

REFERENCES

[1] Haojiang Gao, , Yisheng Zhang, Shuyun Liang,Dequn Li “A new chaotic algorithm for image encryption”,Chaos, Solitons & Fractals, Elsevier,Volume 29, Issue 2, 2006, pp. 393–399.

[2] Zhao Song, Li Hengjian ,Yan Xu, “A Secure and Efficient Fingerprint Images Encryption Scheme”, IEEE conference ICYCS 2008, DOI 10.1109/ICYCS.2008.49, 2008, pp. 2803 – 2808.

[3] Muhammad Khurram Khan, Jiashu Zhang, “An Efficient and Practical Fingerprint-Based Remote User Authentication Scheme with Smart Cards”, Second International Conference, ISPEC 2006, Hangzhou, China, DOI 10.1007/11689522_24, 2006, pp. 260-268.

[4] Tiegang Gao, Zengqiang Chen, "A new image encryption algorithm based on hyper-chaos", Physics Letters A,Vol. 372, Issue 4, 2008, pp. 394–400.

[5] Sahar Mazloom, Amir MasudEftekhari-Moghadam, “ Color image encryption based on Coupled Nonlinear Chaotic Map. Chaos, Solitons and Fractals, Vol.42 ,2009, pp. 1745-1754.

[6] Zhang Jun, Li Jinping, Wang Luqian. A New Compound Chaos Encryption Algorithm for Digital Images. International Forum on Information Technology and Applications (IFITA-2010).

[7] Sanjay Kumar, D.K Shaw, “Chaos based Encryption Mechanism for Wireless Local Area Network Authentication, “International Journal of Applied Engineering Research”, Vol. 10, No. 15, 2015, pp. 35147-35152.

[8] https://en.wikipedia.org/wiki/List_Of_chaotic_maps.

[9] Nithyanandam.S, Gayathri.K.S, Priyadarshini P.L.K “A New IRIS Normalization Process For Recognition System With Crytographic Techniques”, Internationtional Journal of Computer Science Issues, Vol 8, Issue 4, No 1, July 2011, pp. 342-348.

AUTHORS PROFILE

	Sanjay Kumar is an associate professor of Department of Computer Science and Engineering at National Institute of Technology, Jamshedpur, India. His areas of research are Cryptography and Network security, mobile computing, parallel computing and VANET.
	Dr. Dilip Kumar Shaw is an associate professor of Department of Computer Application at National Institute of Technology, Jamshedpur, India. His areas of research are Supply Chain Management,Data Mining, Cryptography, Computational Complexity, Network Optimization.
	Surjit Paul is an M.Tech scholar of Department of Computer Science and Engineering, National Institute of Technology, Jamshedpur, India. He is UGC-NET-JRF qualifiedand his areas of research interests are mobile computing, VANET, Cryptography and Network Security.