International Journal of Wireless Communications and Mobile Computing
2017; 5(1): 1-5
http://www.sciencepublishinggroup.com/j/wcmc
doi: 10.11648/j.wcmc.20170501.11
ISSN: 2330-1007 (Print); ISSN: 2330-1015 (Online)

Enhancing Security of Networks Through a Novel Biometric Signature Based Approach

Sherin Zafar

Faculty of Engineering, Jamia Hamdard University, New Delhi, India

Email address:
Sherin_zafar84@yahoo.com

To cite this article:
Sherin Zafar. Enhancing Security of Networks Through a Novel Biometric Signature Based Approach. *International Journal of Wireless Communications and Mobile Computing*. Vol. 5, No. 1, 2017, pp. 1-5. doi: 10.11648/j.wcmc.20170501.11

Received: October 20, 2016; **Accepted**: February 9, 2017; **Published**: March 4, 2017

Abstract: This paper focuses on a biometric signature based system as a novel tool for enhancing security in networks. The novel authentication approach takes into consideration a standardized database for analysis. Biometric perception is considered to be the most neoteric technology for sustaining security in various systems by involving exclusive identification features. The attainment of biometric perception depends upon image procurement and biometric perception system. This proffered algorithm focuses on attaining image procurement as well as biometric perception by an effective exploitation of bi-orthogonal wavelets for encoding biometric information. The biometric system is enhanced by incorporating cryptographic features which results in better solution against various security breaches.

Keywords: Biometrics, Iris Perception and Authentication Approach, Specificity and Sensitivity Analysis

1. Introduction

Various intrinsic vulnerabilities are present in different networks making security as the most basic and preeminent specification for users who desire number of services like, authentication, integrity, non-repudiation, confidentiality, key and trust management and access control for performing protected peer-to-peer communication over multi-hop wireless channel. Therefore, security is the most critical issue that require immediate research attention due to the dynamic and unpredictable nature of most networks and also as they diversify from each other enormously from the perspective of application area.

Security solutions exploited by most of the conventional approaches include simple encryption, username-password authentication on one hand and cryptography that imply a strong demand for secure and decisive key management structure on the other hand.

Also, there is a requirement of a proper authentication mechanism that should restrict the entree of the foreign nodes into the network. Security mechanisms are indispensible for various networks as they are inherently vulnerable to attacks hence, posing both challenges and opportunities for future research analysis and design. Therefore, this research study focuses on one of the most unique, popular and considered to be the most enhanced security solution for various networks and devices, referred as biometrics. The study of the physical and behavioral characteristics of human beings for the purpose of authentication is referred as biometrics. Depending upon the sort of typical behavior of a user the behavioral modalities make an attempt to identify the user, for e.g. how a person walks, how holds a pen, how presses the key when enter Personal Identification Number (PIN), etc. Physiological methods on the other hand identify physical traits namely; fingerprint, face-iris, retina, etc., typical to a particular user. Two categories are stated by biometric systems namely identification and verification. “Who you are” is specified by identification system while “Are you the one whom you claim to be” is specified by the verification system. From olden times biometric identification is applied. Thumb impressions, signature, photographs and identity cards are quite important for the verification of the identity of human beings. Automated biometric is the growing area of research of biometric technology. Face, fingerprint, voice, iris, speech, hand geometry, retina, etc., are some of the traits of human beings utilized by a biometric system. For various critical processes reliable personal recognition is quite important. Systems safeguarded for security and reliability, against criminal attacks are important in modern day world, that’s why

various public and private organizations have improved the traditional security systems with biometric systems.

Main aim of developing a secure biometric system is to enact identification based on who is the person rather, what are the possessions of system or what the person remembers (e.g. ID card or password).

For various networks, user authentication is quite critical for preventing various unauthorized users from causing modification of resources of the network. Due to the dynamic nature of such systems there is an extremely high chance of system being captured in a hostile environment therefore, there is frequent and continuous requirement of authentication.

Various validation factors namely, knowledge factors, possession factors and biometrics factors are exploited for performing user authentication. Passwords as knowledge factors and tokens as the possession factors are quite easy to be implemented but distinguishing an authenticated user from impostor becomes difficult since, no direct connection exist betwixt user and password or user or token.

The technology of biometrics deals with recognition of fingerprints, irises, faces, retina, etc., provides various possible solutions for the authentication problems that exist in different networks.

The prospective approach described in this paper is formulated under 5(five) main segments. Segment I, focuses on various vulnerabilities present in networks and how biometrics can be a fruitful secured solution. Segment II, outlays the novel crypt-iris based authentication approach. Segment III, describes specificity and sensitivity analysis results of proposed neoteric iris perception approach. Conclusion is outlaid in Segment IV. The paper is concluded by biography of author and various references.

2. Implementation of Novel Crypt-Iris Based Authentication Approach

The proposed neoteric "crypt-iris based perception and authentication approach" has been implemented in MATLAB to provide enhanced security solutions for various networks through biometrics and elliptic curve cryptography. It undergoes the various steps namely: Segmentation (Iris Segmentation/ Disjuncture), Normalization, Encoding (Template Formation or Encoding), Matching and Authentication. The basic operations of the proposed neoteric "crypt-iris based perception and authentication approach" are specified in figure. 1.

The proposed methodology attempts to achieve enhanced security solution utilizing iris templates which are generated from the individual eye image. These iris templates are utilized to generate the domain criterions of the elliptic curve and private keys. Iris is considered as one of the most decisive biometric feature which is chosen in the proposed methodology due to its exclusive signature. This signature is quite unlikely to be formed from another respective eye or even from other eye of the same person. Figure 2 shows the basic GUI for ECC embedded with iris perception algorithm.

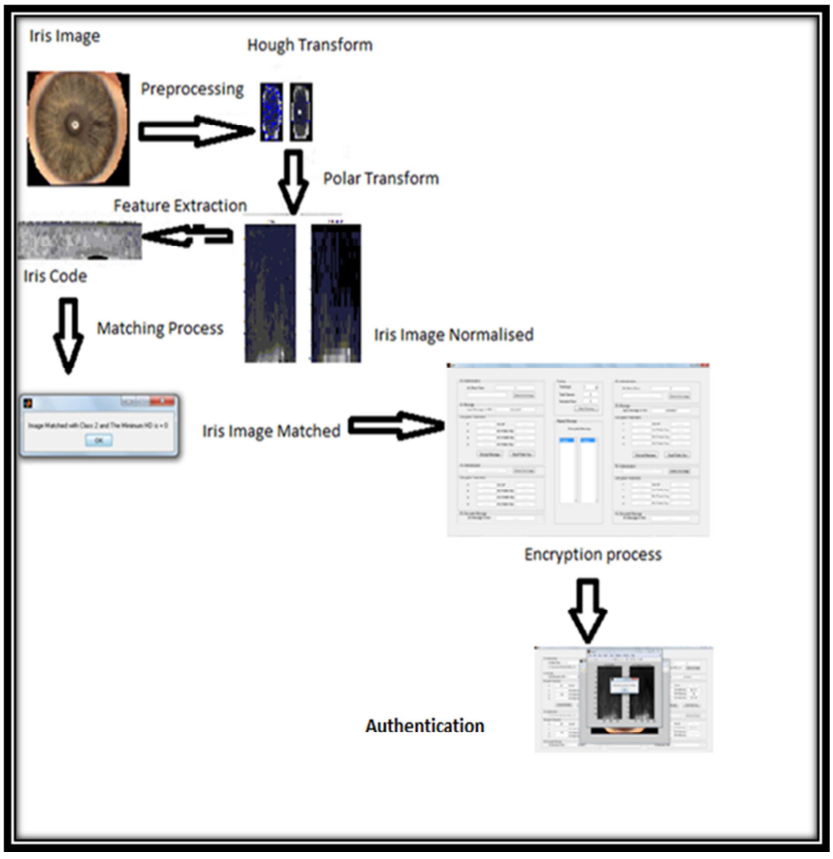

Figure 1. *Basic Operations of Neoteric Crypt-Iris Based Perception and Authentication Approach.*

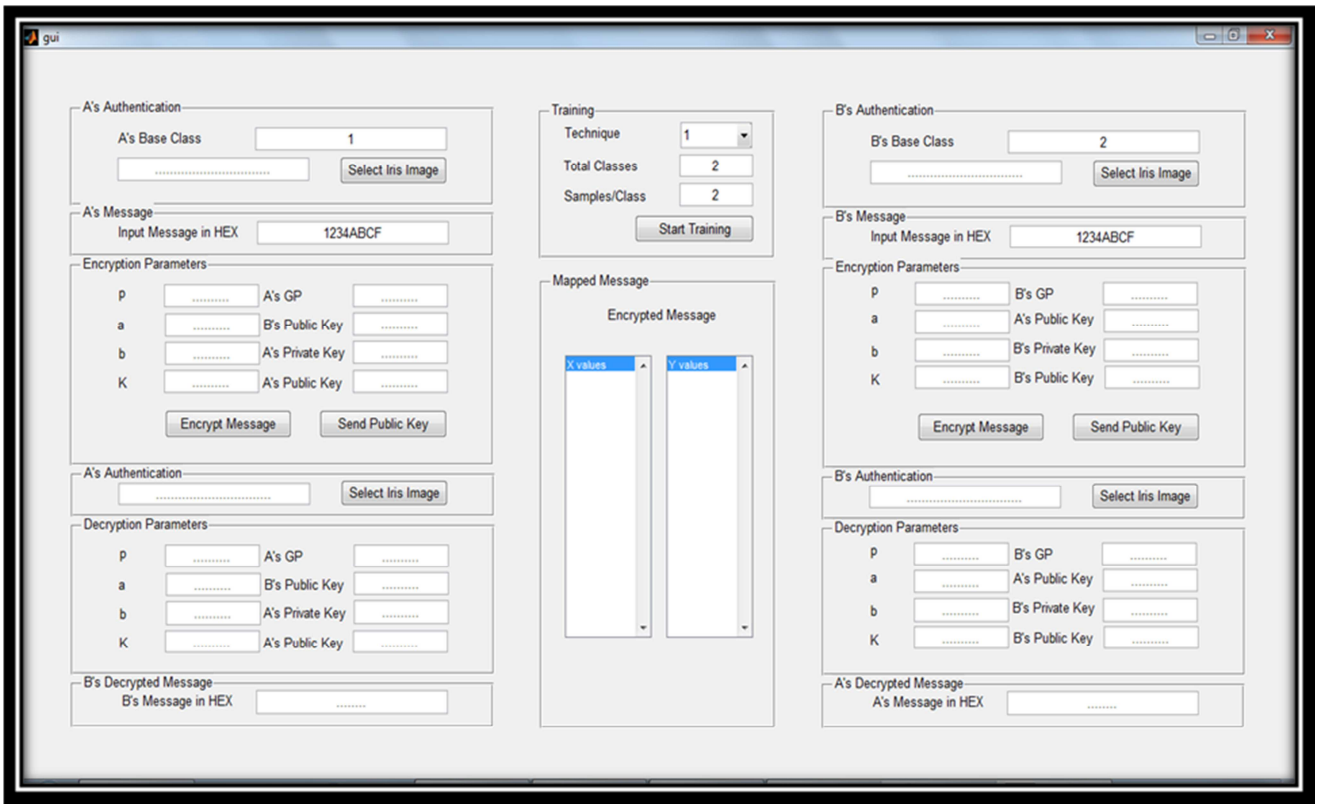

Figure 2. *Basic Graphical User Interface (GUI) for "Crypt-Iris Based Perception and Authentication Approach.*

Biometric provide number of advantages but some security and privacy apprehensions still can occur; biometric can be genuine but not necessarily private (secret). Eliminating or abolishing biometric is not possible. If once lost, they are exposed permanently and to apprehend humans cross-matching is employed barring their approval. Consequently, impinging the constraints of biometrics as discussed, iris templates generated through proposed neoteric iris perception methodology are taken to produce domains of elliptic curve cryptography for enhancing security in networks. The vulnerability of the devices having constraint resources increases as various networks suffers from attacks like DOS due to their wireless nature. Hence, for ensuring availability of nodes in networks implementation of threshold cryptography takes place. The intended receiver receives the actual message without having to compromise any of the security issue like confidentiality, integrity and authentication. Sharing of a key or splitting the message either before or after encryption by multiple individuals is performed by threshold cryptography. Avoidance of just one individual node for performing the job is done by TC with the main objective for sharing the authority in a way such that each individual node in the network performs computation on the secret message without revealing any secret information of its partial message. Threshold cryptography maintains a distributed architecture for a hostile environment by referring certain number of nodes as the threshold which are required for the encryption and decryption of the message, maintaining confidentiality and integrity against various malicious nodes. Verification of correct data sharing is achieved without revealing the secret key. So, in this research paper threshold cryptography is considered as a perfect solution for securing networks along-with neoteric CIB approach. Similar results are generated for B's authentication as produced. An authentication failure if user tries to access another image than the one utilized for encryption purpose. Hence, justifying the strong authenticated approach of the proposed methodology

3. Specificity and Sensitivity Analysis of Proposed Neotric Iris Perception Approach

Since, the paper deals with the biometric component iris, the validation of the proposed methodology cannot be completed without the analysis of the various specificity and sensitivity factors listed below:

Specificity and Sensitivity Analysis: It is defined as the classification function in statistics specified as statistical measures of the performance of a binary classification test which is specified through true positive rate (sensitivity) or recall rate, which is performed to analyze the proportion of actual positives in the given set of classifications and true recall rate, which is performed to analyze the proportion of actual positives in the given set of classifications and true negative rate (specificity) is performed to analyze the proportion of negatives.

Table 1. *Sensitivity and Specificity Analysis of Proposed Iris Perception Approach.*

S.No	Total Iris Classes	Images Per Class	Training Time (s)	Training Samples /Class	TPR	TNR	FPR	FNR	Precision	Accuracy	Recall	F-Measure
1.	3	1	7.332	1	1	1	0	0	1	1	1	1
2.	3	2	48.21	2	1	1	0	0	1	1	1	1
3.	3	3	60.7902	3	1	1	0	0	1	1	1	1
4.	5	1	12.0465	1	1	1	0	0	1	1	1	1
5.	5	2	23.8026	2	1	1	0	0	1	1	1	1
6.	5	3	35.7757	3	1	1	0	0	1	1	1	1
7.	10	1	23.8813	1	1	0.98765	0.012346	0	0.94444	0.98889	1	0.96296
8.	10	2	47.0779	2	1	0.98765	0.012346	0	0.94444	0.98889	1	0.96296
9.	10	3	67.3037	3	1	0.98765	0.012346	0	0.94444	0.98889	1	0.96296

Various formulae's stated for sensitivity and specificity analysis are, True Positive Rate (TPR) = TP/P, True Negative Rate (TNR) = TN/N, False Positive Rate (FPR) = FP/N, False Negative Rate (FNR) = FN/P, Accuracy = (TP + TN)/(P + N), Precision = (TP)/(TP + FP), Recall = (TP)/(TP + FN) and F-measure = 2*Precision*Recall/(Precision + Recall) where, True Positive (TP) = correctly identified, False Positive (FP) = incorrectly identified, True Negative (TN) = correctly rejected, False Negative (FN) = incorrectly rejected. The above equations signify that sensitivity is the proportion of true positives that are identified correctly by a diagnostic test and show how good the test is whereas specificity indicates the proportion of how correctly true negatives are reported by a test for identifying a normal(negative) condition. Accuracy is the proportion of various true results either true positive or true negative in a given set and measures the degree of veracity of a test. Higher the value of sensitivity, less likely a test returns false positive results. For e.g. sensitivity=99%, specify that a diagnostic test on a patient with a certain disease has a 99% chance that patient will be identified as positive. High sensitivity captures all possible positive conditions without missing anything. Specificity gives the representation that the probability of test diagnosis gives false positive results. Table 1. above shows the validity of CIB approach by taking into account sensitivity and specificity factors which are very important for justification of any biometric based approach. The results of the approach discussed in this paper shows various factor analysis like True Positive Rate, True Negative Rate, False Positive Rate, False Negative Rate, Precision, Recall, Accuracy and F-Measure with effective performance values. The results of the proposed approach performance factors are compared with the similar previous approaches validating the effectiveness of the proposed approach. Specificity and sensitivity factors analysis performance further validates the reliability of the proposed approach.

4. Conclusions

Secure Corroboration through CIB approach is effectively validated through the various simulation results diagrammatically discussed above as well as the combined simulation results presented through the table drawn above. Utilizing the concepts of cryptography through elliptic curve and biometric through strong iris specification proved to be a great security booster for the above approach. A two user authentication system for enhancing security of various networks is developed and implemented involving iris signature to generate domains of ECC and private key, providing two levels of security solutions. Authentication is provided as only authenticated nodes will be authorized for data transmission and communication along the network. No node will be able to pretend to be trusted therefore; data transfer will not be affected across the network. Neither sender nor receiver can deny the transmission of messages. Occurrence of various active and passive attacks will be limited in MANET being secured by the approach developed in this research study. No malicious node can affect the transmission of various services hence, DOS attack will be limited. No data packets could be updated, modified or altered without signature matching of the intended sender and receiver. A flexible simulation environment of the iris perception approach, allows varying of the iris classes as well as images per class, providing effective values for various specificity and sensitivity parameters like TPR, TNR, FPR, FNR, Precision, Accuracy, Recall and F-Measure. Time for training various iris classes is not very high even with increase in the number of iris classes and images per class. Approximately very accurate values of TPR=nearly 100%, TNR=nearly 100%, FPR=nearly 0%, Accuracy=100%, Recall=100% and F-Measure= Nearly 100% are achieved by the neotric iris perception approach. When compared with Masek (2003) work on iris recognition which achieved FNR and FPR (with different classes per samples) as 4.580 and 2.494 on LEI database and 5.181 and 7.599 on CASIA database, the proposed methodology serves as a neotric approach achieving required values of FNR=0 and FPR=0.012346 (many parameters included in the proposed methodology are not being specified by any of the conventional approaches) leading to enhanced security solution for MANET. Similarly, Abhyankar and Schuckers (2010) achieved values of FNR=0.00 and FPR=3.3 not better than the proposed approach. Also, Panganiban et al. (2011) have achieved accuracy of 94.5 in their developed iris recognition system, when compared with the proposed approach which achieved accuracy of 96.2.

References

[1] Abhyankar, A. and Schuckers, S., "Wavelet Based Iris Recognition for Robust Biometric System", *International Journal of Computer Theory and Engineering*, 2 (2). [Accessed April 2010].

[2] Boles, W. W. and Boashash, B., "A Human Identification Technique using Images of the Iris and Wavelet Transform", *IEEE Transactions on Signal Processing*, 46 (4), 1998.

[3] Daugman, J., "Biometric Personal Identification System Based on Iris Analysis", *United States Patent*, 5291560, 1994

[4] Haas, Z., Deng, B., Liang, P., Papadimitratos. and Sajama, S., "Wireless Ad-hoc Networks", *Journal of Proakis, In: Wiley Encyclopaedia of Telecommunications John Wiley and Sons,* 2002.

[5] Ma, L., Wang, Y. and Tan, T., "Iris Recognition using Circular Symmetric Filters", *National Laboratory of Pattern Recognition*, Institute of Automation, Chinese Academy of Sciences, 2002.

[6] Masek, L., "Recognition of Human Iris Patterns for Biometric Identification", *University of Western Australia*, 2003.

[7] Cheng, H., "Genetic Algorithms with Immigrants Schemes for Dynamic Multicast Problems in Mobile Ad-hoc Networks", *Engineering Applications of Artificial Intelligence Elsevier*, 806-819, 2010.

[8] Panganiban, A., Linsangan, N. and Caluyo, F., "Wavelet-Based Feature Extraction Algorithm for an Iris Recognition System". *Journal of Information Processing Systems*, 7 (3), Accessed September 2011.

[9] Reddy, T. B., Karthigeyan, B. S., Manoj. and Murthy, C. S. R., "Quality of Service Provisioning in Ad-hoc Wireless Networks: A Survey of Issues and Solutions", *Elsevier Transactions on Ad-hoc Networks*, 83-124, Accessed June 2004.

[10] Ritter, N., "Location of the Pupil-Iris Border in Slit-Lamp Images of the Cornea" *In: Proceedings of the International Conference on Image Analysis and Processing*. *IEEE International Symposium on Signal Processing and Information Technology*, 1999.

[11] Wildes, R., "Iris Recognition: An Emerging Biometric Technology" *In: Proceedings of the IEEE,* 85 (9), 1997.

[12] Wildes, R. P., Asmuth, J. C., Green, G. L. and Hsu, H. C., "A System for Automated Iris Recognition" *In: Proceedings IEEE Workshop on Applications of Computer Vision,* 121-128, 1994.

[13] Zafar Sherin, Soni. M. K., Beg M. M. S "An Optimized Genetic Stowed Biometric Approach to Potent QOS in MANET" Procedia Computer Science Volume 62, 2015, Pages 410–418 (Elsevier) Proceedings of the 2015 *International Conference on Soft Computing and Software Engineering (SCSE'15).*

[14] Zafar Sherin, Soni. M. K. "Biometric Stationed Authentication Protocol (BSAP) Inculcating Meta-Heuristic Genetic Algorithm". *I. J. Modern Education and Computer Science,* 28-35, 2014.

[15] Zafar Sherin, Soni. M. K. "A Novel Crypt-Biometric Perception Algorithm to Protract Security in MANET" *I. J. Computer Network and Information Security,* 64-71, 2014.

[16] Zafar Sherin, Soni. M. K. "Secure Routing in MANET through Crypt-Biometric Technique", *Proceedings of the 3rd International Conference on Frontiers of Intelligent Computing: Theory and Applications (FICTA)*,713-720, 2014.

[17] Zafar Sherin, Soni. M. K., Beg M. M. S "QOS Optimization in Networks through Meta-heuristic Quartered Genetic Approach" *ICSCTI*, IEEE, 2015.

Biography

Dr. Sherin Zafar has PhD degree in Computer Engineering from Manav Rachna International University Faridabad in 2015. She is now Assistant Professor in Faculty of Engineering, Jamia Hamdard University, New Delhi. She has 10 years of teaching experience, with around 20 published papers in IEEE, Springer and Elsevier. She is an editor and reviewer of some important journals and conferences. In teaching, she has been focusing on Computer networks, Big Data Analytics, Network Security, DBMS etc. Her research interests include ad-hoc networks, meta-heuristic algorithms and network security.