Iris Signature Methodology for Securing MANET

Sherin Zafar
Asstt. Professor,
Faculty of Engineering,
Jamia Hamdard University,
New Delhi, India
E-mail: sherin_zafar84@yahoo.com

M.K. Soni
Professor & Dean,
Faculty of Engineering,
MRIU, Faridabad INDIA
E-mail: ed.fet@mriu.edu.in

M.M.S. Beg
Principal,
Zakir Hussain College of Engineering,
Aligarh Muslim University,
U.P. India
E-mail: mmsbeg@hotmail.com

Abstract: This paper presents a novel Iris Signature Methodology (ISM) to utilizing iris as a biometric mechanism along with elliptic curve cryptography to procure security in networks. The ISM approach is developed in MATLAB that takes into consideration a standardized database for analysis. Biometric percipience is contemplated to be the most neoteric technology for sustaining security in various vulnerable networks like mobile ad-hoc networks (MANET) by implicating exclusive identification features through attainment of biometric perception that depends upon image procurement (IP) and biometric perception system (BPS). Security of MANET is considered as the most important task for better performance improvement hence along with strong biometric feature like iris further enhancement is done in the underlying approach by fabricating an iris signature utilizing features of elliptic curve cryptography. IP and BPS is attained by an effective exploitation of bi-orthogonal lazy wavelets to conceal biometric information.

Keywords: ISM; image procurement and biometric perception system; elliptic curve cryptography.

I. INTRODUCTION

In many whereabouts, a communication network is vital where there is no rooted infrastructure and neither there is time to create such a framework like military operations, law enforcement, rescue operations and personal area networking. A network developed in such situations where the nodes are mobile is called MANET or a network constituted vigorously from scratch employing and manipulating wireless connections and composed of mobile nodes is referred as mobile ad-hoc network. Since, the network is composed of mobile nodes it is referred as MANET. Content, pace of organization and less reliance on a permanent framework when grouped with conventional wireless networks are some of the unique features provided by MANET. Figure 1 shows a mobile ad-hoc network build ondemand without any infrastructure. Lim et al. (2001); Yanchao et al. (2007); have stated that MANET's other than standard data networks face various challenges due to their dynamic nature. Ad-hoc networks must be equipped with competence and fulfil various security goals, to emulate topology transitions, as they have continuous dynamic connectivity between their nodes.

Also, there is a requirement of a proper authentication mechanism that should restrict the entree

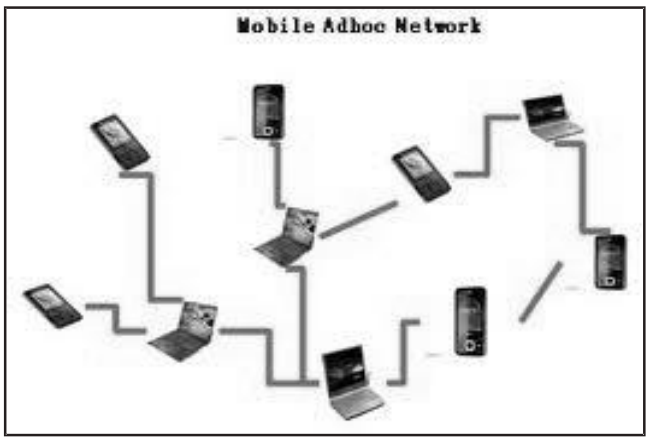

Fig. 1: Mobile Ad-hoc Network
http://virtual-labs.ac.in/cse28/ant/ant/7/theory/

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 MANET, referred as Iris Signature Methodology (ISM).The study of the physical and behavioral characteristics of human beings for the

purpose of authentication is referred as biometrics. Commonly exploited biometrics modalities are represented in Fig.2 which can be classified as behavioral or physical. 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.

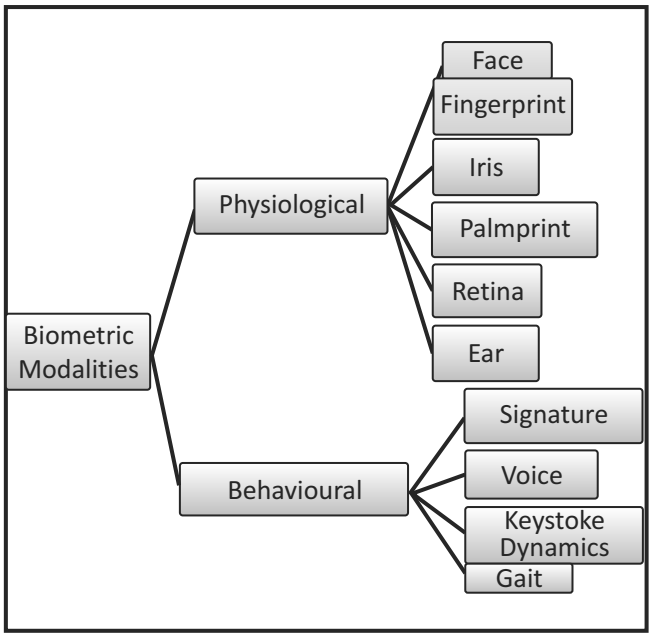

Fig. 2: Biometric Modalities

For MANET, user authentication is quite critical so as to prevent various unauthorized users from causing modification of the resources. 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.

II. IRIS SIGNATURE METHODOLOGY (ISM)

Boles and Boashash (1998); Daugman (1994); Ma et al. (2002); Wildes (1997); Wildes et al. (1994); have focussed that biometric identification is becoming quite a popular tool and gaining more acceptance in various sectors. One of the highly accurate and reliable methods to be considered for biometric identification is iris recognition as the iris is considered to be very stable, highly unique and easy to capture when compared with other biometric identifiers. For personal identification, image processing and signal processing the unique epigenetic patterns of a human iris are employed for extracting information which is encoded to formulate a "biometric template". This biometric template is stored in a database and also utilized for identification purposes. The proposed wavelet based ISM is developed for securing MANET which results in a highly secure environment.The proposed neoteric ISM has been implemented in MATLAB to provide enhanced security solutions for MANET through biometrics and elliptic curve cryptography (ECC). 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 "ISM" are specified in Fig. 3.

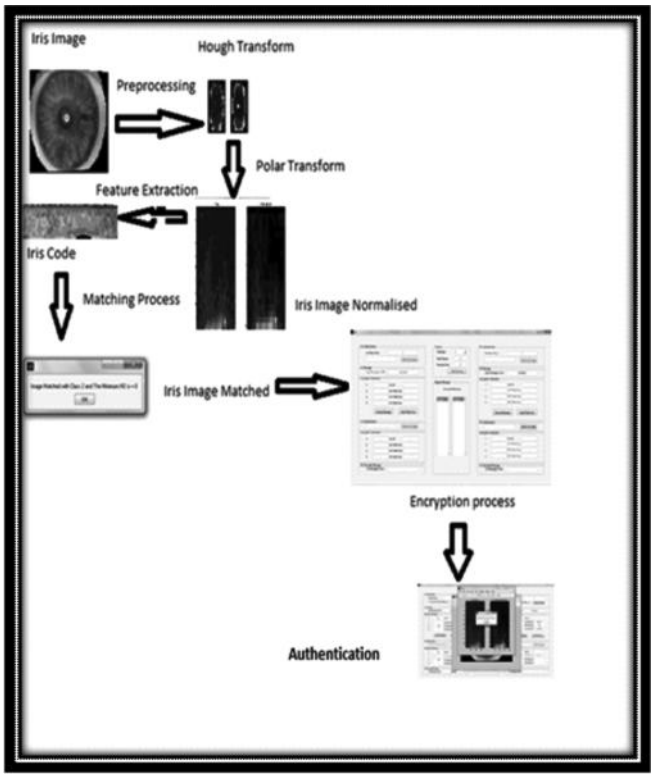

Fig. 3: Basic Operations of ISM

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.

Enhanced security solutions are achieved as only the respective eye produces the iris signature. The system design architectonics of ISM is shown in Fig.3. Calculation of various domain parameters of ECC along with the private keys which are generated through iris template is shown in Fig. 4 and Fig. 5. The most enhanced factor of the proposed methodology is that an individual produces a different private key each time during key regeneration.

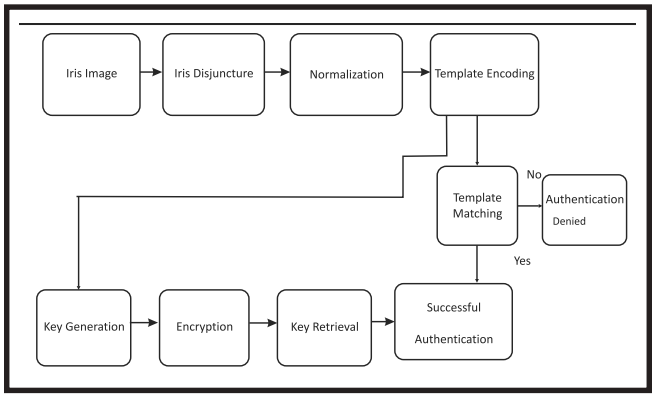

Fig. 4: System Design Architecture of ISM

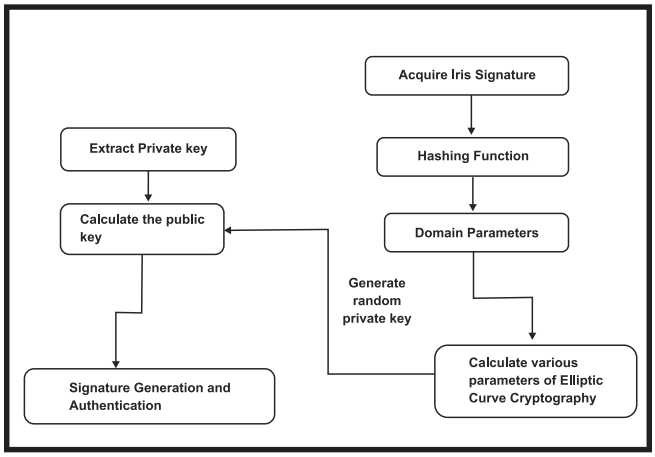

Fig. 5: System Design of ECC Generated Through Iris Signature

Iris signature is the main base for generating the domains of ECC and the private key. The following algorithm describes ISM:

1. Select image of individual eye from the database.
2. Perform iris perception algorithm as described in Fig.3 and Fig. 4 through the below described sub algorithm:

A. **Iris Segmentation/ Disjuncture:** A circular Hough transform is explored for detecting the iris and pupil boundaries which involves canny edge detection to generate an edge map. Linear Hough transform is considered moreadvantageous over its counterpart which is the parabolic version, as it has less parameter to deduce resulting in computationally less demanding process. The proposed methodology successfully carries out iris segmentation of all the images specified in the database, extracting the area of interest from the iris image and removing all the unwanted parts from it, resulting in an accurate input for the next stage of iris perception approach.

B. **Normalization:** Normalization is performed through histogram equalization method. When compared with the other methods of performing normalization available in literature, histogram equalization enhances the contrast of iris images by transforming the values in an intensity image so that the histogram of the output iris image approximately matches a specified histogram.This method usually increases the global contrastof iris images, especially when the usable dataof the image is represented by close contrast values.When compared with other conventional iris recognition algorithms, proposed normalization process is able to perfectly reconstruct the same pattern from images with varying amounts of pupil dilation, as deformation of the iris results in small changes of its surface patterns. Even in the images where pupil is smaller, the proposed normalization process is able to rescale the iris region to achieve constant dimension.The proposed methodology generates the rectangular representation from 10,000 data points in each iris region taking into account all the rotational inconsistencies (misalignment in the horizontal (angular) direction). Rotational inconsistencies will be accountedin the matching stage. The output of the previous segmentation

stage where area of interest was selected by a perfect Hough transform and canny edge detection provided the input for the normalization stage. Normalization if not perfectly done will lead to an inappropriate matching, that will not build a perfect security solution for MANET which is the key requirement of this research study.

C. **Template Formation or Encoding:** Template formation or encoding in the proposed methodology is performed through convolving the normalized iris pattern with bi-orthogonal wavelets 3.5. The 2D normalized pattern is broken up into 1D-signals. The angular direction is taken rather than the radial which corresponds to columns of the normalized pattern, as the maximum independence occurs in the angular direction. Transformation of the segmented iris information into a normalized iris data is done using the bi-orthogonal tap. In the proposed method rather than utilizing the traditional Multi-Resolution Analysis (MRA) scheme, a novel lifting technique is explored for the construction of bi-orthogonal filters. The main advantage of this scheme over the classical construction methods is that it does not rely on the Fourier transform and results in faster implementation of wavelet transform.Bi-orthogonal 3.5 tap is selected for encoding the iris information by adjusting the frequency content of the resulting coefficients to get a separated band structure. In the lifting scheme the filters are designed using the lifting steps as they are completely invertible. Transformation of the data into a different and new basis is performed by the filters, where large coefficients correspond to relevant image data and small coefficients corresponds to the noise. Thresh-holding is performed once again and referred as image de-noising. The data encoded by the wavelet is scalable and localized, making matching possible of the features at same location using various scales resulting in information of bit-stream of 1s and 0s referred as the "iris template". For performing comparison band pass Gabor pre-filtering is performed for encoding the information and generating the filter using Gaussian filters. Then utilizing this approximation for generating wavelet coefficients that are quadrature quantized, resulting in information of bit-stream of 1s and 0s. This is performed for all the iris images and the formulated bit-pattern is referred as the 'iris template' having angular resolution of 20, radial resolution of 200 and length as 8000 bits. The noisy parts of the image are located by the mask template that is formed along with the iris template.

D. **Matching Process:** Matching unlike other conventional eye recognition processes is not done by taking only one single matching criterion into consideration but in the proposed methodology matching is performed through two parameters. Hamming distance as well as normalized correlation coefficient is utilized as metrics for recognition since, bit-wise comparisons are necessary. Noise masking is incorporated by the Hamming distance algorithm so that only significant bits are used in calculating HD. Although in theory two iris templates generated from the same iris will have a Hamming distance of 0.0, in conventional methods this has not happened as normalization is not perfect and also there will be some noise that goes undetected, so some variation will be present when comparing two intra-class iris templates. But in this neoteric approach, normalization is perfectly done also encoding done through bi-orthogonal wavelets providing a bit stream away from noises. Hence, Minimum Hamming Distance=0 and Maximum Normalized Correlation Coefficient=1 both are achieved. Next matching parameter utilized is the Normalized Correlation (NC) betwixt the acquired and database representation for goodness of match.Normalized correlation is advantageous over standard correlation as it is able to account for local variations in image intensity that corrupts the standard correlation calculation. The proposed iris perception approach is able to achieve ideal value of matching i.e. Maximum Normalized Correlation = 1.

3. Iris signature obtained in step 2 is being hashed to generate domains and private key for ECC.

4. Authentication is then performed between two users.

III. RESULTS AND DISCUSSIONS

The above algorithm gives an individual variety of different private keys as every time a new key is

regenerated by user hence, enhancing authentication of iris perception approach, which is the chief security goal for various networks. Fig. 6 shows the basic GUI for ECC embedded with iris perception algorithm. Proposed approach of ECC utilizes iris signature generated by neoteric IPA (Fig.2) and produces a strong authentication system.Simulated through MATLAB the proposed methodology obtains various successful results, as shown in figs. 6-10 (A's authentication). Fig. 5 depicts the basic two user authentication system (A and B) utilizing iris templates for generating domain values of elliptic curve hence, resulting in a strong secure authentication system for various networks.

Similar results are generated for B's authentication as produced in Fig. 5-9 for A's authentication, followed by encryption and authentication as depicted in Fig.12-13. Fig.11depicts an authentication failure if user tries to access another image than the one utilized for encryption purpose, which justifies the strong authenticated approach of the proposed methodology.

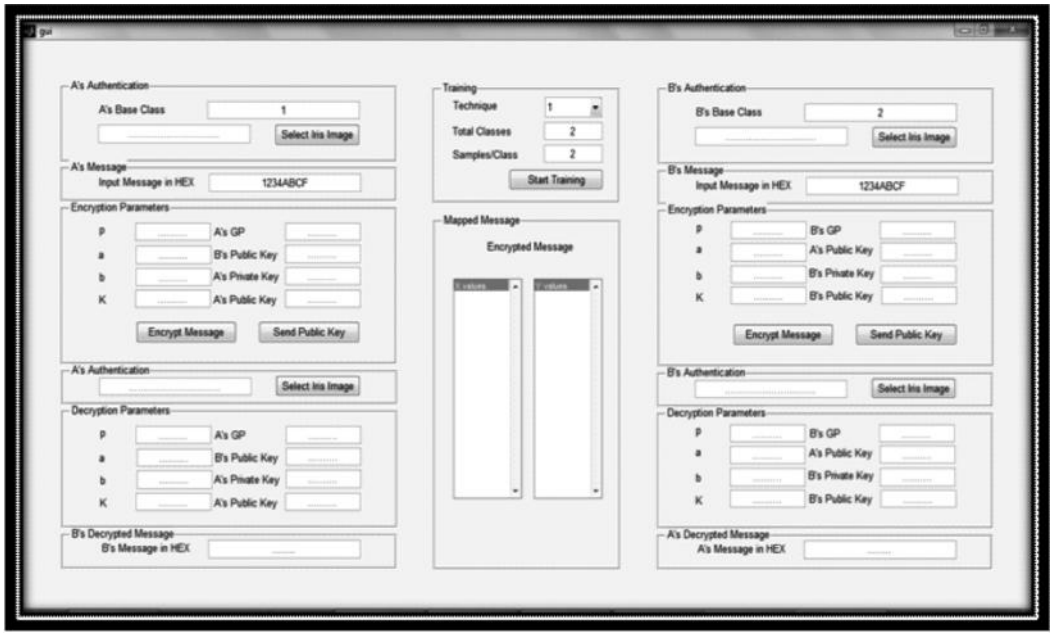

Fig. 6: Basic Graphical User Interface (GUI) for ISM

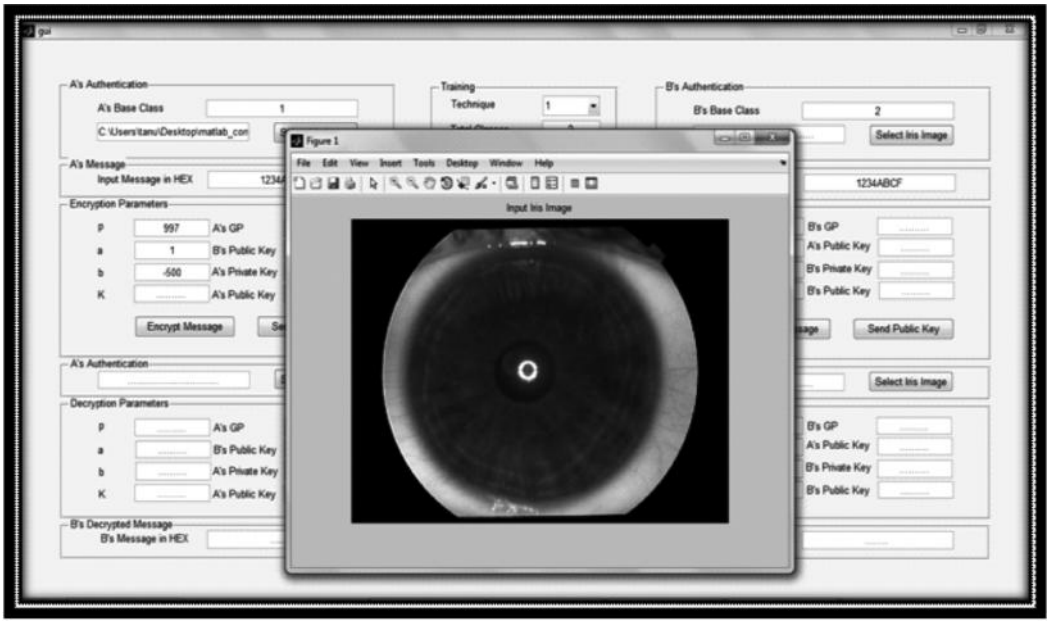

Fig. 7: Selection of Iris Image for A's Authentication

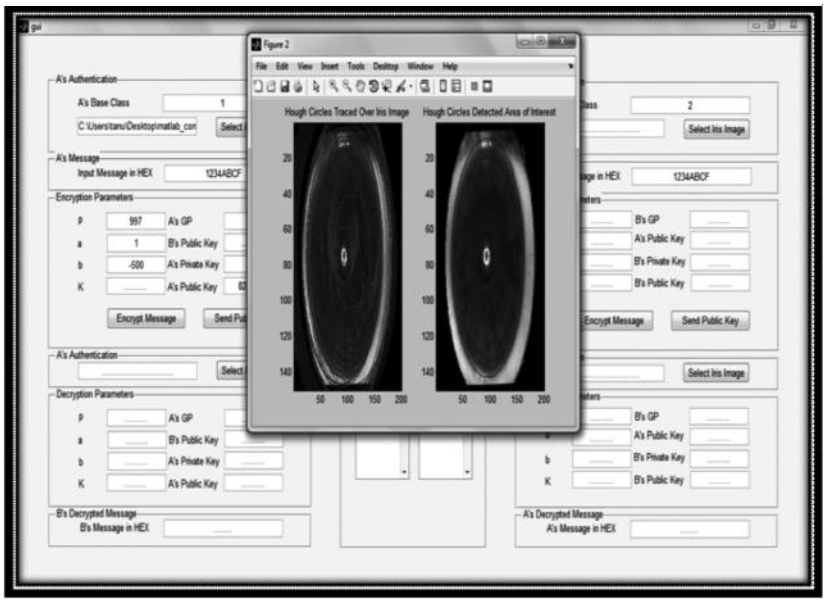

Fig. 8: Hough Circles Traced for Detecting Area of Interest of A's Iris Image

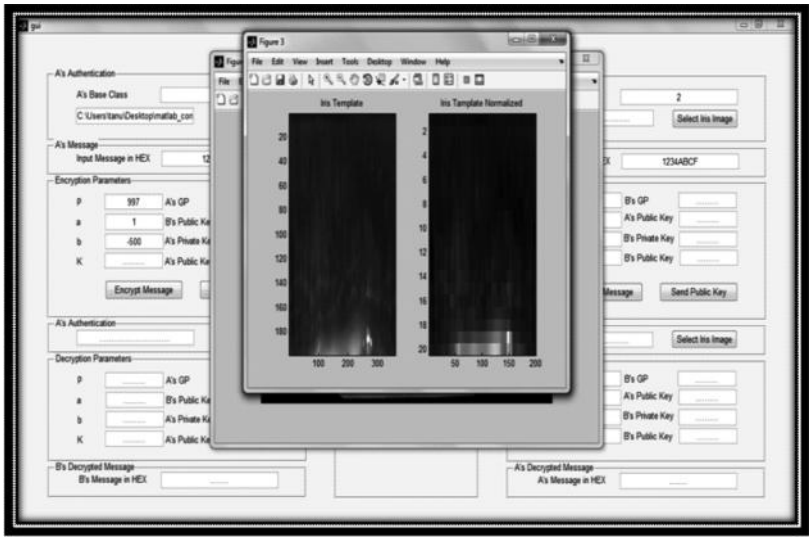

Fig. 9: Iris Template Generated and Normalized for A's Authentication

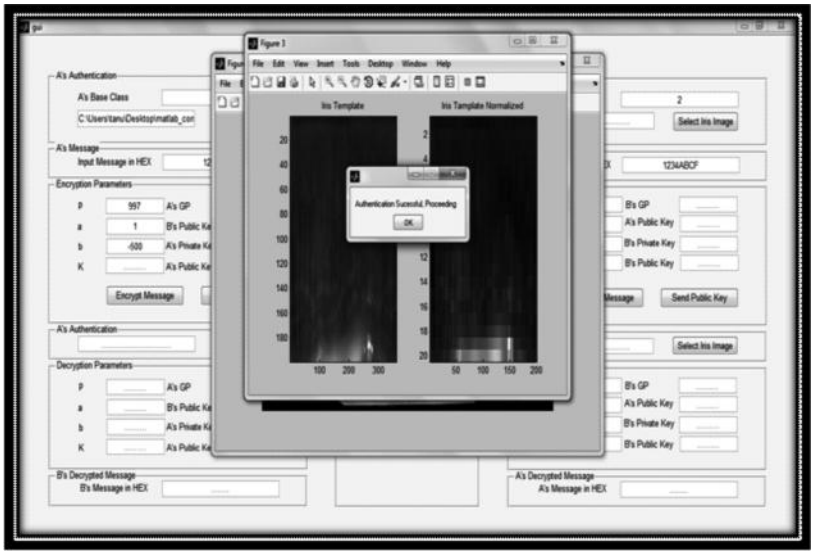

Fig. 10: Successful A's Authentication

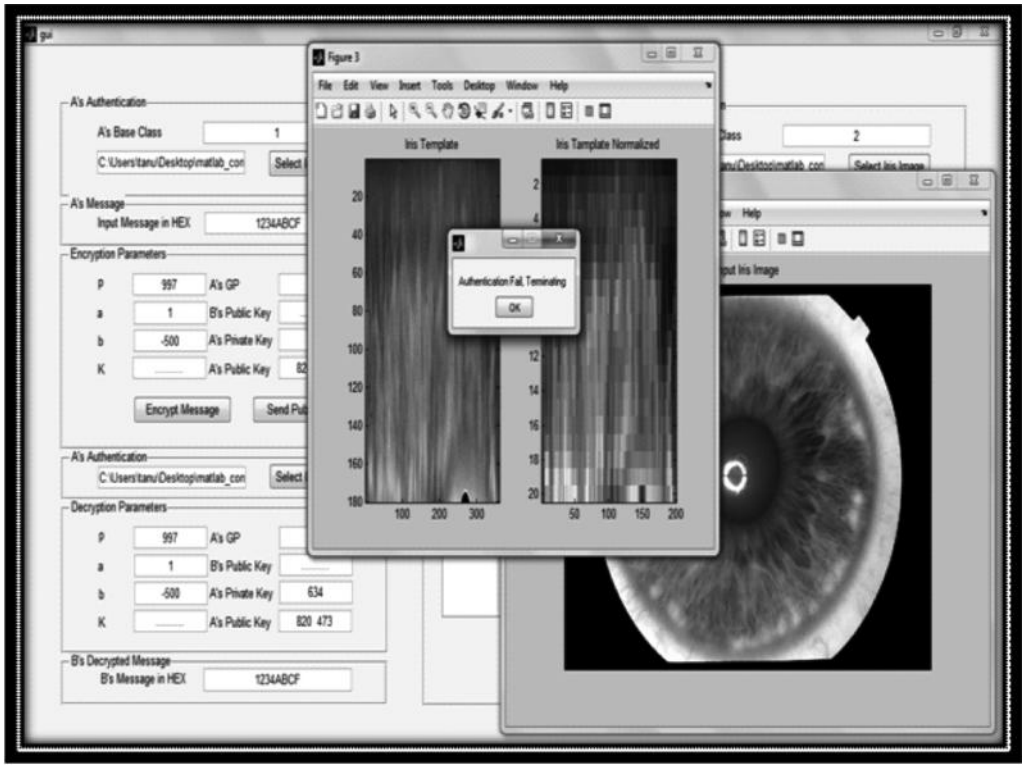

Fig. 11: Authentication Failed

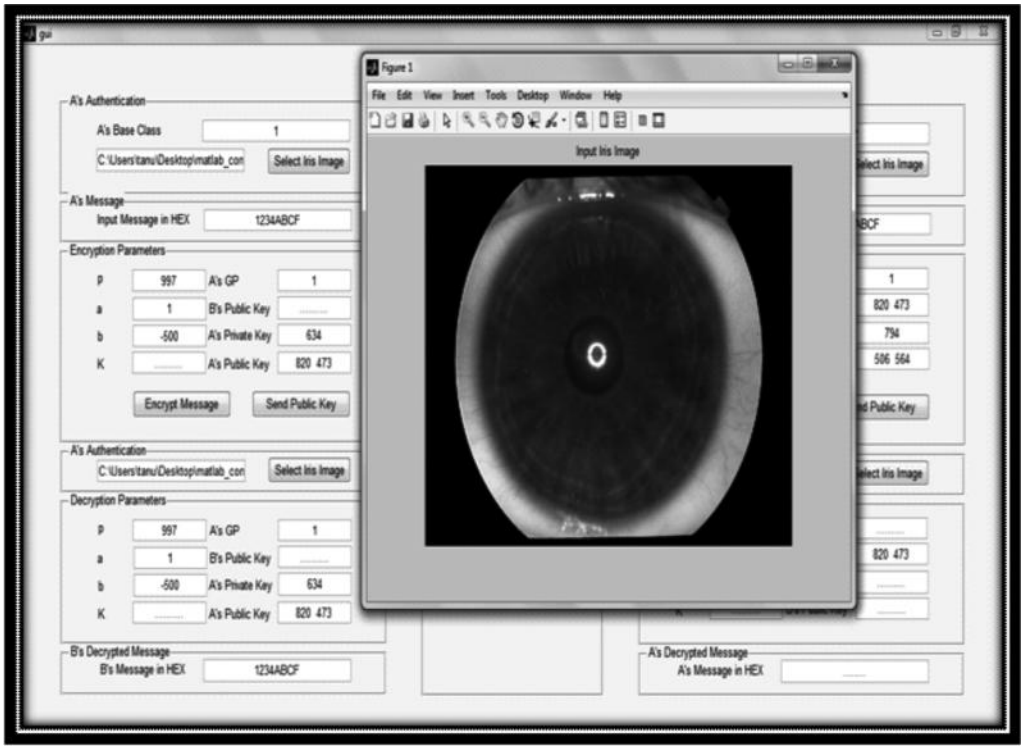

Fig. 12: Authentication with Iris Image at Receiver End

IV. CONCLUSIONS

The implementation of the neoteric "ISM" is performed in the previous sections and subsections. A two user authentication system for enhancing security of MANET 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 the nodes whose biometric templates achieves ideal matching conditions; minimum HD=0 and maximum NC=1 find an exact match in the database. Only those 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. By utilizing iris templates generated through proposed neoteric iris perception approach for producing domains of novel "crypt-iris based perception and authentication method", confidentiality is ensured. Sensitive information is accessible only to the intended sender and receiver whose signature will be authenticated by the proposed methodology. Integrity is also preserved in this approach as only those nodes whose biometric templates that achieve minimum HD=0 and maximum NC=1, will enter the network and no malicious node will be allowed entry in MANET. Hence, no data will be modified by malicious nodes. As signature of both sender and receiver are authenticated hence, non-repudiation security goal is also preserved. 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.

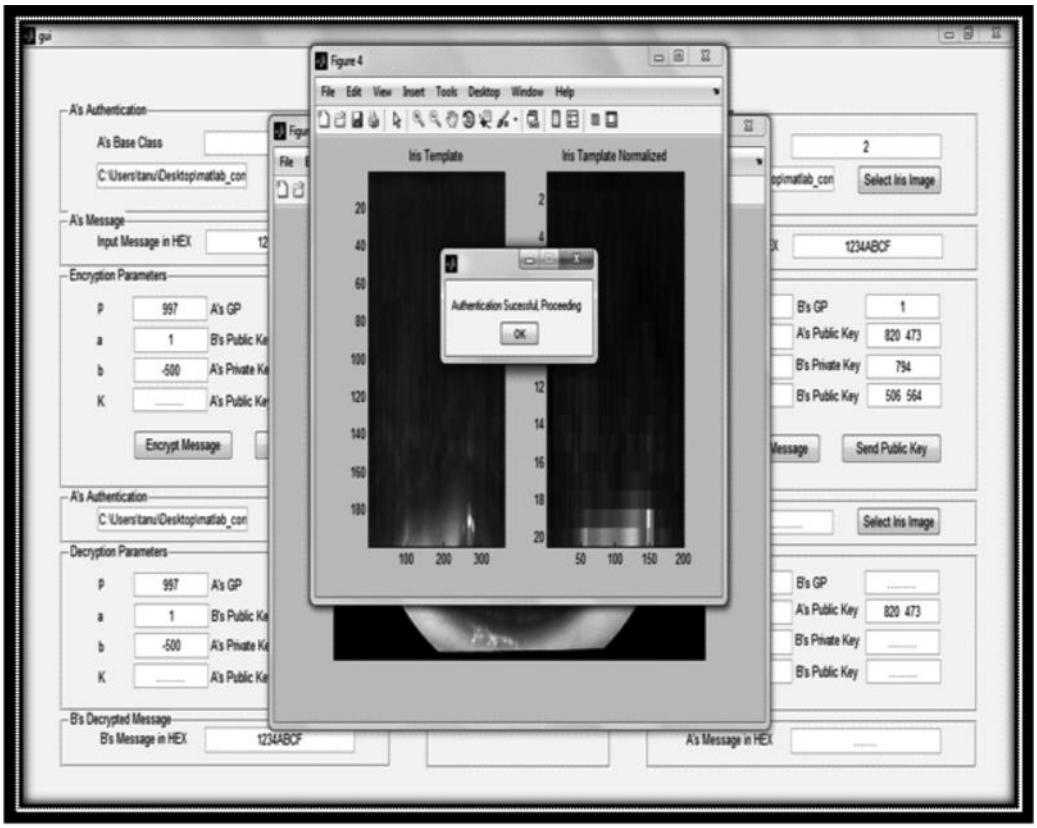

Fig. 13: Authentication Successful

REFERENCES

[1] Abhyankar, A. and Schuckers, S., 2010. 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., 1998. A Human Identification Technique using Images of the Iris and Wavelet Transform. *IEEE Transactions on Signal Processing*, 46 (4).

[3] Calderbank, A.R. Daubechies, I.,Sweldens, W. andYeoB.L., 1998. Wavelet Transforms that Map Integers to Integers. *Applied and Computation Harmonic Analysis* (3), 332-369.

[4] Daubechies, I. and Sweldens, W., 1998. Factoring Wavelet Transforms into Lifting Steps. *Journal of Fourier Analysis and Applications*, 4 (3), 245-267.

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

[6] Lim, S., Lee, K., Byeon, O. and Kim. T., 2001. Efficient Iris Recognition through Improvement of Feature Vector and Classifier. *ETRI Journal*, 23 (2).

[7] Lim, S., Yu, C. and Das, C., 2005. A Randomized Communication Scheme for Improving Energy Efficiency in Mobile Ad-hoc Networks. *Proceedings of 25th International Conference on Distributed Computing Systems (ICDCS)*, 123-132.

[8] Masek, L., 2003. Recognition of Human Iris Patterns for Biometric Identification. *University of Western Australia*. Cheng, H., 2010. Genetic Algorithms with Immigrants Schemes for Dynamic MulticastProblems in Mobile Ad-hoc Networks. *Engineering Applications of Artificial Intelligence Elsevier*, 806-819.

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

[10] Ritter, N., 1999. 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*.

[11] Struc,V., Gajsek,R. and Pavasic,N., 2009. Principal Gabor Filters for Face Recognition 3rd IEEE International Conference on Biometrics: Theory, Applications and Systems, 1-6. [Accessed September 2009].

[12] Sweldens, W., 1995. The Lifting Scheme: A New Philosophy in Bi-Orthogonal Wavelet Constructions. *Wavelet Applications in Signal and Image Processing III, SPIE 2569*, 68-79.

[13] Sweldens, W., 1997. The Lifting Scheme: A Construction of Second Generation Wavelets. *SIAM Journal of Math Analysis*, 29 (2), 511-546.

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

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

[16] Yanchao, Z., Wenjing, L., Wei, L. and Yuguang, F., 2007. A Secure Incentive Protocol for Mobile Ad-hoc Networks. *Conference on WINET*, 13 (5). [Accessed October 2007].

[17] Yang, H., Luo, H., Ye, F. and Lu, S., 2004. Security in Mobile Ad-Hoc Networks: Challenges and Solutions. *IEEE Transactions on Wireless Communications*, 98-102. [Accessed February 2004].

[18] Yen,Y.S. et al., 2008. A Genetic Algorithm for Energy-Efficient Based Multicast Routing on MANET. *Conference on Computer Communications*, 2632-2641.

[19] Yujun, L. and Lincheg, H., 2010. The Research on an AODV-BRL to Increase Reliability and Reduce Routing Overhead in MANET. *In: Proceedings of International Conference on Computer Application and System Modelling (ICCASM)*, 12, 512-530.[Accessed October 2010].

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

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

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

[23] Zafar Sherin, Soni.M.K. 2014. 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.

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

❐