International Journal of Engineering & Technology, 7 (2.7) (2018) 1091-1095

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

A survey on biometric based crypto techniques

K. Ruth Ramya [1] *, S. Saahithi [1], T. Gnaneswar [1], SD. Afsar Jaha [1]

[1] Department of Computer Science and Engineering, Koneru Lakshmaiah Educational Foundation, Guntur
**Corresponding author E-mail: ramya_cse@kluniversity.in*

Abstract

The biometric based crypto techniques extract the features from grayscale images and use those features in encryption process i.e., key will be generated from extracted features. In attribute based crypto-systems attributes of the user like email, usernames etc.…will be treated as a public key. Secret key is associated with each attribute i.e. for email there will be a secret key and for username there will be another secret key. In biometric based crypto systems, an access policy is built from the extracted biometric features.

Keywords: *Attribute Based Encryption; Image Processing; Finger Prints; Palm Prints*

1. Introduction

Biometrics authentication systems came into existence to validate users. Mean while Attribute-Based-Encryption is another technique in public key crypto systems. Encrypting with user biometrics will enhance the complexity of crypto-system. Previously biometrics and ABE were used separately for encryption [1, 2]. Now a day's biometrics are used for providing authentication to the systems where sensitive data is stored. Biometrics is the technique of applying the statistical analysis of a user biological data in order to identify a person uniquely. Most generally used biometrics are physical attributes of the user like finger prints, facial features, hand geometry, iris templates etc.…Finger print biometric technique is frequently used and most affordable. Advantages of using finger print biometrics are collisions will be less because among the biological features of a person finger prints are the one which will not match among individuals. Two types of portions need to be taken into consideration while extracting features from biometrics. Curved lines seen on finger are called ridges and the remaining part surrounding the ridges is called valleys. After biometric is enhanced ridges are black in color and valleys are white in color. Process of extracting features includes five main steps namely Image segmentation, Image enhancement, Binarization, Thinning, Extraction [9, 10].

Image segmentation means reading image pixel-wise in order to perform necessary actions. Images scanned may not be noise free but sometimes noise will occur during scanning and all ridges may not be scanned properly due to sensor problems so, image once scanned must be enhanced to get a clear picture of ridges and valleys. Binarization means further enhancing image into black and white format (binary format) and increase the color intensity. After binarization the finger prints will look with high intensity so, it need to be processed further to improve minutiae map involved which is called thinning. Finally, required features are extracted after all the enhancements are once done as shown in figure 1.

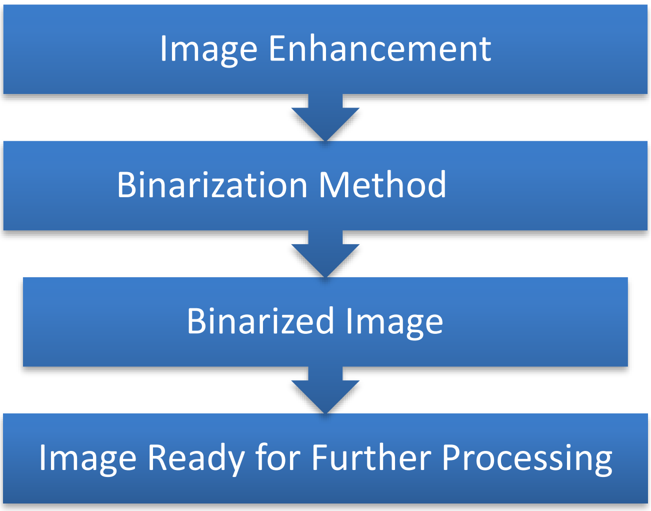

Fig. 1: Binarization Process Flow Chart.

1.1. Binarization techniques

Binarization techniques are of two typesGlobal andLocal. Global techniques include fixedthresholding [11], [12], [13], Otsu [14], Kittler[14]and Local techniques include Adaptive [14], Niblack [15], Sauvola [16], [17], Bernsen [8].

1.2. Thinning algorithm

Delete pixels inside biometric image without changing shape of the image as shown in figure 2.Check whether neighboring pixels of current pixel are 0 or 1 as shown in figure 2.Compute N(P1) = P2+P3+…+P9 which is number of non-zero pixels.P1 is present pixel and neighbors are P2,P3,P4,P5,P6,P7,P8, and P9.Compute S(P1) which is the number of transitions with different states i.e. number of transitions on 0 to 1 and number of transitions on 1 to 0 as show. This algorithm consists of two passes one after the other as shown below.

Pass 1: Mark the pixel only at the edge not satisfying atleast one of the below conditions

N (P1) = 0 (Isolated pixel)
N (P1) = 1 (Tip of the edge)
N (P1) = 7 (Located in concativity)
N (P1) = 8 (Not boundary of image)
S (P1) >= 2 (Acting as a bridge connecting two or more edge pixels)
Pass 2: Delete all the marked pixels.

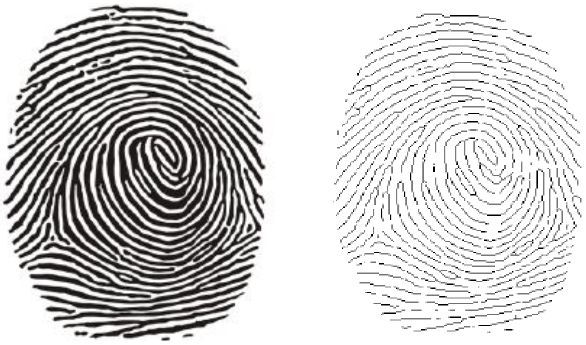

Fig. 2: Before Thinning After Thinning.

2. Literature survey

Christian Holz et al., [18] proposed secure method for fast device authentication for web services. Earlier, there is a cross device authentication using OTP and Christian Holz et al., [24] changed it into request approval

Mohammed Nasir Uddin et al [19] made a survey on biometrics and their usage and mentioned several applications of biometrics like banks, ATMs, smart phones, computer networks etc.… and explained each and every biometric technique and how the features are being extracted from the biometric samples and elaborated the essence of biometrics and the level of security that can be provided. Examining the usage of biometrics and the security issues in internet access with increasing growth in internet usage day-by-day a prototype of accessing the web content by authenticating the user with hand geometry was proposed.

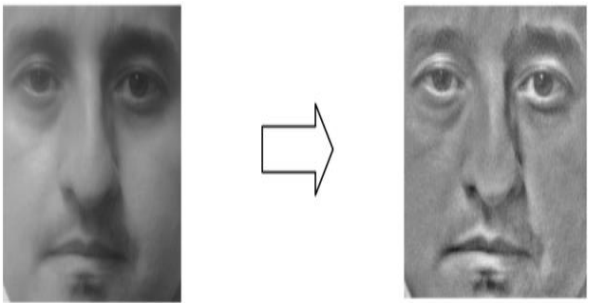

Fig. 3: Biometric Method Used for Mobile Authentication for African Farmers.

Shah Faisal Darwaish et al., [20] found increase in level of mobile devices usage for business and personally and proposed a solution for authenticating android smart phones using biometrics of user in offline mode and implemented it for African cashew farmers for their fund transfers which will provide secure authentication. Proposed method is first scan the face of user, detect eyes and other points on face, measure the distances, store them in the form of keyas shown in figure 3and found that their implementation has 9.6% error rate. They trained system using 1000 images and tested 3 times with 250 images each and the error rate was 9,6% in all three sets.

Izem Hamouchene et al., [21] made a proposal of an algorithm for iris recognition using texture analysis of iris image portion. CASIA iris database was used for implementation. The portion of iris is taken as rectangular iris and that rectangular iris is converted into iris code which is in the form of binary iris code. Scanned pixel values starting from top left corner moving in clockwise direction. Rotation of image was handled using Rotation invariant Neighbourhood-based Binary Pattern as shown in Figure 4.

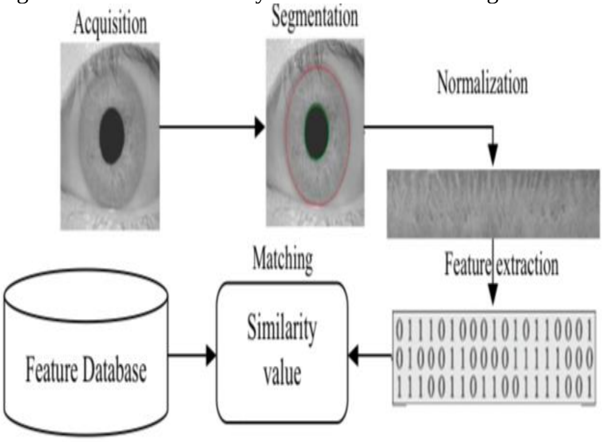

Fig. 4: New Texture Analysis for Iris Recognition.

Inass SH. Hussein et al., [22] proposed a methodology for verification of hand or palm print by their own method of preprocessing and verification as shown in figure 5.This method involved preprocessing and verifying modules. Pre-processing stage is converting the whole image into binary image and then extracting only palm image from whole binary image. In Verification stage image is queried from database and compared with the image that is binarized. This method gave 97.99% accuracy rate of verification by using IITK database.

Fig. 5: IITK Database Palm of Single Person.

Hugh Wimberly et al., [23] told that Password is the weakest portion of many important systems. They made 96 employees to register in two accounts each and then made a survey how strong the passwords are.They made a proposal for verifying users by their biometrics. Replacing passwords with biometrics was the prototype proposed. Weak passwords may be hacked but biometric authentication can’t be guessed by others because finger prints are the one which can’t be matched between individuals.

Dhiraj Sunehra [24] proposed a Finger print authentication for the ATM machines. They used embedded system for dumping the algorithm into PIC micro-controller. If the finger prints given by scanner and the queried one matches then the cash box opens else alarm will fire.

Kumar Ankit [25] as shown in figure 6proposed a method to use biometrics as a crypto method for network security.

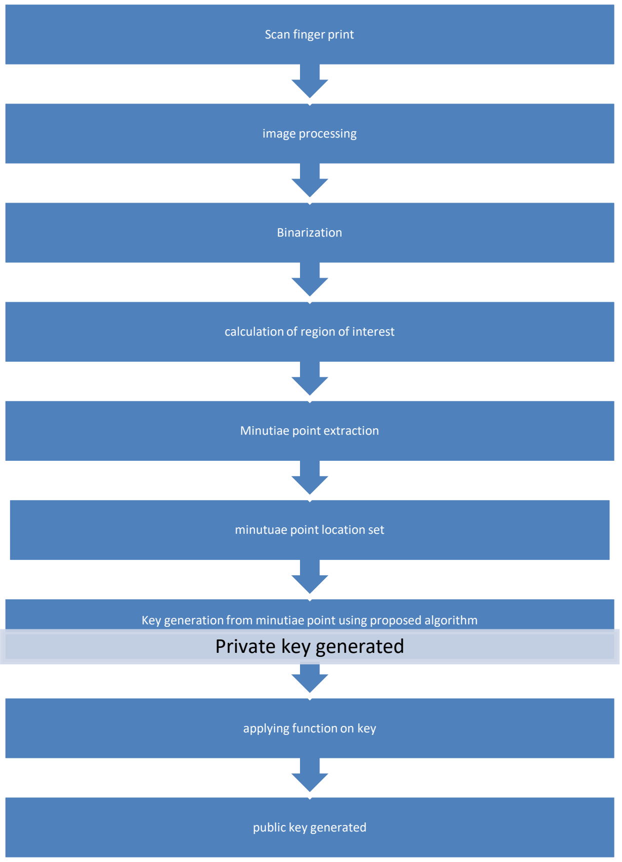
Scan finger print
image processing
Binarization
calculation of region of interest
Minutiae point extraction
minutuae point location set
Key generation from minutiae point using proposed algorithm
Private key generated
applying function on key
public key generated

Fig. 6: Biometric Network Security Approach.

Sang-Hyeon Ryu [26] showcased a speaker distinguishing proof utilizing voice-based cryptography for portable VoIP secure voice correspondence framework. The cryptographic open key was produced from the client's voice and used to encode the exchanged voice information over IP systems. The voice unique mark from the voice information was decoded for the speaker ID in view of Bayesian data measure.

Sattar B. Sadkhan [27] audited majority of encryption systems which receive mayhem based cryptography, and delineates the utilized confusion based voice encryption strategies in remote correspondence too. The audit condensed the conventional and present day strategies of voice/discourse encryption and exhibited the plausibility of receiving mayhem based cryptography for in remote correspondences.

Musheer Ahmadet al [28], proposed a chaos based keystream generator for voice information encryption. The voice information bitstreams are encoded utilizing mixed key stream. High dimensional chaotic frameworks like Lorenz and Chen are utilized to produce more complex and un-predictable six chaotic sequences as shown in figures 7a & 7b.

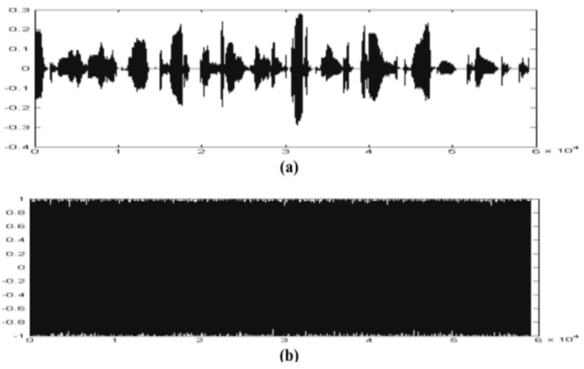

Fig. 7: Original Voice Signal, 7b: Encrypted Signal.

Jiaa, Huanga and Zhang [29] projected palmprint verification based on the robust line orientation code. Modified finite random transform has been utilized for feature extraction that extracts the orientation features. Line matching schemehas been used for matching test image with the training image that is based on pixel-to-area algorithm.

Prasad, Govindan and Sathidevi [30] proposed palmprint authentication by means of Fusion of Wavelet Based Representations. Highlights extricated are includestextureand also line highlights. Framework pre-preparing includes low pass shifting arrangement, area of invariant focuses, not withstanding arrangement and extraction of ROI, OWEis utilized for the element extraction. The match scores are created for surface and line includes independently and in joined modes too. Weighted whole govern alongside item administer is utilized for score level coordinating

Dai and Zhou [31] presented high determination approach for palmprint acknowledgment usingmethods for different highlight extraction. Highlights like details, thickness, and introduction with chief lines are taken for include extraction. Particular extraction Gabor channel is utilized for edge change as indicated by the nearby edge heading and thickness. Thickness outline assessed by utilizing the composite calculation, Gabor channel, Hough change.

Dai, Feng, Zhou [32] presented a fragment based palmprint coordinating and combination calculation, where entire palmprint picture is isolated into various locales and after that each district is independently coordinated to manage the mutilation. The likeness of two palmprints is processed by melding the similitude scores of different portions utilizing a Bayesian system as shown in figure 8.

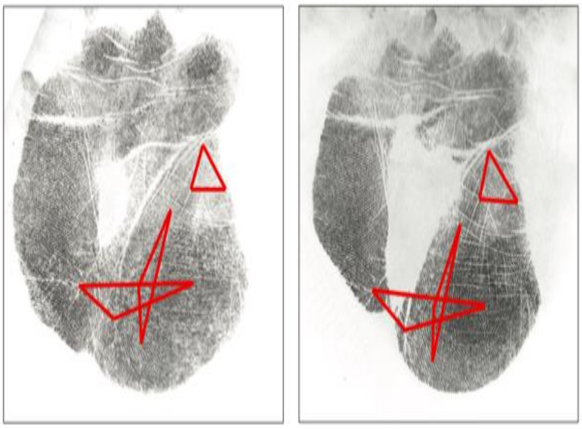

Fig. 8: Palm Identification Method.

P.S. Sanjekar [33] has utilized Haar wavelet for the palmprint recognizable proof which is a picture based procedure. Coordinating contrast vector blueprint is utilized that includes standard deviation and mean as shown in figure 9.

Biometrics can be considered as user attributes. So, encryption using biometrics can also be an attribute based encryption. Taking a biometric sample from the users, extracting features as mentioned above, using those features to build an access policy (key) [6,7]and ten encrypt data. In Decryption scanner triggers to scan the access policy (key) again and scanned biometric samples are used to generate decryption access policy (key). If the biometric samples of both the encryption and decryption keys are same then there won’t be any problem and the decryption will be done.

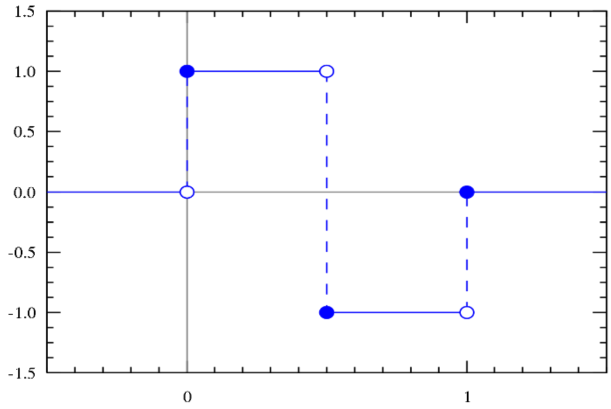

Fig. 9: Haar Wavelet.

Figure 10 describes usage of biometric technologies. When compared to other biometric technologies like Iris, Face recognition, Palm vein etc., Fingerprints are highly recommended for using as attributes in attribute based encryptions (ABE).

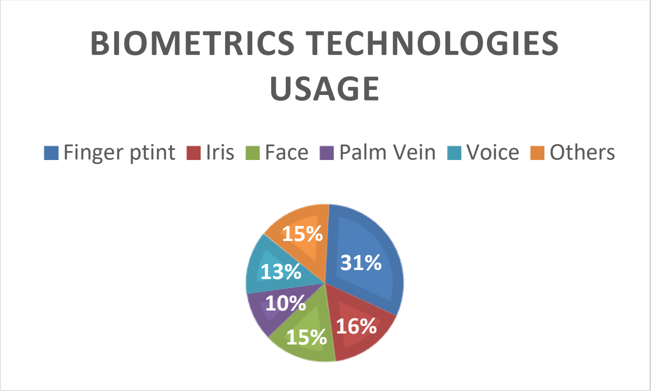

Fig. 10: Biometric Technologies Usage.

Table 1 compares various biometric technologies lice Fingerprint, Face Recognition etc., based on Accuracy, Ease to use, user Acceptance.

Table 1: Comparison of Various Biometric Technologies

Modality	Accuracy	Ease to use	User Acceptance
Face	Low	High	High
Finger Print	High	Medium	Low
Iris	High	Medium	Medium
Palm Vein	High	High	Medium
Voice Medium	Medium	High	High

Figure 11 explains graph for False Rejection Rate (FRR) and False Acceptance Rate (FAR) for various biometric techniques and results shows that Face Recognition has higher FAR & FRR when compared to remaining biometric techniques.

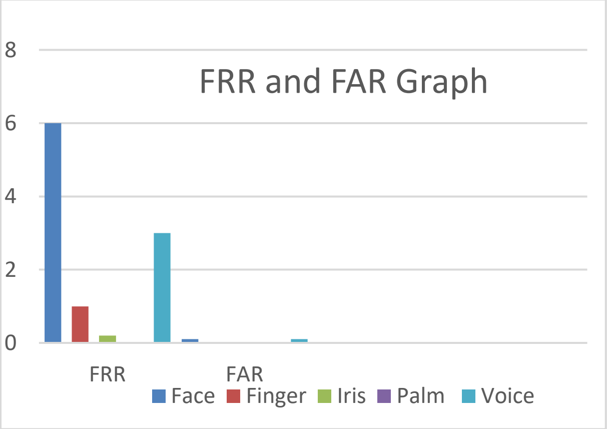

Fig. 11: X-Axis - Rate of Acceptance or Rejection.

Y-Axis- Biometric Techniques
Fig 11: Biometric Technologies FRR & FAR Graph

3. Conclusion& future scope

Survey on biometric feature extractions like minutiae points from fingerprints, hand geometry and facial features. Using minutiae points as attributes for encrypting data. Concluded that finger print based biometrics will be more accurate and affordable among all the biometric techniques, as it doesn't match between individuals and doesn't change with age. So, decided to use finger prints in future work on biometrics, extracting minutiae points from finger prints of a single or multiple users to build access policy and encrypt text or image file using CP-ABE [3], [4], [5].

References

[1] Identity Based Encryption - David Oswald.
[2] Shamir, "Identity based crypto systems and schems" – Document.
[3] J. Bethencourt, A. Sahai, and B. Waters, "Cipher text-policy attribute- based encryption," IEEE.
[4] Mr. Anup R. Nimje #1, Prof. V. T. Gaikwad*2, Prof. H. N. Datir^3 "Attribute - Based Encryption Techniques in Cloud Comp uting Security: An Overview" International Journal of Computer Trends and Technology - volume4Issue3 - 2013.
[5] Zhibin Zhou, Member, IEEE Dijiang Huang, Senior Member, IEEE, and Zhijie Wang "Efficient Privacy-Preserving Ciphertext-Policy Attribute Based Encryption and Broadcast Encryption".
[6] J. Katz, A. Sahai, and B. Waters, "Predicate encryption supporting disjunctions, polynomial equations, and inner products,"
[7] Rafail Ostrovsky, Amit Sahai,Brent Waters "Attribute based encryption with Non-Monotonic access structure."- eprint.iacr.org
[8] Eric zaxahoni, Luis J. Dominguez, Shigeo Mitsunari, Ana H. Sanchez Ramirez, Tadanori Teruya-Henriquez, "Software implementation of Attribute based encryption scheme"- IEEE.
[9] Chaohong WU, "Advanced feature extraction algorithms for automatic fingerprint recognition systems".
[10] Asker M. Bazen, "Finger print feature extraction, matching & database search", - ist.psu.edu.
[11] M.I. Sezan, "A peak detection algorithm and its application to histogram - based image data reduction", Computer Vision, Graphics, and Image Processing 49 (1) (1990) 36 – 51.
[12] Rosenfeld, P. de la Torre, "Histogram concavity analysis as an aid in threshold selection", IEEE Transactions on System, Man, and Cybernetics 13 (1983) 231 – 235.
[13] T. Pavlidis, "Threshold selection using second derivatives of the gray - scale image", in: Proceedings of the ICDAR, 1993, pp. 274 – 277.
[14] N. Otsu, "A thresholding selection method from gray - scale histogram", IEEE Transactions on System, Man, and Cybernetics 9 (1979) 62 – 66.
[15] Khurram Khurshid, Imran Siddiqi, Claudie Faure, Nicole Vincent, "Comparison of Niblack inspired Binarization methods for ancient documents", 16th International conference on Document Recognition and Retrieval, 2009.
[16] J. Sauvola, T. Seppänen, S. Haapakoski, M. Pietikänen, "Adaptive document binarization" , Fourth International Conference Document Analysis and Recognition (ICDAR), p. 147 - 152, Ulm, Germany, August 1997.
[17] Madhuri Latha, Chakravarthy, "An Improved B ernsen Algorithm Approaches for License Plate Recognition", IOSR Journal of Electronics and Communication Engineering (IOSR - JECE) ISSN: 2278 - 2834, ISBN: 2278 - 8735. Volume 3, Issue 4 (Sep - Oct. 2012).
[18] Christian Holz, Frank R. Bentley [24], "On-Demand Biometrics: Fast Cross-Device Authentication" #chi4good, CHI 2016, San Jose, CA, USA
[19] Mohammed Nasir Uddin, Selina Sharmin, Abu Hasnat Shohel Ahmedand Emrul Hasan, Shahadot Hossainand Muniruzzaman, "A Survey of Biometrics Security System", IJCSNS International Journal of Computer Science and Network Security, VOL.11 No.10, October 2011.
[20] Shah Faisal Darwaish, Esmiralda Moradian,Tirdad Rahmani, Martin Knauer,"Biometric identification on android smartphones ", 18th International Conference on Knowledge Based and Intelligent Information & Engineering Systems - KES2014.

[21] Izem Hamouchene, Saliha Aouat, A New Texture Analysis Approach for Iris Recognition, 2014 AASRI Conference on Circuit and Signal Processing (CSP 2014).

[22] Inass SH. Hussein and Md Jan Nordin, “Palmprint Verification using invariant moments based on wavelet transform”, Journal of Computer Science 10 (8): 1389-1396, 2014.

[23] Hugh Wimberly, Lorie M. Liebrock , “Using Fingerprint Authentication to Reduce System Security: An Empirical Study”, 2011 IEEE Symposium on Security and Privacy.

[24] Dhiraj Sunehra, “Fingerprint Based Biometric ATM Authentication System”, International Journal of Engineering inventions.

[25] Kumar Ankit and Jayaram Rekha, “Biometrics as a Cryptographic Method for Network Security ”, Indian Journal of Science and Technology, Vol 9(22), DOI: 10.17485/ijst/2016/v9i22/95288, June 2016

[26] Sang-Hyeon Ryu and Hyoung-Gook Kim, “Speaker identification using voice-based cryptography for mobile VoIP secure voice communication”, - IEEE

[27] Sattar B. Sadkhan, Ali Al-Sherbaz, Rana S. Mohammed, “”Chaos based cryptography for voice encryption in wireless communication”, -IEEE

[28] Musheer Ahmad, Bashir Alamand Omar Farooq, “Chaos based mixed keystream generation for voice data encryption”.

[29] Huang,W. Jia, D. Zhang, “Palmprint verification based on robust line orientation code,” Pattern Recognition, Science Direct, pp. 1504 – 1513, 2008.

[30] S. M. Prasad, V.K. Govindan, P. S. Sathidevi, “Palmprint Authentication Using Fusion of Wavelet Based Representations,” IEEE, pp. 978-1-4244-5612-3, 2009.

[31] J. Dai and J. Zhou, “Multi feature-Based High- Resolution Palmprint Recognition,” IEEE Transaction on Pattern Analysis and Machine Intelligence, Vol.33, No. 5, pp. 0162-8828, May 2011.

[32] J. Dai, J. Feng, J. Zhou, “Robust and Efficient Ridge- Based Palmprint Matching,” IEEE Transaction on Pattern Analysis and Machine Intelligence, Vol.34, No. 8, pp. 0162-8828, August 2012

[33] P.S. Sanjekar, “Palmprint Identification by Wavelet Transform,” Proc. Of international conf. on Image Processing and vision System, Vol 1, Oct 2011.