Thumb based Biometric Authentication Scheme in WLAN using Gauss Iterated Map and One Time Password

Sanjay Kumar*
Department of Computer Science and Engineering National Institute of Technology Jamshedpur, Jharkhand, India sanjay.cse@nitjsr.ac.in

Surjit Paul
Department of Computer Science and Engineering National Institute of Technology Jamshedpur, Jharkhand, India paul.surjit55@gmail.com

Abstract Due to advancement in E-commerce, M-Commerce and rapid development in wireless technology shift of users from wired network to wireless network have increased day by day. Since wireless networks are easy to break and prone to security threats, it is important that all wireless users are required to be authenticated before using the information present in the wireless LAN. Also doing secured online transaction in wireless LAN, authentication of user is the upmost requirement. Due to uniqueness of biometric traits it can be used in authentication. In this paper, we proposed a finger based biometric authentication scheme. During enrollment, minutia points are generated and encrypted using Gauss Iterated Map. The encrypted template is stored in the template database. During authentication, a matcher algorithm is used to match the minutia points of the decrypted thumb template of the particular user captured during enrollment with the minutia points generated during authentication. If match is found then server will generate a One Time Password (OTP) and send to the user for further level of authentication. If user enters the correct OTP through client interface to the server then ARAS (Advanced Remote Authentication Server) grants permission to access the system to that user otherwise access is denied to the user.

Keywords: Wireless LAN; OTP; Gauss Iterated Map; Bio-cryptography; Authentication.

1. Introduction

Traditionally, username and password was common method for authentication and was initially used in plaintext format. Later on username and hashed password was used. To further strengthen the authentication scheme, salted hashed password is used. People use small passwords because it is difficult to remember long and complex password which can be easily guessed by the attackers. Further to increase the level of authentication two authentication factors is used i.e. something known and something possesses like debit card and PIN number. But there is chance of stealing and loss of the debit card.

Because of the problem with username and password, PIN number stated above; researchers started looking into the alternative method for authentication. Biometric traits are unique feature for every person and it cannot be stolen or lost. It is categorized into two categories i.e. physiological and behavioral. In Physiological finger print, thumb images, retina, palm print, DNA, Voice, and Face etc. are used whereas for behavioral keystroke, signature, voice etc. are used. Our proposed biometric authentication system consists of two phases. The first phase is enrollment phase and the second is the authentication phase. In the enrollment phase, the thumb biometric sensor is used to capture the thumb print of an individual and then preprocessing and feature extraction is carried out to generate a template. Then the template is encrypted using Gauss iterated Map. The encrypted thumb print is stored in the database along with user credentials like username, address, mobile no. etc. During authentication phase again thumb biometric sensor is used to capture the thumb then preprocessing and feature extraction is done on the capture thumb image to generate the template. The minutia points of decrypted thumb template of the user are matched with the minutia points of the current template in order to verify the claimed identity. Further to ensure higher level of authentication, an OTP is generated by the ARAS (Advance Radius authentication server) and sent to the requester's registered mobile. The requester has to enter the sent OTP through client interface. If OTP is matched then the system grants permission to the user and is authenticated to access the system.

The paper consists of five sections. Section 1 Introduction, Section 2 deals with related work, Section 3 deals with system architecture of the proposed authentication scheme; Experimental results are discussed in Section 4. Finally, section 5 deals with conclusion and future work.

2. Related work

Based on the comparison of password and password with fingerprint system was studied for 96 volunteers. It was found that account created using password with fingerprint was1/3000 times difficult to break than password (Wimberly and Liebrock, 2011) [1]. An efficient smart card based one-way collision free hash function using fingerprint user authentication scheme was proposed (Khan and Zhang, 2006) [2]. This system enhances the security. Image encryption technique in which, image pixels are shuffled and then hyper chaotic was applied for diffusion in order to gain security and large key space (Gao and Chen, 2008) [3]. To expand the secret key space and to improve anti-aggressive ability a two Chaos algorithm namely Lorenz Chaotic system and Logistics map was used to generate the pseudo-random sequences (Jun et al., 2010) [4]. To encrypt the color images, a Coupled Nonlinear Chaotic Map and a chaos-based image encryption algorithm were used (Mazloom and Moghadam, 2009) [5]; in which, a symmetric key cryptography and a stream cipher were used. In this combined structure, 240 bits key was used to generate the seed and parameter of the chaotic map. The privacy and security trade-off of a single biometric system were measured by information theory techniques and by biometric measurements respectively (Lai et al., 2011) [6]. To increase the security, various different biometric traits are used. The Logistic and BSPS (Bio chaotic Security aware packet scheduling) were combined to strengthen the security levels in the WLAN (Kumar and Shaw, 2015) [7].

3. Proposed scheme

In the proposed biometric system there are two phases i) Enrollment and ii) Authentication.

i) Enrollment: In the enrollment phase, thumb is captured by Manta MFS 100 thumb scanner. Then the raw thumb image is preprocessed and correct minutia points are extracted from all the minutia points and stored in the file. To make the encryption process simple the binarized template is further divided into small blocks of 128 bits. From these blocks, a random block is chosen to generate the initial condition for the secret key. The image bits of this block are encrypted by using Gauss Iterated Map and stored in the template database. The block diagram of the proposed scheme is shown in Fig 1 and its corresponding steps have been discussed as follows.

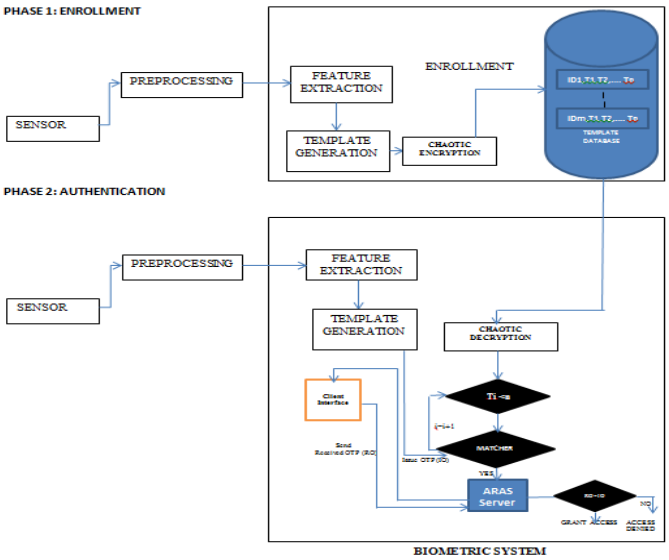


Fig 1. Block diagram of proposed biometric system

3.1. Preprocessing and feature extraction

Under this phase, firstly the thumb image was captured by thumb biometric scanner. The captured image was brightened, filtered, converted into gray scale, eroded and dilated as shown in the Fig 2 to Fig 6.

Fig 2. Original image and corresponding brightened image

Fig 3. Brightened image and its corresponding gray image

Noise removal: Median filter is used to remove the noise present in the thumb image.

Dilation and Erosion: To add pixels to the boundary of the thumb image Dilation is used where as to remove the pixels from the boundary of the thumb image, erosion is used.

Fig 4. Noisy image and its corresponding median filtered image

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

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

Where $-B=\{-\beta | \beta \in B\}$

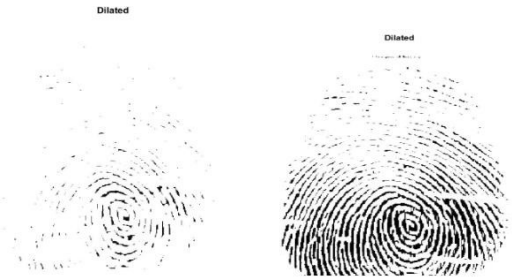


Fig 5a Fig 5b

Dilation with rolling ball element Dilation with line structure element

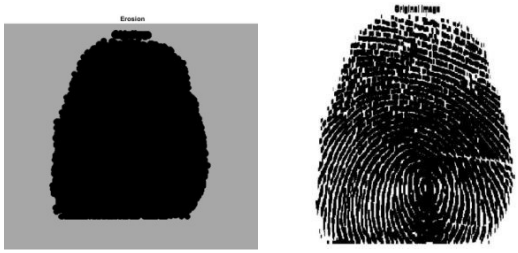


Fig 6a Fig 6b

Erosion with rolling ball element Erosion with line structure element

Feature Extraction: During feature extraction, the binarize image is converted into thin image. From thin image minutia points are generated which contains false minutia points also. This is further removed by using Euclidian distance between two points .Then region of interest (ROI) is selected and corresponding minutia points within ROI is generated and stored in the file for matching of minutia point during authentication. The following figure Fig 7 shows the steps used in feature extraction.

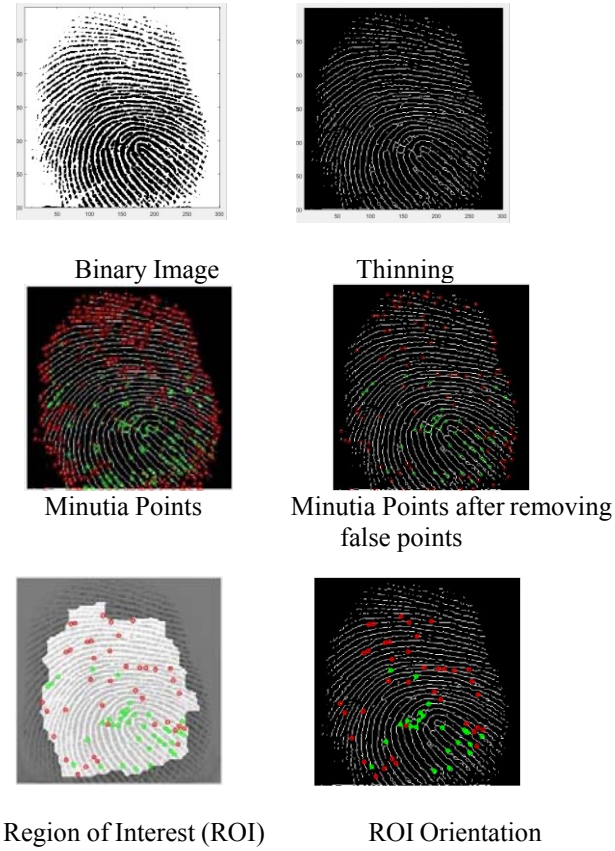


Fig 7. Steps of Feature Extraction

3.2. Segmentation

In this process, the thumb image is partitioned into different non-overlapping region shown in Fig 7.

Thresholding: Here we convert the gray-scale thumb image into a binary image based on a threshold value.

Fig 8. segmented image

Fig 9.Threshold image

3.3. Encryption Process

In this process, encrypted image is generated from the thumb template image by doing XORing operation. The flowchart of the proposed chaotic algorithm is shown in Fig 9. Its algorithm is as follows.

Step 1: Initial Condition X_0 is generated by obtaining a random value in between 0 and 255. Step 2: Using the initial condition obtains the series

$X_{n+1}=\text{Exp}(-\alpha.X_n^2) + \beta$

Where n=1, 2, 3… is the map iteration index. The value of α is any positive value, whereas the value of β ranges between [-1, 1]. We generate the gauss iterated map for different values α and β. which is in the next section.

Step 3: The biometric key is obtained by selecting a random number between 0 and 1. For every Pixel(x,y).

KEY[x,y] = Xi, where i is a random number between 0 to 1.

Step 4: Ciphered Image is obtained by XORing the KEY with input image.

Ciphered Image= P[x,y] XOR KEY[x,y]

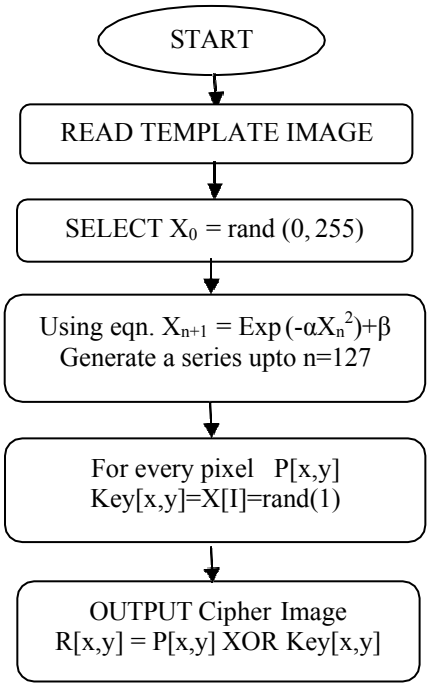


Fig 10. Flow Chart of Chaotic Algorithm

3.4. Decryption Process

In this process, decryption is done by XORing 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 $\oplus$ Key

Where $\oplus$ indicates Exclusive OR operation.

ii) Authentication

In the authentication phase, the thumb image is captured using the Mantra MFS100 finger scanner. The captured image is preprocessed and its features are extracted. Finally its template is generated. This template contains the minutia points which are used to match with the minutia points generated after decryption of the stored template in the template database. If match is found then the ARAS (Advance remote authentication server) will generate an OTP (One time password)and send to the client. Client has to enter the OTP sent by the ARAS server. The both OTP (client and server) is matched by the ARAS. If match is found then user is authenticated and gained access to the system otherwise the system denied to access the system.

4. Experimental results

In our proposed system the encryption and decryption is performed using Gauss Iterated Map. It is derived based on the following mathematical function.

$$X_{n+1} = \text{Exp}(-\alpha . X_n^2) + \beta$$

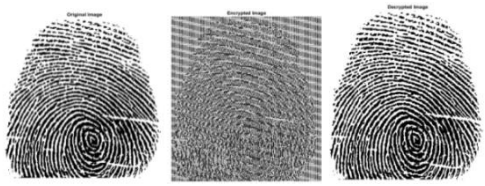
Where,

α is any positive value.

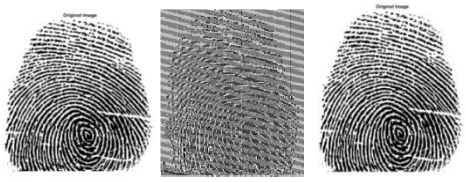
β value ranges between [-1, 1].

The experiment is conducted for encryption and decryption of the thumb image for various value of α and β shown in Fig 11. For the value of α=4.9 and β=-0.38, the Gauss Iterated Map shows the maximum randomness and chaotic behavior. It is used for generating the key for encryption and decryption of the template.

α =4.9 β=-0.38

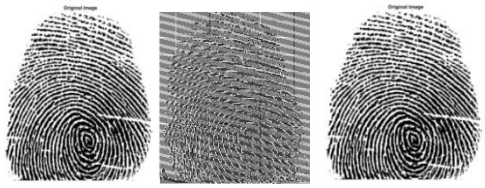


α=1.90 β=-0.25



α =2.25 β=-0.29

α=2.70 β=-0.42



α=4.90 β=0.58

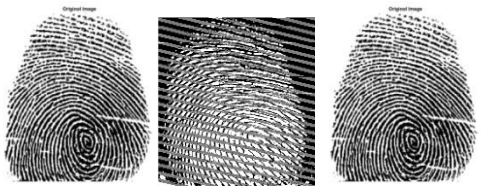


Fig11. Encryption and decryption of thumb images

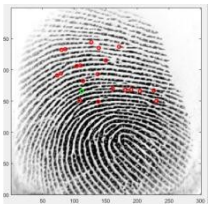


Fig 12. Minutia point matched

Minutia points of the region of the interest (ROI) are matched with the minutia points of the region of interest of decrypted template. If 95% of the points are matched then user is authenticated otherwise user is not authenticated. Matched minutia points of the thumb image are shown in the Fig 12.

5. Conclusion

The system security is judged by how robust its encryption technique is. In the proposed scheme, 128 bit symmetric key generated by gauss iterated map is chaotic in nature and it is difficult to guess by the adversary. The variation of key generated by Gauss Iterated Map for different values α and β are numerous and any one of them can be chosen for encryption and decryption. But for α=4.9 and β=-0.38, the Gauss Iterated Map shows the maximum randomness and chaotic behavior. Further OTP enhances the security mechanism and makes the system robust.

References

[1] Wimberly, H; Liebrock, L.M. (2011): Using Fingerprint Authentication to Reduce System Security: An Empirical Study. IEEE Symposium on Security and Privacy, pp. 32-46.

[2] Khan, M. K; Zhang, J. (2006): 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, pp. 260- 268.

[3] Gao, T; Chen, Z. (2008): A new image encryption algorithm based on hyper-chaos. Physics Letters A, 372(4), pp. 394– 400.

[4] Jun, Z; Jinping, L; Luqian,W. (2010): A New Compound Chaos Encryption Algorithm for Digital Images. International Forum on Information Technology and Applications (IFITA-2010), Kunming, China, DOI: 10.1109/IFITA.2010.117, pp. 277-279.

[5] Mazloom, S; Moghadam, A. M. E. (2009): Color image encryption based on Coupled Nonlinear Chaotic Map. Chaos, Solitons and Fractals, 42(3), pp 1745-1754.

[6] Lai,L; Ho, Siu-Wai; Poor, H.V. (2011): Privacy–Security Trade-Offs in Biometric Security Systems—Part I: Single Use Case. IEEE Transactions on Information Forensics and Security, 6(1), pp.122-139.

[7] Kumar, S; Shaw, D.K. (2015): Chaos based Encryption Mechanism for Wireless Local Area Network Authentication. International Journal of Applied Engineering Research, 10(15), pp. 35147-35152.