A Fuzzy Vault Based Multimodal Biometric Cryptosystem for Enhancing Security

Dr Gandhimathi Amirthalingam[1], G.R. Janarthanan[2]
[1]*Department of Computer Science, King Khalid University, Kingdom of Saudi Arabia*
[2]*Department of Information System, Nehru Technologies, India*

(E-mail: mathymca@yahoo.com)

***Abstract*—** Unimodal Biometric systems stumble upon a noisy sensor acquisition, non-universality performance rate and variety of security problems. It may be inclined to different attacks like a man-in-the-middle attack, Trojan horse attack, collision attack, and replay attack. Template security and privacy are essential issues to be addressed for assuring successful biometric deployment. To overcome these problems, multibiometric systems are now prevalent. In this study, we proposed a method for face and ear multimodal biometric system. The exact shape of the face and ear are obtained by employing a modified region growing algorithm and texture by Local Gabor XOR Pattern (LGXP) technique. Template security and accuracy of the multibiometric system are increased by using fuzzy vault multibiometric cryptosystem. The feasibility of these algorithms for analyzing is obtainable through experimental analysis. The experimental results of the proposed method are evaluated using False Matching Rate (FMR), False Non-Matching Rate (FNMR) and Genuine Acceptance Rate (GAR). The performance of the suggested method shows the promising growth in the multimodal biometric recognition and template security**.**

***Keywords*— *Multimodal biometric, Biometric recognition, Fuzzy vault, Cryptosystem, LGXP, Modified region growing algorithm, Face recognition, Ear recognition*.**

I. INTRODUCTION

In recent years, authentication has become a progressively more important issue. In many applications, it is extremely significant to verify the identity of a person that who claims to be. The traditional approach, the use of passwords and pins has increasingly endured from defects like forgotten or easily guessed passwords. Biometric is the trustworthy indicator to recognize the individual than the traditional systems like password and PINs. It comprises fingerprints, iris, retina scans, voice, gait, hand, face, ear geometry, hand vein, nail bed recognition, signature recognition, DNA and palm print etc. to establish identity[1]. The unimodal biometric system faces the dangerous issues in secure the templates from the various critical issues in the unimodal biometric system is protecting the templates from various risks [6]. The issues can be solved by combining two different unimodal biometric systems. Template security is essential to protect both the confidentiality of the users and the unity of the biometric systems.

Multimodal biometrics has recently attracted significant interest for its high performance in biometric recognition system [9]. Due to the integration of multiple independent features, these systems are expected to be more reliable and it has been universally applied for person authentication and verification. Multibiometric systems present numerous advantages such as improving the accuracy of the biometric recognition, population coverage increased, provide greater security, more flexibility, and user convenience. A multibiometric system put together different modality of a person on the same system.

Face and ear traits are passive and non-intrusive unlike fingerprint and signatures [8]. The high accuracy of the system is identified in real time under various conditions. Ear biometrics has become a popular biometric feature, provides better biometric performance because of uniqueness, permanence and unaffected by aging. Multimodal biometric is capable to combine dissimilar unimodal biometric verification, and exploits of the merits of all types of unimodal biometrics to extend the performance of the system to attain a more robust system [7].

II. LITERATURE REVIEW

Single modal biometric systems encounter a variety of security problems and present sometimes unbearable error rates. Multimodal biometrics provides high recognition accuracy and population coverage by combining different biometric sources. The multimodal biometric systems propose considerably grant higher security in distinction to unimodal and fewer exposed to assail. Some of the approaches have been presented below:

Ajay Kumar et.al [3] investigated a new approach to achieve performance improvement for the hand-based biometric measurement systems by incorporating user quality during the matching stage. Fusion of palm print and hand geometry performance is estimated on the assurance of producing a reliable matching score from the user templates.

Norman Poh et.al [10] presented the methodological approach drawing on a Bayesian framework (with explicit graphical representations). Identified two primary roles quality measures play: 1) as auxiliary measurements or 2) as control parameters. Describes two types of quality-based fusion algorithms: feature-based and cluster-based. Several variants of the cluster-based approach are distinguished, depending on the state of clusters: observable, hidden, or changing (from observable to hidden). In the proposed framework, each formulation can be implemented using either a generative or a discriminative classifier.

Aglika Gyaourova et.al [2] suggested a method for generating fixed-length codes for indexing biometric databases. An index code is constructed by computing match

scores between a biometric image and a fixed set of reference images. Candidate identities are retrieved based on the similarity between the index code of the probe image and those of the identities in the database. The proposed technique can be easily extended to retrieve pertinent identities from multimodal databases.

III. PROPOSED METHOD

Multibiometric systems are widely applied in large-scale biometric applications and template may be modified by the attackers [11]. To deal with this issue, in this paper we propose multibiometric cryptosystem to secure multibiometric template. Figure 1 shows the Multibiometric cryptosystem. Biometric cryptosystem merges biometrics and cryptography to promote from the strength of both fields [5]. Figure 2 presents the proposed schematic diagram of the multimodal recognition system. Input face and ear image are preprocessed using the Gaussian filter to reduce or eliminates the noise and shadow. Face and ear shape feature are extracted by employing a modified region growing algorithm, and the texture feature extracted by LGXP method. Both these shape and texture features will extract the distinctiveness of the images.

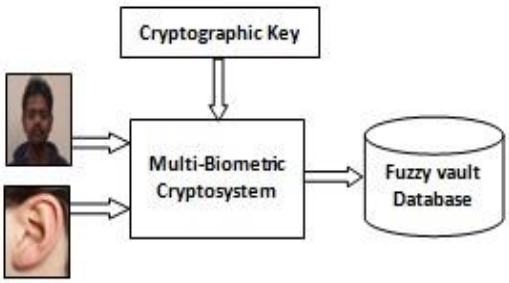

Fig.1. Multibiometric cryptosystem

Multibiometric cryptosystem generates cryptographic keys from the multibiometric face and ear features. The biometric template is effectively encoded with a secret key for enrolled template protection. During authentication, the protected template is decoded and thus recovers the secret key as well as the enrolled biometric template. The chaff points will be used to sketch out the feature points in the multibiometric template. The multi-biometric template feature set and the input key are applied to produce the fuzzy vault. For decoding, the multibiometric feature set and the stored fuzzy vault are combined to produce the secret key. The proposed method includes the three processes, they are

1. Image Preprocessing
2. Feature Extraction, and
3. Fuzzy Vault Generation phase

A. Image Pre-Processing

Image preprocessing involves removing low-frequency background noise, reflections, masking portion of images and standardize the intensity of the individual particles images. Face and ear images are cropped, and colored images are then converted to the grayscale images. The Gaussian filter is employed for noise suppression to smooth out the noise and also to convert the signal less fuzzy. Gaussian filter technique enhances the data images prior to computational processing with edge detection; it reduces edge position displacement, phantom edges, and edge vanishing.

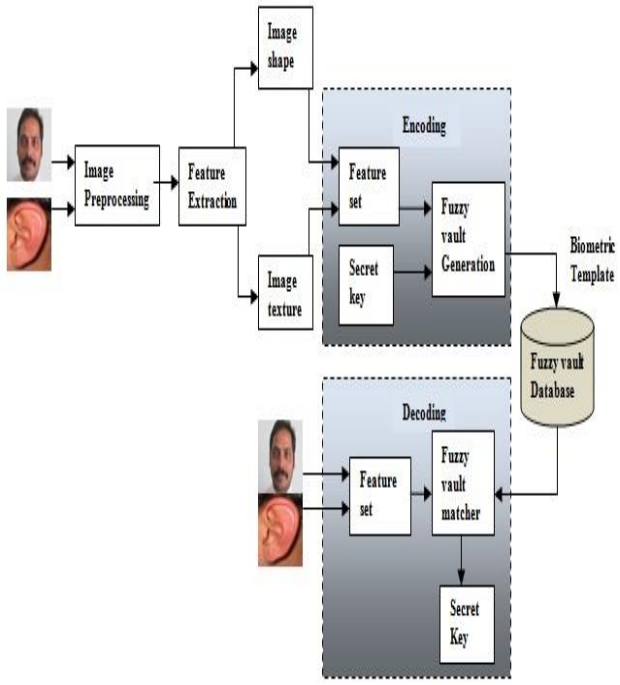

Fig. 2. Schematic diagram of the proposed model

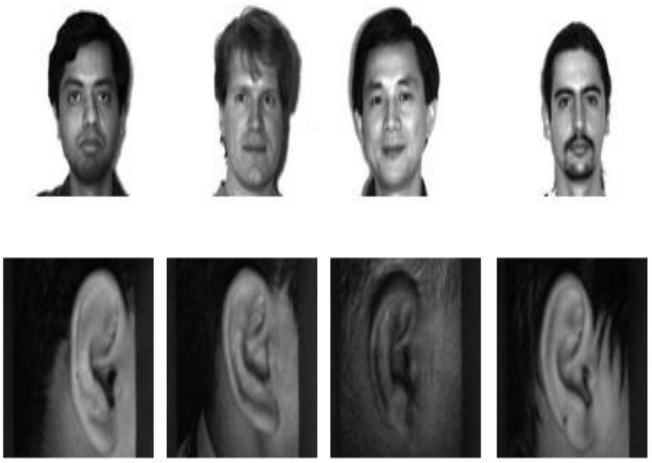

Fig. 3. Sample face and ear images

B. Feature Extraction

The shape and texture features of the grayscale image are extracted. In image segmentation, shapes of the face and ear object is segmented by using a modified region growing algorithm. LGXP method is applied to extract the texture of the images.

a) Modified Region growing Algorithm: Modified region growing method involves the selection of the seed points in the pixel-based image segmentation. In this method, the intensity threshold and the orientation threshold of the image are considered for region growing process. The shape of the image is segmented efficiently and more information can be obtained.

The gray scale image is partitioned into several smaller grid images. The exact location of the grid initial seed point is selected; it visits and determines the neighbor pixel to be added to the region. Constraints of the modified region growing are the "intensity" and the "orientation" of the image.

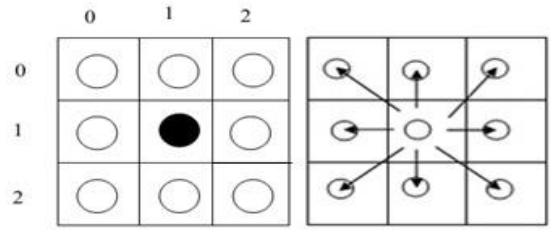

Fig. 4. Representation of the initial seed point and the neighboring pixel

b) LGXP Technique: The texture of the images is extracted with the LGXP method. The face and ear images were given to the Gabor filter. Gabor features have been known to be effective face recognition. Gabor filters are bandpass used with different orientations, as all facial features are not present at the same orientation. Scaling is done at each orientation to get the maximum frequency information. In different quantized phases of the central pixels and each of its neighbor pixels is applied with LXP operator. The local patterns are formed by joining the consequential binary labels.

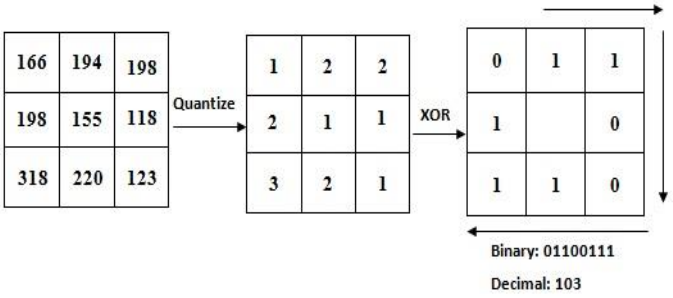

Fig. 5. Example of encoding method of LGXP quantize

C. Fuzzy Vault Generation Phase

Fuzzy vault approach is tolerant of intra-user variations in biometric data and this tolerance is determined by the error correcting capability of the associated codeword [4]. Fuzzy vault improves the security of the biometric template by the addition of secret key concept into the feature set. The Fuzzy vault generation phase consists of as follows

a) Fuzzy Vault Encoding: Fuzzy vault is a cryptographic construction, to use an unordered set A to lock a secret key K, yielding a vault V_A. During encoding, the vault is created applying polynomial evaluation and error correction. To hide the secret key K in the fuzzy vault, the secret key is divided into *(n+1)* parts and the parts become the coefficients of an *n* degree polynomial. The secret key K is encoded to construct the Polynomial P and all the elements of the unordered set A are to evaluate the Polynomial P. The polynomial for the secret key [4257] is shown in (1). The feature set of face and ear are concatenated to form the Lock matrix where the x and y-coordinates are stored. With this step, the polynomial can be discarded and now the secret key can only be recreated using this Lock matrix.

$$P(x) = 4x^3 + 2x^2+5x+7 \quad (1)$$

The feature set along with polynomial evaluations together with chaff point set C represents the vault.

$$V = A \cup C \quad (2)$$

Chaff points are a few extra random points included with the shape and texture features points. Chaff points are generated to cover the complete range of the fuzzy vault but not overlap with the Lock matrix coordinates. Combining the chaff points with the code matrix coordinates forms the fuzzy vault. The genuine point's positions are hidden from the attacker by the combination of the chaff points. The number of secret key points produced is dependent on the number of digits. The fuzzy vault matrix is the secure template that is stored in the biometric fuzzy vault database.

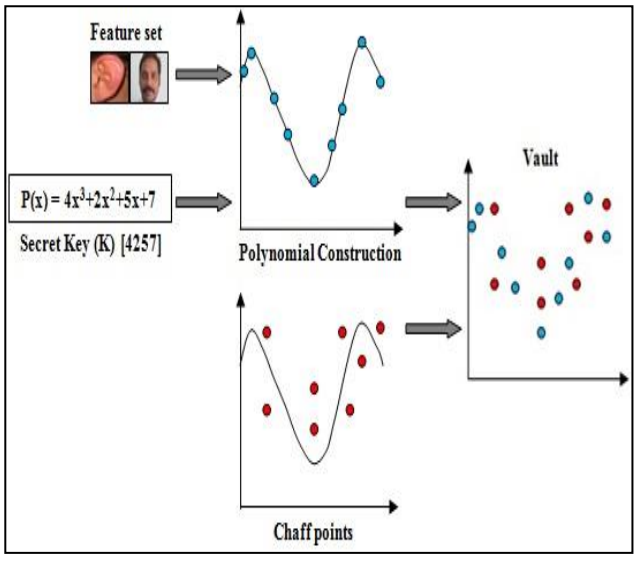

Fig. 6. Fuzzy Vault Encoder

Fuzzy Vault Decoding: During decoding, the fuzzy vault is unlocked with another unordered set B. The fuzzy vault V is compared with the biometric query feature set B. The feature set collected from the query image may not have the exact same coordinates as the values within the vault. Therefore, the nearest neighbor of the feature set must be found and it separates a sufficient number of points from the vault. A new set of x-coordinates are used for subsequent procedures while the previous set of values from the feature set is discarded. The equivalent y-coordinate value can also be read from the fuzzy vault matrix to form unlock matrix. Polynomial interpolation is used to reconstruct query image polynomial based on the unlock matrix. Polynomial decoding is performed where all the coefficients of the polynomial are concatenated to re-form the secret Key K. Secret key K obtains only if B overlap substantially over A, or else the authentication will not pass. The polynomial reconstruction impossibility and the amount of chaff points applied in the system shows it's secure.

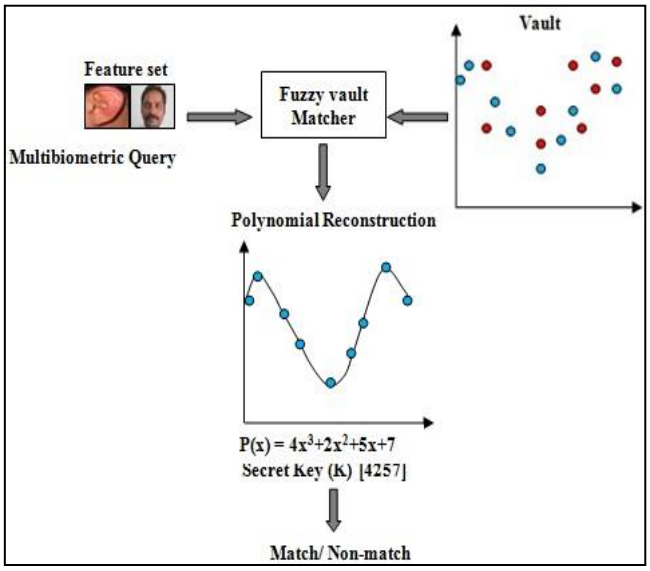

Fig. 7. Fuzzy vault decoder

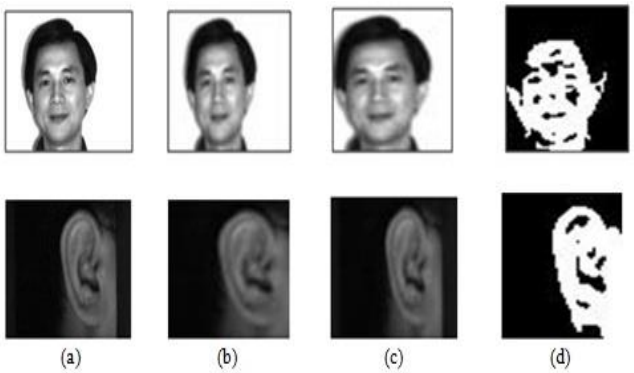

Fig. 8. Images output at various stages. (a) Input images(b) Filter image (c) cropped image (d) Shape extracted image.

IV. Experiment Result and Discussion

After The proposed method was executed with the Yale Face Database which contains 165 gray scale images of 15 individuals, and IIT Delhi ear image database which contains 121 individuals and has three ear images of each. The experiment has been conducted with 15 face and ear images. The performance of the proposed system was evaluated using the False Matching Rate (FMR), False Non-Matching Rate (FNMR), and Genuine Acceptance Rate (GAR). The evaluation is through the presence of noise, the absence of noise, and by varying the secret key size.

A. False Matching Rate (FMR)

The probability that the system wrongly matches the input sample to a non-matching pattern in the database. It measures the percent of invalid inputs which are erroneously accepted.

$$FMR = \frac{Invalid\ inputs\ which\ are\ incorrectly\ accepted}{Total\ number\ of\ inputs} \quad (3)$$

B. False Non-Matching Rate (FNMR)

The probability that the system unsuccessful to detect a match between the input sample and a matching pattern in the database. It measures the percent of valid inputs which are incorrectly rejected.

$$FNMR = \frac{Invalid\ inputs\ which\ are\ incorrectly\ rejected}{Total\ number\ of\ inputs} \quad (4)$$

C. Genuine Acceptance Rate (GAR)

GAR is the evaluation of the performance that correctly classified the genuine sample as genuine

$$GAR = 1 - FNMR \quad (5)$$

The face and ear images at the various stages of execution are shown in this section. In figure 8, A represents the input image, B represents the filtered image, C represents the cropped image and D represents the shape extracted image. The proposed method results are also compared to the existing method artificial neural network. It acquires high GAR and low FNR vaules with irrespective of secret key and noise. The performances are analyzed to the ANN and it shows the efficiency and constancy of the proposed method.

TABLE I. Evalution metrics obtained without noise

Secret Key Size	ANN		Proposed Method	
	FMR	GAR	FMR	GAR
1	20%	80%	15%	85%
2	20%	80%	15%	85%
3	20%	80%	15%	85%
4	20%	80%	15%	85%

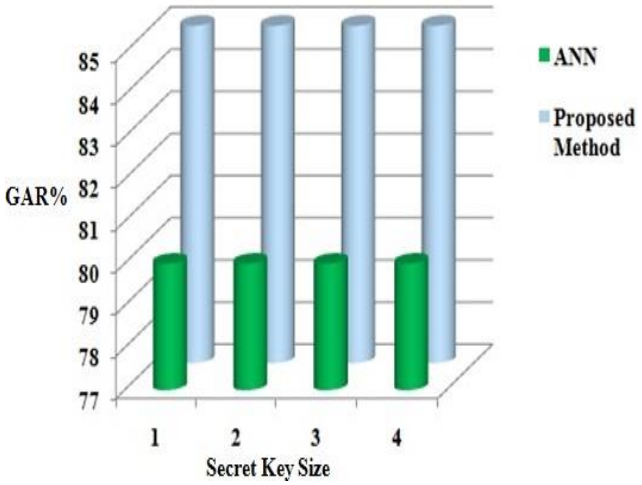

Fig. 9. GAR values without noise

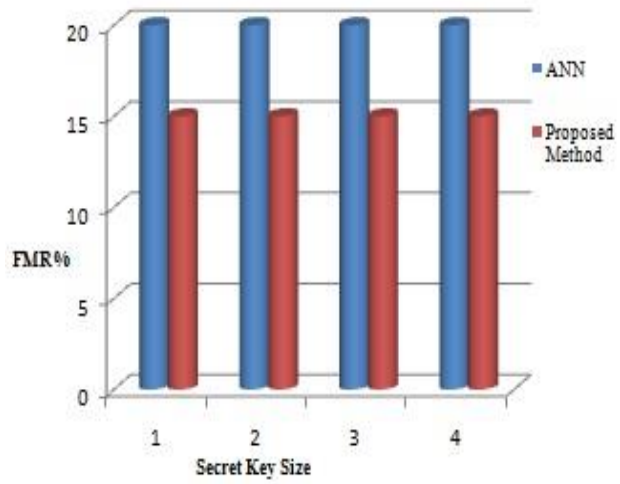

Fig. 10. FMR values without noise

TABLE II. EVALUTION METRICS OBTAINED UNDER NOISE

Secret Key Size	ANN		Proposed Method	
	FMR	GAR	FMR	GAR
1	35%	65%	30%	70%
2	35%	65%	30%	70%
3	35%	65%	30%	70%
4	35%	65%	30%	70%

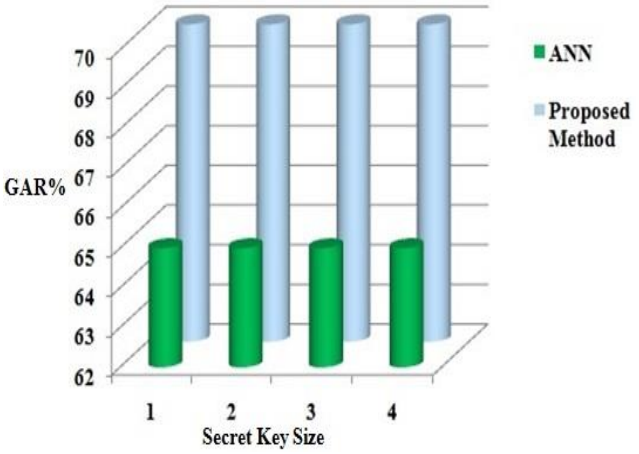

Fig. 11. GAR values under noise

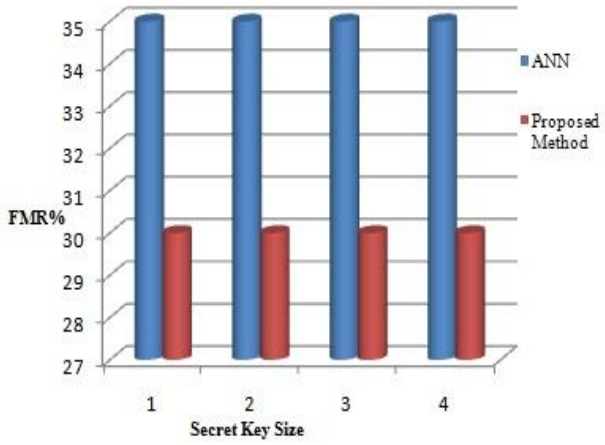

Fig. 12. FMR values under noise

V. SUMMARY AND FUTURE WORK

Unimodal biometric systems are subjected to a variety of attacks and not good enough to provide security, diversity, and revocability to biometric templates. In this paper, multimodal biometric face and ear are suggested and the proposed method is given. Modified region growing algorithm and LGXP algorithm are employed to extract the shape and texture of the input image. The proposed method presented here provides precision and security to the multibiometric template with the cryptosystem based on fuzzy vault. Fuzzy vault is constructed with the encoding and decoding secret key. The performance of the system is measured with FMR, FNMR, and GAR. The experimental result shows the accuracy of the face and ear biometric recognition and template security.

The available biometric template protection schemes are not yet effectively established for a large-scale operation, there is a tendency to store more information in the template. This increase the risks associated with template maltreatment. The issue of template security and reliability are considered and further research is conducted in this direction.

REFERENCES

[1] A. K. Jain, A. Ross and S. Prabhakar, "An introduction to biometric recognition". IEEE Transactions on Circuits and Systems for Video Technology, 2004, Vol. 14, pp. 4–20.

[2] Aglika Gyaourova and Arun Ross, " Index codes for multibiometric pattern retrieval", IEEE Transactions on information forensics and security, Vol 7, No. 2, PP 518-529, April 2012.

[3] Ajay Kumar and David Zhang, "Improving Biometric Authentication Performance From the User Quality", IEEE Transactions on instrumentation and measurement, Vol. 59, No. 3, PP 730 -735, March 2010.

[4] Anil K. Jain, KarthikNandakumar, and Abhishek Nagar, "Biometric Template Security", EURASIP Journal on Advances in Signal Processing, Vol. 2008, pp. 1-23.

[5] R Christian Rathgeb and Andreas Uhl," A survey on biometric cryptosystems andcancelable biometrics", EURASIP Journal on Information Security, Vol.3, 2011,pp. 1-25.

[6] Gandhimathi. A, Radhamani.G, " A multimodal Approach for Face and Ear Biometric System", International Journal of Computer Science Issues, Vol. 10, Issue 5, No 2, September 2013, pp.234-241.

[7] JuCheng Yang, "Biometrics Verification Techniques Combing with Digital Signature for Multimodal Biometrics Payment System", In proc. of IEEE International Conference on Management of e-Commerce and e-Government, pp. 405 - 410, 2010.

[8] M. Turk and A. Pentland, "Eigenfaces for recognition", Journal of Cognitive Neuroscience, 1991,Vol.3(1), pp.71-86.

[9] M.I. Ahmad, W.L. Woo and S.S. Dlay, "Multimodal Biometric Fusion at Feature Level: Face and Palm print", In proc. of the 7th International Symposium on Communication Systems Networks and Digital Signal Processing (CSNDSP), pp. 801 - 805, 2010.

[10] Norman Poh, and Josef Kittler, " A Unified Framework for Biometric Expert Fusion Incorporating Quality Measures", IEEE Transactions on pattern analysis and machine intelligence, Vol 34, No.1, PP. 3-18, January 2012.

[11] UmutUludag, SharathPankanti, SalilPrabhakar, and Anil K. Jain, "Biometric Cryptosystems: Issues and Challenges", Proceedings of the IEEE, Vol.92, No. 6, June 2004, pp. 948-960.