

Chaos based Improved Double Bio-cryptic Authentication Process to Access WLAN

Perabathula Naganjaneya Prasad
Dept. of Computer Science & Engineering
Swarnandhra College of Engineering&Technology
JNTUK, West Godavari, India

Kodeti Haritha Rani
Dept. of Computer Science & Engineering
Swarnandhra College of Engineering&Technology
JNTUK, West Godavari, India

ABSTRACT

The usage and applicability of Information and Communication Technology (ICT) is increased from the past three decades. Monitoring quality-of-Service (QoS) pertaining to networks is a major challenge for the researchers and academicians. Bandwidth, Latency, Jitter, Loss of data and security are some of the important parameters related to the network QoS. Especially security plays an important role regarding data confidentiality in wired or wireless networks is concerned. Particularly, there is a need to strengthen the authentication process in Wireless Local Area Network (WLAN). This paper introduces a novel Double Chaotic Bio-cryptic Security aware Packet Scheduling (DCBSPS) algorithm to improve WLAN's authentication mechanism. DCBSPS algorithm comprises different security levels in association with chaos based cryptic biometrics like face, fingerprint, Iris, and thumb print. In addition, DCBSPS algorithms take the advantages of Chaotic Bio-cryptic Security aware Packet Scheduling (CBSPS) and Chaotic Multilevel Remote Sensing Data encryption (CMRSDE) algorithms to improve the Quality-of-Authentication in WLAN. The experimental results of DCBSPS were compared with the chaotic and non-chaotic, based procedures like CBSPS and Multi-merged Bio-cryptic Security aware Packet-scheduling (MMBSPS). The obtained results exhibits, DCBSPS algorithm performs better than the rest in terms of reliability, security level, guarantee ratio and Overall Performance.

General Terms

Security, Algorithms, Networks.

Keywords

Double Chaotic Bio-cryptic Security aware Packet Scheduling, CBSPS, DCBSPS, Chaotic, Chaos, Logistic map, Henon map and encryption.

1. INTRODUCTION

The ICT became more popular because of its wide range of applications like Internet-of-Things (IoT). The future of IoT covers a wide range of applications like Health care, Automotive, Wearables, Smart cities, Smart manufacturing and Home automation [1]. To meet the security of the requirements of the Web 3.0, there is a need to strengthen the Wireless Local Area Networks (WLAN). Many security risks like Denial-of-Service, Man-in-middle attack, Rogue Access Point, Illicit entry and other risks make WLAN weaker [2]. In order to restrict the Illicit entry attack, the authentication process needs to be improved in WLAN. According to the CISCO Survey report-2015 states that, 70 company users experienced 1751 threats on an average per month and Spam volume increased 250 percent from January 2014 to November 2014 [3]. Common security is one reason for this

numerous attacks and drastic change in the spam volume. Maintaining security levels for various users, according to requirements, will be a better option for minimizing the intelligence security threats. In the literature of the security levels, many researchers and Engineers proposed various solutions, which has reduced the security loss and improved the fast and reliable communication between the client-server. Whereas Bio-cryptography technique improved the authentication process rather than traditional cryptic-text methods [4]. Especially the Chaos theory and related maps brought a novel revolution in the image encryption domain. Maps like Logistic, Cubic, Arnold cat's, Baker's, Henon etc. are more popular maps for the cryptic-images.

This work introduces a new authentication process, which will improve the performance of the WLAN security. Novel double chaotic map encryption is adopted and applied on the biometric templates like thumb-print and Iris. Previously, researchers discussed the security levels with various algorithms like Watermarking and Chaos. The main objective of this work is to provide the secure authentication to the biometric templates. Especially the Government of India (GOI) initiated the two major projects for the 12.5 million population in the country, named as Digital India and AADHAR. Where Biometric based authentication is going to play a major role. The rest of the details are discussed in the next section.

The significant additions of the paper are as follows: (1) a study and investigation Chaotic based security levels in WLAN; (2) a double Chaos based Bio-cryptography authentication mechanism; and (3) a neoteric measurements by associating the security level and guarantee ratio; (4) a simulation model where the DCBSPS algorithm is developed and executed perfectly. The classification of the article is as pursued. Related works discussed in Section 2 in the area of 2D logistic maps and 2D Henon Maps, security level, and Bio-cryptography. The nominate mechanism DCBSPS algorithm is described in Section 3. The security level Bio-encryption simulations and outcomes defined in Sections 4. The paper terminated in section 5 with a conclusion and future scope.

2. BACKGROUND WORKS

The Security Level (SL) initiation started by Xia Qin for the realtime wireless networks through Security SPSS architecture [5]. Later it is carried out by the Rajesh Duvvuru et al., and proposed Automated Security Aware Packet Scheduling (ASPS), Bio-cryptic Secure Aware Packet Scheduling (BSPS) and Enhanced Bio-cryptic Secure Aware Packet Scheduling (EBSPS) for the strengthening the authentication process through Biometric and RSA algorithm. [6][7][8]. In addition to this Avala Ramesh et al., developed the Enhanced Merged Bio-cryptic Secure Aware Packet

Scheduling (EMBSPS) and Multi Merged Bio-cryptic Secure Aware Packet Scheduling (MMBSPS), the methods resulted in for the fast and reliable communication in WLAN [9] [10]. Sanjay Kumar introduced the six level Biometric authentication, by adding the voice biometrics in Improved BSPS (IBSPS) [11]. Later Ganesh and Sudhakar Godi proposed the developer came up with the Double BPSP (DBSPS), where Earlier all the mechanisms are single Bio-encrypted[12]. However, the encryption done through the non-bio-encrypted methods. Then, Uma Devi et al, designed and tested Multi Merged Biometric Watermarking Security aware Packet Scheduling (MMBWPS) and it contains the Bio-watermarking encryption technique [13]. Recently the once again Sanjay Kumar et al, proposed a innovative idea in the form of Chaotic BSPS (CBSPS) for the biometric template authentication [14]. Once again, Rajesh Duvvrur performed a multi encryption on Satellite Images using the Chaos based approach, which is named as Chaotic Multilevel Remote Sensing Data encryption (CMRSDE) algorithm [15]. The present proposed work comprises of CBSPS and CMRSDE mechanism.

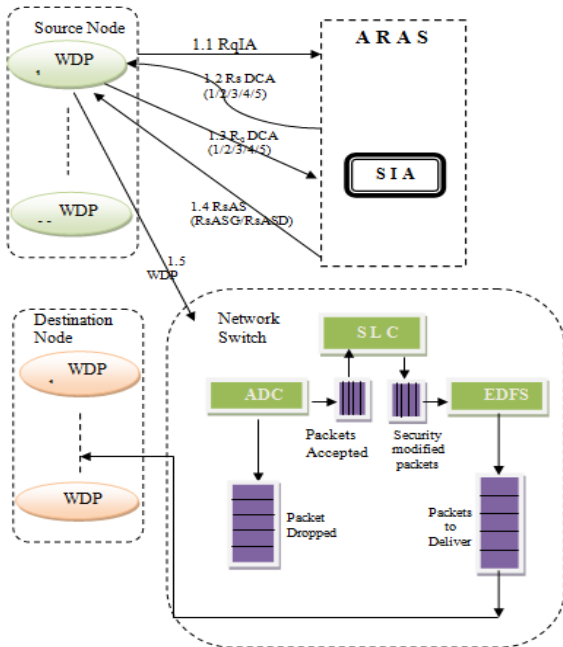


Fig 1: The architecture of the Network Model

2D Henon Chaotic map [16] shown mathematically in equation 1.

$$\text{Henon } (x_{i+1}, y_{i+1}) = (a + x_2 + by, y' = x) \quad \text{----- (1)}$$

Equation 2 shows the 2D Logistic Chaotic map represents as follows [17]:

$$\text{Logistic } (x_{i+1}, y_{i+1}) = (r(3y + 1)x_i(1 - x_i), r(3x + 1)y_i(1 - y_i)) \quad \text{----- (2)}$$

Where Logistic(x_{i+1}, y_{i+1}) is the spatial coordinates of i ranges from 1,2,3,...n and r is a chaotic behavior parameter with value 1.19.

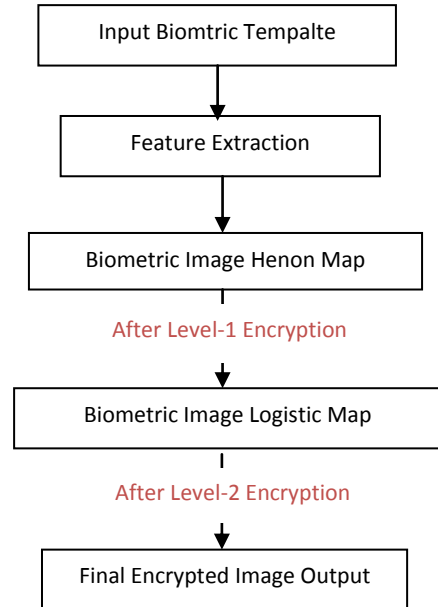


Fig 2: Functional block diagram of the DeBc algorithm

3. DOUBLE CHAOTIC BIO-CRYPTIC SECURITY AWARE PACKET SCHEDULING (DCBSPS)

3.1 Assumptions and Notations

The DCBSPS were assumed with the limited five numbers of SL. A few packet models like Request IP Address packet (RIA) and Response authentication status (RsAS) are inherited from the DBSPS method. It is also presumed that Guarantee Ratio (GR), Dead Lines (DL), Network Delay (ND) is assumed with the Random Probability Distribution (RPD). Feature extraction is not applicable to face image, because the pattern recognition is not possible, if we perform for face.

3.2 The Prototype of Packet

The packets that were adopted contains the bio-cryptic payloads, temporary bits and IP address. The maximum size of the authentication packet is 16 octets (65Kb). The newly designed request and response packets of DCBSPS are as follows:

- Response Double bio-Chaos Authentication Packet (RsDCA)
- Request Double bio-Chaos Authentication Packets (RqDCA)

3.2.1 Response Double bio-Chaos Authentication (RsDCA)

The response authentication consists of only two fields in the packet. Those are SL and Source WN IP address. Where as SL varies from WN to WN based on WN IP and ranges from 1 to 5. The packet is designated as (SL, WNIP).

3.2.2 Request Double bio-Chaos Authentication (RqDCA)

The RsDCA packet servers between Advanced Radius Authentication Server (ARAS) and Source Wireless Node (WN) to gain access of the network switch. The RsDCA can be classified into five types. They are:

- RqDCA1 tuple comprises set of three fields (1, cryptic-text Password, ARASIP). 1 specifies security level 1 and cryptic password.
- RqDCA2 contains certain of four attributes (2, cryptic-text Password, Double Chaos Thumbprint, ARASIP). 2 specifies security level 2, cryptic password and Henon-Logistic-Chaos based bio-cryptic thumb-print.
- RqDCA3 engross firm of five attributes (3, cryptic-text Password, Double Chaos-Thumbprint, Double Chaos-Iris, ARASIP). 3 specifies security level 3, cryptic password, Henon-Logistic-Chaos based bio-cryptic thumb-print, Henon-Logistic-Chaos based bio-cryptic Iris.
- RqDCA4 has six attributes (4, cryptic-text Password, Double Chaos-Thumbprint, Double Chaos-Iris, Double Chaos-Palm-print, ARASIP). 4 specifies security level 4, cryptic password, Henon-Logistic-Chaos based bio-cryptic thumb-print, Henon-Logistic-Chaos based bio-cryptic Iris and Logistic-Chaos based bio-cryptic Palm-print.
- RqDCA5 encompasses with seven attributes (5, cryptic-text Password, Double Chaos-Thumbprint, Double Chaos-Iris, Double Chaos-Palm-print, Double Chaos-face, ARASIP). 4 specifies security level 4, cryptic password, Henon-Logistic-Chaos based bio-cryptic thumb-print, Henon-Logistic-Chaos based bio-cryptic Iris, Henon-Logistic-Chaos based bio-cryptic Palm-print and Henon-Logistic-Chaos based bio-cryptic face.

3.3 The Double chaos based Bio-cryptic (DcBc) Algorithm

Step1: Read the Biometric sample image from human to SWN.

Step2: Apply the Canny edge detection on Biometric samples and extract the features and edges and save image as I1.

Step 2: Encrypt the I1 Biometric images using Henon Chaos based algorithm using and save the image as I2.

Step3: Read the I2 image, apply 2D Logistic Image encryption, and save it I3. Include the outcome I3 image into RqDCA packet. ELSE, GOTO Step1.

3.4 The DCBSPS Algorithm

The DCBSPS algorithm is a combination of DcBc and EBSPS algorithms. The algorithm can be described in the following steps. Step 1: the node i sends RqIA containing the IP address (IPi), requesting access to the network to ARSA (Advanced Radius Server Authentication). Step 2: ARSA selects a suitable security level and replies by RsDCP containing information about designated security level (SLi) and requesting for authentication data. Step 3: The user's system on receiving RsDCP generates the respective RqDCA (1/2/3/4/5) packets for designated security level containing the required authentication data. The RqDCA packets were incorporated with DcBc algorithm. These RqDCA packets are sent back to the network for the authentication. Step4: The ARAS receives RqDCA packets and verifies the credentials and issues RsAS packets accordingly. Step5: IF RsASG, GOTO step 7 else GOTO step6. Step6 : User asked to re-sent

of the credentials Step7: The rest of the algorithm follows the BSPS algorithm steps (From Step7 to 15). Step8: Stop.

4. SIMULATIONS AND OUTCOMES

4.1 Simulation of DcBc Algotihm

Majorly the functional DcBc can be classified into Edge detection, 2D Henon Map and 2D Logistic map. More than 38 Biometric samples are used for the testing of the DcBc Algorithm and tested successfully.

4.1.1 Simulation of Canny Edge detection on Biometric Templates

The simulation of Biometric templates was carried out using the Matlab software, predefined edge(fin_his_eq,'canny'); function is used for the Minutiae feature extraction. The simulation results were discussed in the figure 3.

4.1.2 Simulation of 2D Henon Chaotic Map Biometric Encryption

The edge detected algorithm is subject to the Henon map encryption. The Henon Chaotic Map encryption contains majorly three functions Hudengen(), Keygen() and Henon(). These methods are successfully implemented in Matlab software with 128-bit key. The simulation results are discussed and outcomes shown in figure 3.

4.1.3 Simulation of 2D Logistic Chaotic Map Biometric Encryption

The Henon Bio-cryptic images are once again undergoes for the encryption with the 2D Logistic encryption can be performed by the Logistic2D-image-cipher(), Logistic-MDS(), Logistic-Permutations() and Logistic-Substitutions(). Figure 3 explains the complete procedure of DcBc procedure.

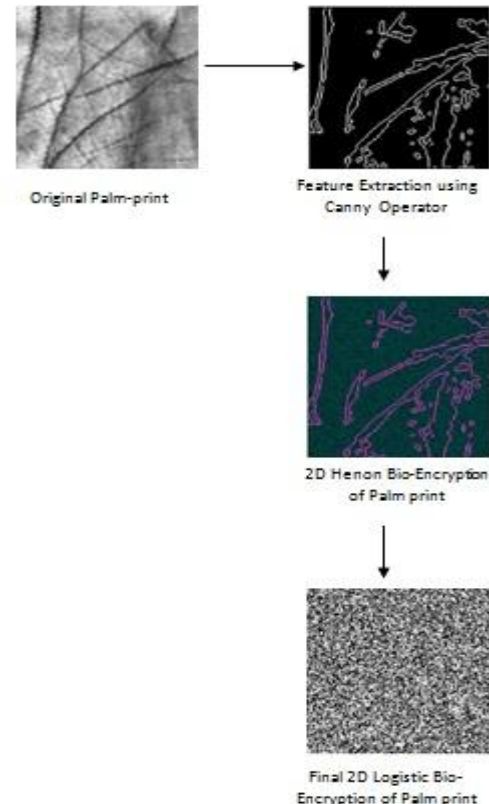


Fig 3: Simulation of DcBc algorithm in Matlab

Table 1. Complete simulation of DcBc Procedure


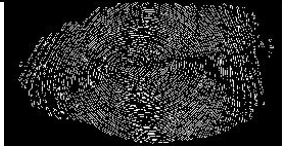
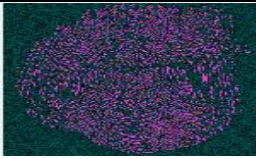
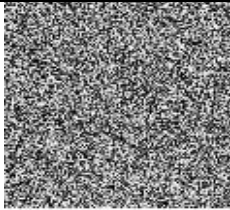
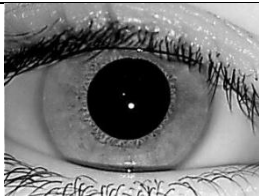
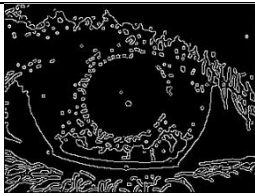
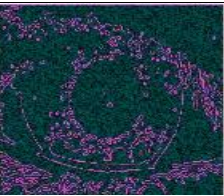
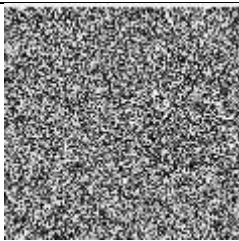


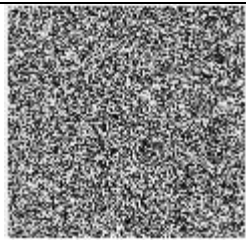
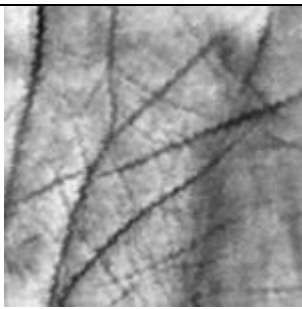


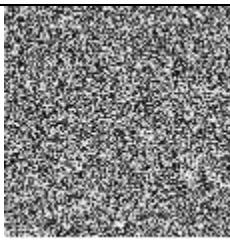
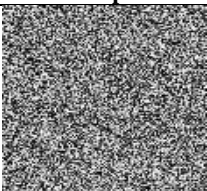
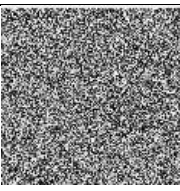
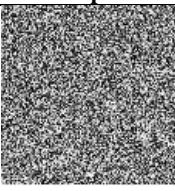
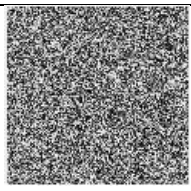
Original Template	Edge detection	Henon Bio-cryptic map	Logistic Bio-cryptic map
			
			
	NOT Applicable		
			

Table2: Result of Complete DCBSPS at Security Level 5

Security Level	Cryptic - Password	Double Chaos-Thumbprint	Double Chaos-Iris	Double Chaos-Palm-print	Double Chaos-face	ARASIP
5	S@W#C\$E% T					128.255.25.4 1

4.2 Simulation of DCBSPS Algorithm

The complete simulation was done using the Matlab software, where all 32 various combination of face, iris, palm-print and thumb-print biometric templates. Figure 4 shows the RqDCA5 packet outcome, where the double encrypted format is applied on the every biometric template. Table 1 and Table 2 shows the complete procedure of the DCBSPS

approach and its outcomes. All the test samples were tested successfully and it also observed that, the henon and logistic combinations are good standard map. The database was collected from the popular Biometric research laboratories [18][19][20][21].

4.3 Impact on Security Levels

The performance evaluation of the DCBSPS and CBSPS were evaluated based on the SL. It is observed that, that the SL are limited to 3 in CBSPS and whereas in DCBSPS is 5. Also it is DCBSPS is more stronger than CBSPS due to double encryption. Figure 4 shows the graphical representation of the results.

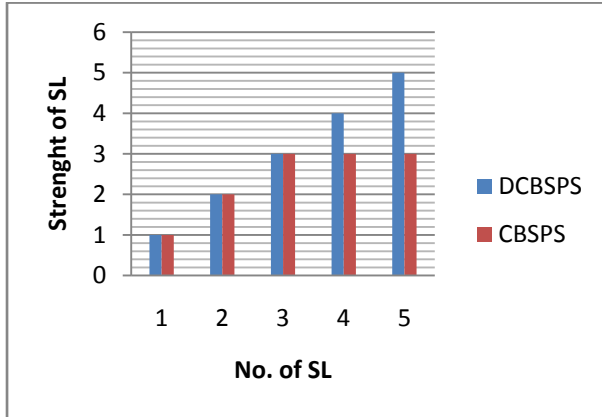


Fig 4: SL comparison between DCBSPS and CBSPS algorithms

4.4 Impact on Overall Performance

The Overall Performance (OP) is designated in the following equation 2.

$$OP = \text{Henon}(x_i, y_i) + \text{Logistic}(x_i, y_i) - ET + (SL * GR) + LNS \quad \text{----- (2)}$$

Where $\text{Henon}(x_i, y_i)$ and $\text{Logistic}(x_i, y_i)$ is the encryption time of the biometric sample using Henon and Logistic map. ET is the total encryption time, SL is security level, GR is the gurantee ratio and LNS is the Load on netwro switch. The OP of DCBSPS is good when compared with the CBSPS

5. CONCLUSIONS AND FUTURE SCOPE

Security is vital parameters that make WLAN into a reliable network. Without reliability, none of the product is worthful. In this paper, a novel DCBSPS algorithm is proposed to enhance the securty in the WLAN. The DCBSPS uses double cryptic technique with the help of logistic and henon chaotic maps. Literature proves that the Chaos map encryption is stronger encryption than Public key cryptography like RSA and ECC. The DCBSPS used 5 SL's for strenthenting the authentication process. The results of DCBSPS are better than CBSPS in terms of SL and its OP. In future the 2D Chaotic map encryption can be replaced with 3D Chaotic maps for the stronger SL in wireless networks

6. REFERENCES

- [1] http://www.ti.com/ww/en/internet_of_things/iot-applications.html (Accessed on 06/06/2015)
- [2] Hiltunen, Kimmo. "WLAN attacks and risks." White Paper, Ericson (2008).
- [3] https://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2015_ASR.pdf (Accessed on 08/07/2015)
- [4] Xi, Kai, and Jiankun Hu. "Bio-cryptography." In Handbook of Information and Communication Security, pp. 129-157. Springer Berlin Heidelberg, 2010.
- [5] Xiao Qin, et, "Improving Security of Real-Time Wireless Networks Through Packet Scheduling," IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, VOL. 7, NO. 9, pp.3273-3279, September 2008.
- [6] Rajesh Duvvuru, Sunil Kumar Singh, G. Narasimha Rao, Ashok Kote, B.Bala Krishna and M. Vijaya Raju, "Scheme for Assigning Security Automatically for Real-Time Wireless Nodes via ARSA," In Proc. Of QSHINE 2013, LNICST 115, Springer, pp. 185-196, January, 2013.
- [7] Duvvuru, Rajesh, P. Jagadeeswara Rao, and Sunil Kumar Singh. "Improving Security levels in WLAN via Novel BSPS." Emerging Trends in Communication, Control, Signal Processing & Computing Applications (C2SPCA), 2013 International Conference on. IEEE, 2013.
- [8] Duvvuru, Rajesh, et al. "Enhanced Security levels of BSPS in WLAN." International Journal of Computer Applications 84.2 (2013): 33-39.
- [9] Ramesh, Avala, and S. Pallam Setty. "Enhanced Merged Security Levels of BSPS in WLAN." International Journal of Computer Applications 88.7 (2014): 26-34.
- [10] Ramesh, Avala Ramesh and S. Pallam Setty. "Enhanced Authntication Mechanism in WLAN via MMBSPS", In IJMER, Special edition , April 2014.
- [11] Kumar, Sanjay. "Enhancing the Security Levels in WLAN via Novel IBSPS." Advanced Computing, Networking and Informatics-Volume 2. Springer International Publishing, 2014. 351-359.
- [12] Godi, Sudhakar. "Improved Security Levels of Wireless LAN through DBSPS." International Journal of Computer Applications 106.14 (2014).
- [13] Gedddada, Uma Devi, and Kaligithi Rajesh Kumar. "MMBWPS FOR STRENGTHENING AUTHENTICATION PROCESS IN WIRELESS LOCAL AREA NETWORKS." International Journal of Computer Engineering and Applications, Volume VIII, Issue I, Part I, 174-184, October 14.
- [14] Sanjay Kumar and D K Shaw. " Chaos based Encryption Mechanism for Wireless Local Area Network Authentication." International Journal of Applied Engineering Research 10.15 (2015): 35145-35152.
- [15] Duvvuru, Rajesh, P. Jagadeeswara Rao, and Gudikandhula Narasimha Rao. "Multi-Level Chaos Based Encryption Mechanism to Enhance Security of High Security Zone Areas on Google Map Satellite Images of India." International Journal of Applied Engineering Research 10.3 (2015): 8059-8072.
- [16] Wei-bin, Chen, and Zhang Xin. "Image encryption algorithm based on Henon chaotic system." In Image Analysis and Signal Processing, 2009. IASP 2009. International Conference on, pp. 94-97. IEEE, 2009.
- [17] Wu, Yue, Gelan Yang, Huixia Jin, and Joseph P. Noonan. "Image encryption using the two-dimensional logistic chaotic map." Journal of Electronic Imaging 21, no. 1 (2012): 013014-1.

- [18] Ajay Kumar, "Incorporating Cohort Information for Reliable Palmprint Authentication," Proc. ICVGIP, Bhubneshwar, India, pp. 583-590, Dec. 2008
- [19] Ajay Kumar, Sumit Shekhar, "Personal Identification using Rank-level Fusion," IEEE Trans. Systems, Man, and Cybernetics: Part C, pp. 743-752, vol. 41, no. 5, Sep. 2011.
- [20] D. Yadav, N. Kohli, R. Singh, and M. Vatsa, Revisiting Iris Recognition with Color CosmeticContact Lenses, 6th IAPR International Conference on Biometrics, June, 2013.
- [21] A. Sankaran, M. Vatsa, and R. Singh, Hierarchical Fusion for Matching Simultaneous Latent Fingerprint, In Proceedings of International Conference on Biometrics: Theory, Applications and Systems, 2012.