I.J. Computer Network and Information Security, **2014, 12, 64-71**
Published Online November 2014 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2014.12.08

A Novel Crypt-Biometric Perception Algorithm to Protract Security in MANET

Sherin Zafar,
Faculty of Engineering, Manav Rachna International University Faridabad, Haryana, 121004, India
Email:Sherin_zafar84@yahoo.com, ed.fet@mriu.edu.in

Prof. (Dr) M K Soni
Faculty of Engineering, Manav Rachna International University Faridabad, Haryana, 121004, India
Email: ed.fet@mriu.edu.in

***Abstract*—**Mobile ad-hoc networks are networks that have properties of self configuration and multi hopping. These networks do not have any fixed infrastructure and need to be dynamic in nature. The specification of dynamism leads to various security breaches that a MANET suffers from such as impersonation, data modification etc. which results in degradation of performance and hence QOS is strongly affected. Hence this paper focuses on improving security performance of MANET by employing biometric technique in combination with cryptography, since biometric perception is specified as the most neoteric technological advancement which enhance security specifications of various networks by specifying exclusive human identification features. Cryptography is designed on computational hardness assumptions making various algorithms hard to break by an adversary. Simulation and experimental results specify that the proposed crypto-metric perception technique leads in achieving better QOS parameters by avoiding security intrusions hence better performance of mobile ad-hoc networks.

***Index Terms*—**MANET, crypto-metric technique, pattern resemblance, hamming distance, correlation coefficient, Hough transform.

I. Introduction

Networks that are autonomous in nature and can be instantaneously developed on demand to carry out definitive tasks for mission support are referred as Mobile ad-hoc networks. Communicating data across such a network is carried out through wireless links where nodes develop a temporary infrastructure to route and transmit data. Since MANET have flexibility and self organizing strength where they can coordinate with or without a wired network renders them a special feature but it also leads to various security impairments .Since mobile ad-hoc networks (MANET) are utilised in various emergency systems like military , weather forecast and disaster management so securing data is the most important feature for such networks. Due to the lack of centralized infrastructure use of various cryptographic algorithms is the most challenging task[1].This novel crypto-metric technique for improving security of MANET tends to remove various security breaches that mobile ad-hoc network suffers from.

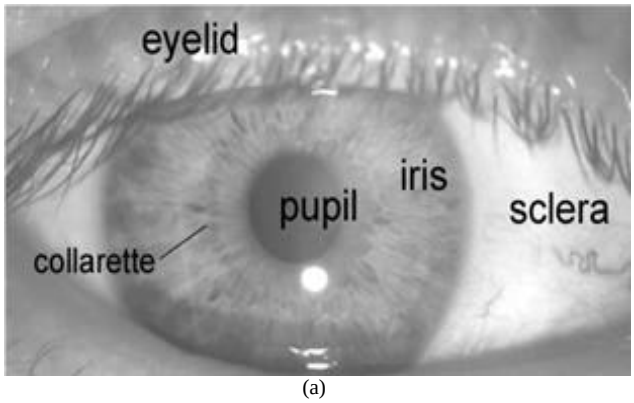
A. Security Impetration of MANET

Mobile Ad-hoc networks suffer from various passive and active intrusions such as unauthorized access, modification, deletion or disruption of information flow etc. It is uttermost important and desirable to maintain confidentiality and integrity of data at the application layer itself in-order to develop an eminent secured authentication system. Various traditional methods to provide authentication like cryptography that performs encryption and decryption of messages are used to overcome various attacks on MANET. But for mission critical and highly sensitive applications above mentioned traditional methods cannot be a full proof measure against various intrusions[1].Therefore the developed crypto-metric technique takes exclusive features by biometric perception and computational hardness of cryptography to help the MANET in overcoming various security intrusions and leading to better QOS parameters.

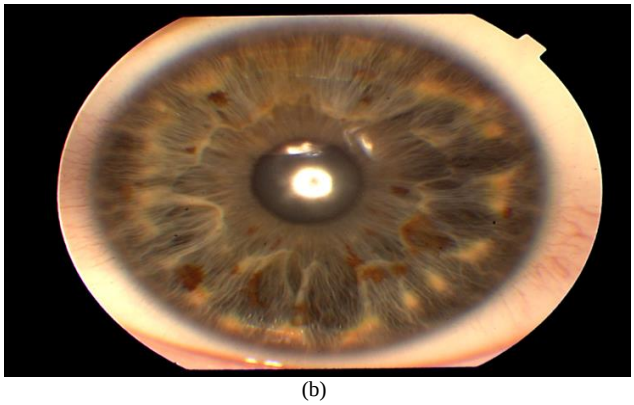
B. Biometrics & Quality of Service(QOS)

Behavioral lineaments of people for motorized recurrence is referred as biometrics which is considered to be one of the most important security feature added in various networks. Biometrics is immensely strenuous to tantamount as it summates an exclusive qualifier that cannot be acquired, jilted or stolen hence a very comprehensive tool for authentication in MANET. Traits of biometric can be divided into two specific sections; first which have extraordinary content and stability referred as strong biometrics, like fingerprints, DNA, iris, retina, etc, on the other hand weak biometrics have low original content and changes increasingly, like hand-geometry, face, keystroke dynamics, etc. Biometric systems although leads in large number of prevalence but still some security and privacy apprehensions occur like although genuine they cannot be eliminated or abolished also once lost biometrics tend to expose permanently and in-order to apprehend human traits cross-matching is done excluding their approval[1].Therefore crypto-metrics solutions are specified in this paper which

involves embedding cryptography (threshold) in nature.



(a)



(b)

Fig.1.(a) A front-on view of the human eye depicting its various parts (b) A close view of iris

with biometrics traits resulting in double security enhancement as biometrics alone cannot be a wholesome security solution for various types of networks.

Research trends of MANET are directed towards various categories like: QOS(Quality of Service), security of data and cross layer design leads to a wide research. Quality of Service is a guarantee specified by the network for various constraints for the user like end to end delay characteristics, availability of bandwidth, average packet loss etc. QOS of MANET includes: QOS models that specify an architecture to specify various services ,QOS routing which is a network layer service that searches a suitable path for resources but does not reserve the resources ,QOS adaptation that develops an interface for QOS control interaction by hiding various environmental features ,QOS signaling Acts which is a control centre for QOS support, QOS MAC protocols which are the quite essential components for QOS in MANET as they solve problems of medium contention by supporting reliable communication and leads to resource reservation. Fig.1.(a) focuses on view of human eye and its various parts and (b) depicts the headmost prospective of annular component called iris which is permeated adjoining to its mean through an annular circular fissure specified as the pupil. Iris regulates the extent to which light can insinuate through the pupil and this function is carried by the sphincter and the dilator muscles by modifying pupil size .Iris may have T average diameter of 12 mm whereas pupil size varies from 10% to 80% of the iris diameter [2]. An iris template can be created from 173 out of relatively 266 peculiar inclinations hence iris perception is the most assuring biometric mechanics[3].There is a requirement of procreation of various iris perception algorithms since it is proving to be an enhanced security tool for MANET. Later portions of the paper deals with related works on iris perception technique in section II then the neoteric crypto-metric technique discussed in section III and IV followed by experimental results ,conclusion and future recommendations in section V and VI respectively.

II. Related Works

A strong biometric security system tends to provide a mechanized perception of unique individual traits (iris or fingerprint) of individuals [4], so the most compelling security task which is dealt in this paper focuses on evolving a system of iris disjuncture residing noises such as varying eyelid, pupil & reflection. The iris perception system is affected by above mentioned noise parameters since iris code is produced using an iris pattern and that pattern is an outcome of iris disjuncture. Hence a secure iris perception algorithm demands vigorous iris disjuncture which is quite effectively carried out in this paper and validated through experimental results. The iris disjuncture process undergoes two important steps namely data procurement and iris disjuncture. The first step namely data procurement obtains various iris images through infrared illumination which is employed so as to get better image quality. The average considered diameter of iris is averagely 10 millimetres, and the recommended pixel number in iris diameter is generally more than 150 pixels. Regulations of “good quality”, "acceptable quality" and "marginal quality" by international standards are 200,150-200 and 100-150 pixels respectively. Hence smaller pixel iris image is considered as being a better quality image and a bigger pixel as being a lesser quality image [5].The iris disjuncture process restrict iris region in the image by suppressing number of noises employing various boundary espial algorithms. Addison [6] construe wavelet(mathematical function) employed to dissect a given function or a continuous-time signal into varying frequency components and consider every component with a resolution that affirm its scale. Eminence of wavelet transforms over conventional Fourier transforms is precise reconstruction and deconstruction of non-periodic bounded, and/or non stationary functions that have discontinuities and sharp peaks [7]. The above mentioned features make wavelets pertinent to create feature vector required for an iris perception algorithm.

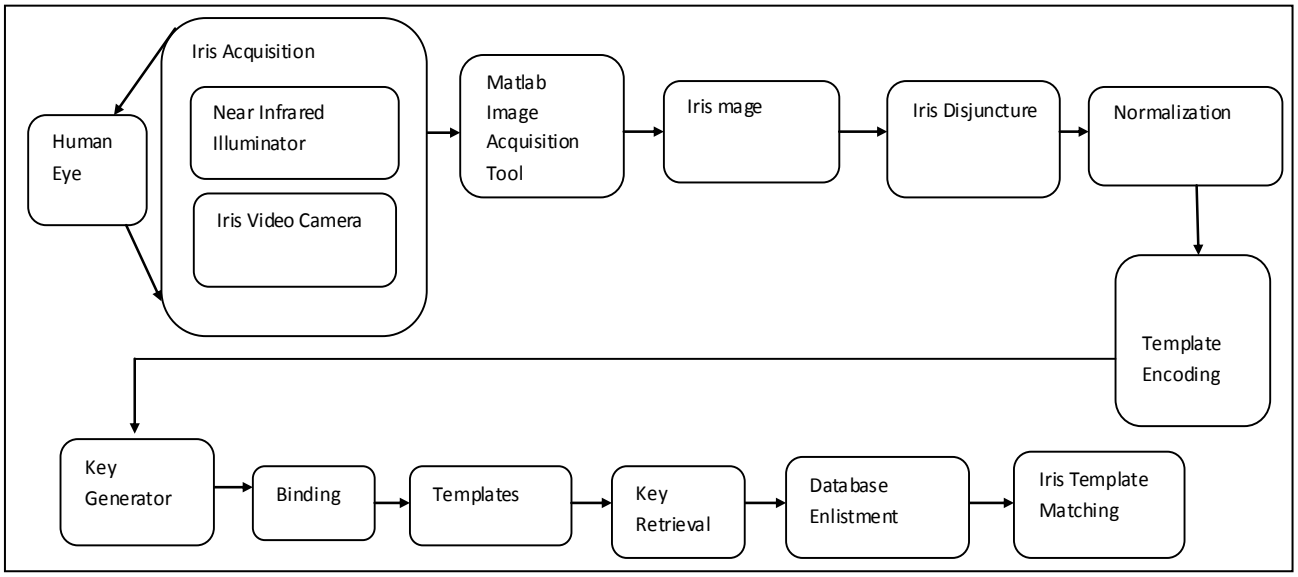


Fig.2. Novel Crypto-Metric Perception Algorithm

A large number of researches are made in the area of iris disjuncture and iris localization[7,8,9,10,11,12,13] in which Daugman and Wilde studies are considered quite fruitful in iris perception algorithms as they achieve a false rate(FAR) of 1 in four million and also false reject rate(FRR) of 0. Here refining undergoes a iris dissolution process which exploits for ascertaining iris as well as pupil contour which is illustrated by the given equation :

$$Max(r, x0, y0)G\sigma(r) * \partial \div \partial x \int r, x0, y0 I(x, y) \div 2 \prod rds \quad (1)$$

where:

- R, $x_{0,}$ $y_{0:}$ This is specified as the centre and radius of coarse circle (it is referred for each pupil as well as iris).
- G_σ (r): This is the Gaussian function.
- ∂_r: This is the radius extent (range) utilised to penetrate I(x, y) of the initial iris image.

Iris localized structure is altered through Daugman's dissolution algorithm from Cartesian to polar coordinates.

III. The Novel Crypto-Metric Algorithm

Fig.2. outlays novel quartered crypt-biometric perception algorithm which requires hardware as well as software to accomplish iris image acquisition and iris perception .A video camera employing a CCD image sensor whose focus can be adjusted according to manual requirements performs acquisition of the pattern of the iris image that leads to the development of the iris image acquisition system.

Lighting of the area where image is to be captured and distance from camera are essential requirements to improve the quality of iris image. Considering the facts that status of lighting as well as camera focus vary for distinct subjects, an adaptable steel bar backing is devised for the camera and also for the infrared light for the user to set the perfect distance from the camera and light source by the human eye. Also specifying that, focus if not perfectly acclimatized, noise can cause harm to image quality. Every iris image undergoes sampling process once for enlistment and next time for matching. For enlistment as well as matching, the images are taken subsequently acclimatizing the focus only once. A proper chin footing is also interspersed in the device for user adaptation. A digital camera is connected to aframe grabber of the computer by the image acquisition toolbox of MATLAB. All the frames are previewed through a personalized graphical user interface that avow the user for selecting the most pertinent image settings ahead of enlisting it to the iris recognition software.The novel crypt- biometric perception algorithm in Fig.2. portray various functions that are used for actuating and authentication of the iris image. Masek's disjuncture and normalisation methods are employed in this study. The image undergoes disjuncture, normalization, and template encoding. Hough transform is employed for image disjuncture which defines a circle according to equation (2):

$$x \wedge 2\, c + y \wedge 2\, c - r \wedge 2 \quad (2)$$

According to the Hough Transform for circles, each pixel in image space corresponds to a circle in Hough space and vise versa. Upper left corner of image is the origin of coordinate system.

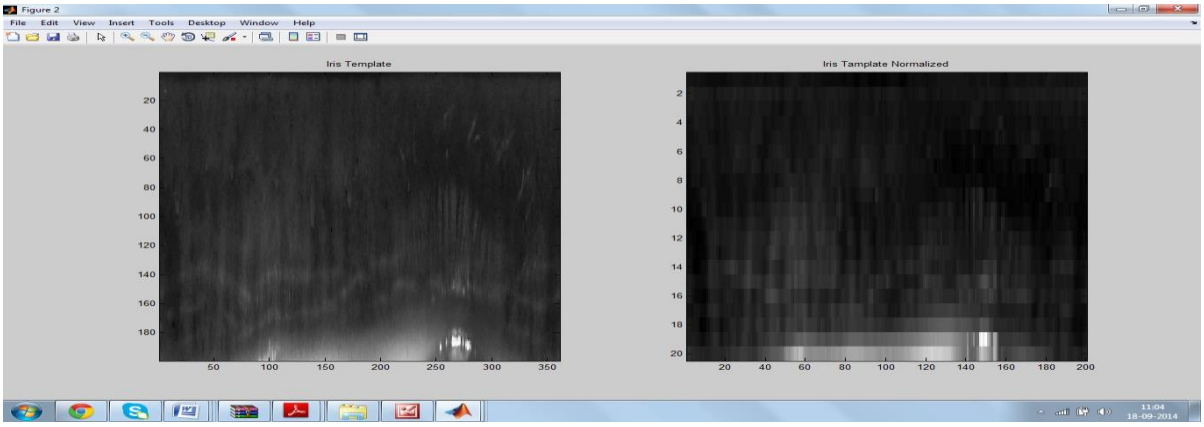


Fig.3. Bi-orthogonal Wavelet 3.5 Disintegration

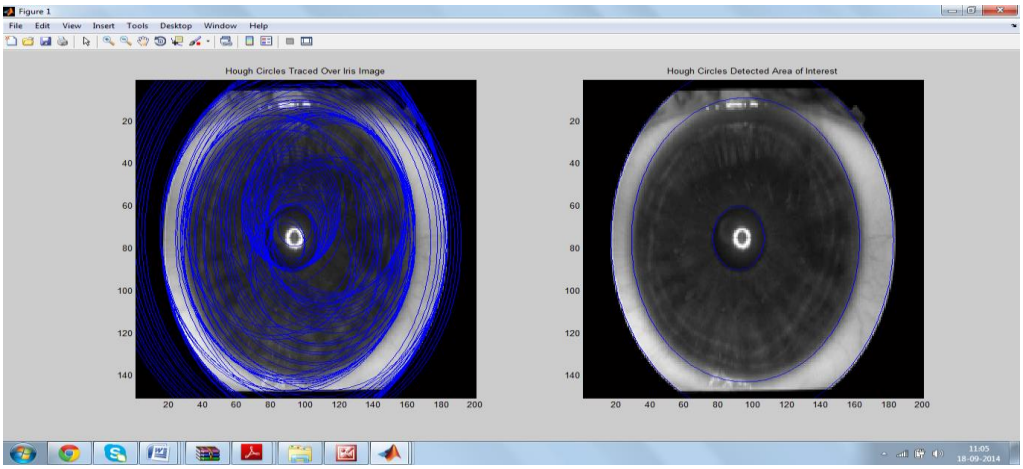


Fig.4. Hough Transformation on Iris Image

For performing Hough transform we have developed the following function in Matlab:

[y0detect, x0detect, Accumulator]=Hough circle (Imbinary, r, thresh, region)

where:

- Imbinary-It specifies a binary image. Image pixels that have value equal to 1 are interested pixels for HOUGHLINE function.
- R-Radius of circles.
- Thresh-A threshold value that determines the minimum number of pixels in image space. Threshold must be bigger than or equal to 4 (default).
- Region-A rectangular region to search for circle center within [x, y, w, h] which must not be larger than the image area. Default is image area
- Y0detect- row coordinates of detected circles.
- X0detect-column coordinates of detected circles.
- Accumulator-The accumulator array in Hough space.

Fig.3. depicts the hoarded iris image. The Hough transform method focalize the annular iris and pupil section, impeding eyelids, eyelashes, and reflections as depicted in Fig.4. Disjunction process is immensely captious for the success of the iris perception system.

IV. Design Of Crypto-Metric Perception Algorithm

A poor disparity betwixt the iris and pupil leads to out-of obligated values of iris sections causing various difficulties in disjunction process producing poor perception rates. For performing various comparisons, discursive iris image is then subjected to the normalization mechanism that performs transformation of the elicited iris region resulting into a rectangular section having perpetual extensity for overcoming imaging discrepancies, since the iris is elongated from differing levels of radiation. A biometric pattern is developed from the normalized section. In this paper, wavelet transposition algorithm is employed for extracting the distinctive information in-order to annex an iris template. Haar and Bi-orthogonal[14] transformations are applied for experimentation. Iris perception application is performed by applying the Hamming distance and Correlation specified by the formulae 3 and 4 respectively:

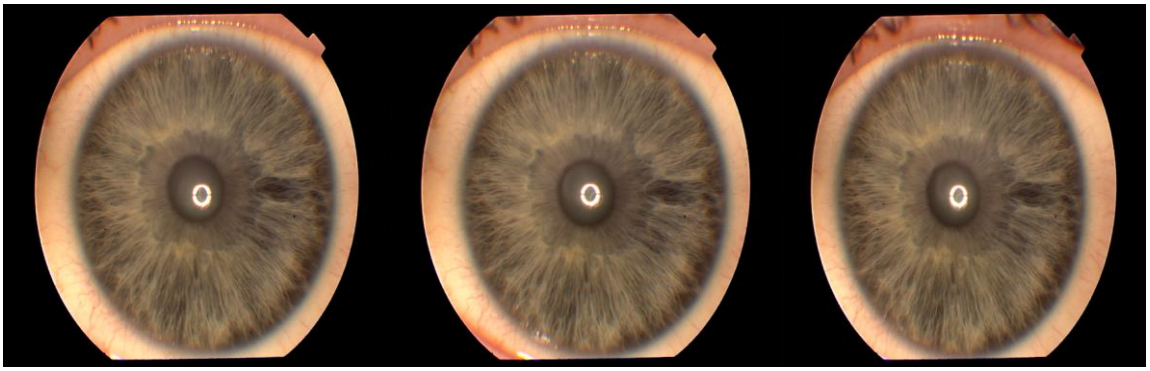
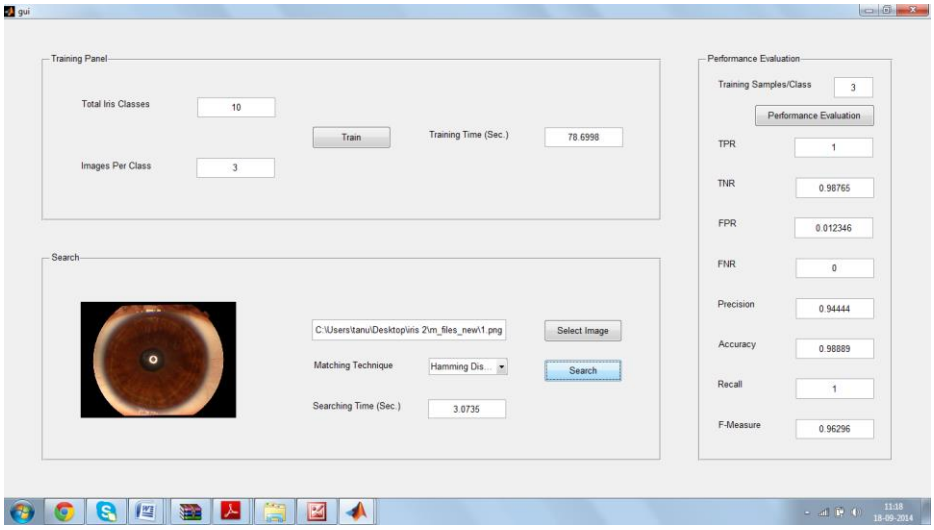
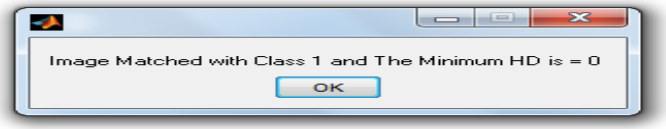


Fig.5. Three iris images of an individual from three different views specified from the developed database





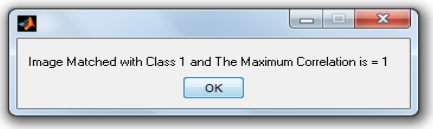


Fig.6. (a) Graphical user interface for iris perception application (b) Minimum Hamming Distance(HD) value (c) Maximum Correlation Value

$$Ham\min g$$

$$Dis\tan ce = 1 \div c\sum_{i=1}^{c} Mi \oplus Ni \quad (3)$$

where:
Mi and Ni = the i-th bit in the series M and N
c = total number of bits in each sequence.
$\oplus$ =Exclusive or operation.
Correlation Coefficient:

$$r = n\sum xy - (\sum x)(\sum y) \div \sqrt{n\sum x\wedge 2 - (\sum x)\wedge 2}\sqrt{n\sum y\wedge 2 - (\sum (y)\wedge 2} \quad (4)$$

where:
N is the number of pairs of data.
The value of r is such that $-1 \leq r \leq +1$. The + and – signs are used for positive and negative linear correlations respectively.Next step of the process is developing crypt-biometrics solutions using elliptic curve cryptography that is chaotic map based which results in

reduction of bandwidth overload of MANET since biometrics have some disadvantages dealing with privacy and exposing permanently once lost. Therefore after pattern resemblance a key generation procedure is undertaken providing two levels of security for this model. Biometric template undergoes binding with the generated key for hoarding into the database; biometric encrypted templates followed by key retrieval. Template matching with the corresponding hoarded images is performed by calculating the hamming distance and correlation. Correlation parameter is never calculated by any biometric perception software providing uniqueness in this study, also it provides two parameters for pattern resemblance and certification hence improving security specifications of MANET and also avoids occurrence of any biometric frauds. The propound software was estimated for its pursuance by conducting various biometric evaluation metrics on it so as to actuate whether the purpose of study is fulfilled or not.

V. Simulation and Experiment

Several iris images were tested from various individuals. The propound technique took total 10 iris classes with 3 images per class and training was done to create iris templates. Fig.5. shows three iris images of an individual from three different views. Fig.6(a). exemplifies the graphical user interface (b) Minimum Hamming Distance value (c) Maximum Correlation value advanced by applying MATLAB GUI builder, which encompasses all the components for the iris perception application. Each iris template is hoarded in the database by a specified classifying number. When an image from developed database was selected it matched with class 1 generating a minimum hamming distance(HD)=0 and Maximum Correlation =1which scrutinized our result. Thus two performance parameters hamming distance and correlation provides a double check on various biometric templates hence enhancing security solutions for mobile ad-hoc networks. Iris disjuncture results were evaluated during the complete trials period as disjuncture results are very important and critical for the completion and success of the iris perception system. A database is maintained for storing the iris images of various individuals whose templates are later used for pattern resemblance.

The iris image which is encoded and later on crypt-biometric embedded; template undergoes testing the finest wavelet concomitant for analysis. Several testing methods were considered for evaluating the accomplishment of the propound system. The minimal and maximal Hamming distance and correlation values of various templates accessed in the database were examined. Thus based on various results the value of intensity of flexibility is also analysed which is the number of values in the final summation of figure that its free to differ[16].

Oneness of iris pattern is specified by the value of intensity of flexibility(IOF) shown by the template specified by following formula:

$$\begin{matrix} Intensity \\ of \\ flexibilty\ (IOF) \end{matrix} = (\rho(1-\rho) \div \sigma \wedge 2$$

where:
ρ=mean of distribution
σ=standard deviation of the distribution

Since we are dealing with biometric templates sensitivity and specificity classification tests as depicted in Fig.(7) are performed to analyze the proportion of actual positives; referred as true positive rate(sensitivity) or recall rate. In general, Positive = identified and negative = rejected. Therefore:

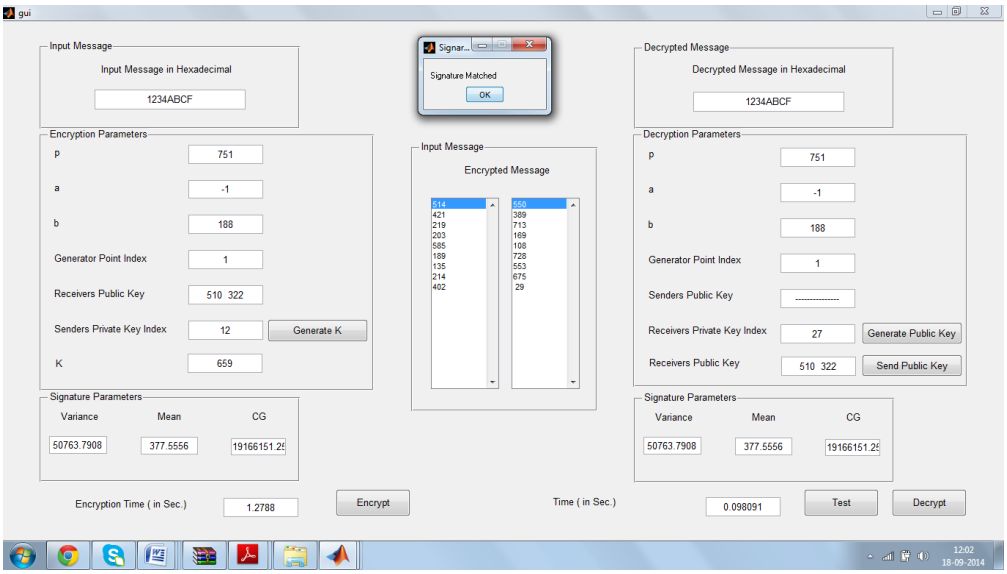


Fig.7. Graphical user interface of threshold(elliptic curve) cryptography

- True positive(TP) = correctly identified
- False positive(FP) = incorrectly identified
- True negative(TN) = correctly rejected
- False negative(FN) = incorrectly rejected
- 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)
- F-measure = 2*Precision*Recall/(Precision + Recall);

True negative rate(specificity) is also analyzed which specifies the proportion of negatives. Hence the developed software further undergoes various performance tests such as TPR(True positive rate),TNR(True negative rate), FPR(False positive rate) and FNR(False negative rate).The example discussed above of iris image matching class 1 having hamming distance =0 and maximum correlation=1 when evaluated using the novel crypt-biometric scheme provided excellent results yielding values like :TPR=1, TNR=0.98765,FPR=0.012346,FNR=0,Precision=0.9444, Accuracy=0.98889,Recall=1,F-Measure=0.96296.

Similarly the generated database with number of iris images was undergone evaluation through our developed technique which led to quite good results through all the above mentioned parameters hence leading to an enhanced security solution for mobile ad-hoc networks. Fig.7. also shows the components of threshold cryptography to encrypt the data. RSA and ECC as homomorphic in nature are applicable to threshold cryptographic systems which allows splitting of various cryptographic operations among multiple nodes of MANET such that any subset comprising of m users(nodes)can perform an operation, where m is a predefined number. Various tests were also undergone for QOS parameters resulting in improved performance.

VI. Conclusions

Conclusion focuses on the various results and parameters being successfully achieved for crypto-metric security algorithm designed to secure as well as enhance QOS performance of MANET. The flexibility and usability of this biometric technique is enhanced with successful values of hamming distance and correlation coefficient. Specificity and sensitivity analysis results also analyze the biometric component of the algorithm providing fruitful results. Use of threshold (elliptic curve cryptography) overcomes various flaws of biometric security technique and by analyzing and comparing various QOS parameters of MANET (network length, width, speed variation, average end to end delay e.tc.) with various other existing secure routing protocols provided an enhanced crypto-metric solution for ad-hoc networks. Meta-heuristic algorithm is an illustrious method consummated to credit, commence or stipulate a lower-level scenario or heuristic (partial exploration algorithm) that execute a relevantly admissible definition to optimization dilemma, confined with remarkable compressed intelligence or cramped data processing capability. They are pertinent for various complications that make deficient hypothesis about the optimization problem being elucidated [17,18].Future considerations deals in embedding various meta-heuristics algorithms with crypto-metric technique for achieving optimized results which will further help in overcoming security breaches of MANET and hence better QOS results.

Acknowledgement

The authors wish to thank Professor M.M. Sufiyan Beg, Professor Department of Computer Engineering, Aligarh Muslim University, for his support and guidance throughout this paper.

References

[1] Sherin Zafar, M.K Soni,"Secure Routing In MANET through Crypt-Biometric Technique ", IEEE FICTA Conference, 2014.
[2] E.Wolff "Anatomy of the Eye and Orbit":7th edition .H.K Lewis Co.Ltd.
[3] P. Khaw, "Iris Recognition Technology for Improved Authentication", SANS Security Essentials(GSEC)Practical Assignment, version 1.3,SANS institute, pp 5-8,2002.
[4] L. Masek, "Recognition of Human Eye Iris Patterns for Biometric Identification", University of west California, 2003.
[5] Biometric Data Interchange Formats-Part 6"Iris Image Data Safety of Laser Products -Part-I "Equipment Classification and User's Guide, IEC 60582-1, 2001.
[6] S.Lim, K.Lee, O.Byeon, and T.Kim, "Efficient Iris Recognition through Improvement of Feature Vector and Classifier ", ETRI Journal Volume 23.No.2, 2001.
[7] J.Daugmann, "High Confidence Visual Recognition of Persons by a Test of Statistical Independence", IEEE Trans 1 on Pattern Analysis and Machine Intelligence, Vol.15, issue11, 1993.
[8] J. Daugman.,"Biometrics: Personal Identification in Networked Society" .Kluwer Academic Publishers, 1999.
[9] J. Daugman. Iris recognition. American Scientist, 89:326–333, 2001.
[10] J. Daugman, "How iris recognition works", IEEE Transactions on Circuits and Systems for Video Technology (CSVT), 14(1):21–30, 2004.
[11] J. Daugman, "Probing the uniqueness and randomness of iris codes: Results from 200 billion iris pair comparisons", Proceedings of the IEEE, 94:1927–1935: Nov, 2006.
[12] R. P. Wildes. Iris recognition: An emerging biometric technology, Proceedings of the IEEE, 85(9):1348–1363, 1997.
[13] R. P. Wildes, a. J. C. Asmuth, C. Hsu, R. J. Kolczynski, J. R. Matey, and S. E. McBride ,"Automated, Non invasive iris recognition system and method" U.S. Patent,(5,572,596) , 1996.
[14] A. Graps, "An Introduction to Wavelets", IEEE Computational Science and Engineering, Summer: 1995.
[15] M. Misiti, Y. Misiti, G. Oppenheim, and J Poggi, Wavelet Toolbox 4 User's Guide ,1997-2009.

[16] J. Daugman, "How Iris Recognition Works", IEEE Proc. on Image Processing, 2002, doi: 10.1109/ICIP, 1037952, pp.33-36:2002.
[17] Sherin Zafar, M.K Soni,"Sustaining Security In MANET: Biometric Stationed Authentication Protocol (BSAP) Inculcating Meta-Heuristic genetic Algorithm", I.J. Modern Education and Computer Science, 2014, 9, 28-35 Published Online September 2014 in MECS (http://www.mecs-press.org/) DOI: 10.5815/ijmecs.2014.09.05.
[18] Sherin Zafar, M.K Soni,"Trust Based QOS Protocol(TBQP) using Meta-heuristic Genetic Algorithm for Optimizing and Securing MANET", IEEE International Conference On Reliability, Optimization & Information Technology (ICROIT), pp173-177,2014.

Author's Profile

Sherin Zafar is an B.E, M.Tech in Computer Science and Engineering from RGPV Bhopal in 2006 and 2010 respectively. Sherin is pursuing her PhD degree in Computer Engineering from Manav Rachna International University Faridabad 2011-12 batch. She is now Assistant Professor in Computer Section in Faculty of Engg. Jamia Millia Islamia New Delhi. In teaching, she has been focusing on Computer networks, DBMS etc. Her research interests include ad-hoc networks, meta-heuristic algorithms and network security.

DR. M.K Soni has degrees of BSc Engg , MSc Engg and PhD with 40 years of academic experience. He is currently Executive Director and Dean in Faculty of Engineering Manav Rachna International University Faridabad. He was formerly Professor in NIT Kurukshetra. His current research areas include microprocessors and microcontrollers.

Manuscript received: May 24, 2014; Accepted September 15, 2014

How to cite this paper: Sherin Zafar, M K Soni,"A Novel Crypt-Biometric Perception Algorithm to Protract Security in MANET", IJCNIS, vol.6, no.12, pp.64-71, 2014. DOI: 10.5815/ijcnis.2014.12.08

