International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9 Issue-2, December 2019

Cryptographic Algorithm based Feature Level Fusion of Fingerprint and Iris in a Multi-Biometric Recognition System

Jayapriya , Umamaheswari K

Abstract*: Biometric encryption is one of the developing exploration area, which is a strategy for merging biometric features with cryptographic keys. Biometric Recognition is based on the anatomical and behavior attributes of the individuals. Multibiometric is the combination of various biometrics like Fingerprint, Iris, and Face, Fingervein etc. Experts are concentrating on the most proficient method to give security to the framework, the template which was produced from the biometric should be ensured. The main objective of this paper is to protect the multi biometric template by creating a protected sketch by deploying bio cryptosystem. Once the biometric template is stolen it turns into a major issue for the security of the framework and furthermore for client protection. In this way, a bio-crypto framework ensures the confidentiality of the information. In this paper bio cryptosystem is proposed to improve the security of multimodal frameworks by producing the biocrypto key from Finger print and iris. Gray level co-occurrence matrix (GLCM) based Haralick features, local binary pattern (LBP), triplet half-band filter bank (THFB) and dynamic features (DF) are extracted from fingerprint and iris. The high dimensionality space of the features are reduced using kernel principal component analysis (KPCA. Finally, the encoding process is matted with biometric key utilizing symmetric RSA (Rivest-Shamir-Adleman) cryptographic algorithm.

Keywords: Multi biometric, recognition system, KPCA, RSA, Fusion, Feature extraction.

I. INTRODUCTION

In recent days securing the information is an unavoidable necessity. Biometric Technology has established that it has a serious issue in the field of security, get to control and checking the different applications as a result of its non-legitimate confirmation strategy [1]. Customary techniques like ID card, passwords can be effectively copied, lost or stolen. The traditional methods is an identity proof and if it is stolen it is accessible for unauthorized person.To overcome these issues, fusion of biometrics like fingerprints, iris, face, palmprint are done [2, 12]. Biometric attributes are easily accessible by unauthorized person. Subsequently, once a biometric data is stolen, fake can be created and the same biometric cannot be used again [3].

Revised Manuscript Received on December 30, 2019.
***** Correspondence Author
Jayapriya*, Department of Information Technology, PSG College of Technology, Anna university, India.
Umamaheswari K, Department of Information Technology, PSG College of Technology, Anna university, India.

In this manner, multi biometric techniques are favored so as to rise both security and accuracy.Multi-biometric frameworks improve security perspective just as it offer improved adaptation to non-critical failure emerging because of biological variables or the client conduct. Since the multi-biometric frameworks combine test information gathered from various sources, it considerably improves accuracy and performance of the framework [4]. It is amazingly difficult to imitation a multi-biometric framework as the spoofers should initially gather numerous biometric identifiers of an individual, which is a close inconceivable task [5]. Commotion in examined information is another enormous issue in uni-modular biometric frameworks that a multi-modular biometric framework can address. The biometric information is debased by commotion for the most part because of slight varieties in the biometric attribute itself or blemished securing conditions [6]. For instance, a unique finger impression picture with a scar or a voice test modified by virus is loud information. Whenever inspected information of a biometric identifier experiences commotion in a multi-biometric framework, the framework can use test information from other biometric identifier of the client [7]. In this way to conquer all the above key issues a multimodal biometrics technique is utilized a testing errand to consolidate different highlights from every methodology to create better recognition results.

Numerous examinations and calculations have been proposed for multimodal biometric combination. Past multimodal biometric frameworks dependent on face and iris recognition have utilized face and iris features [8, 9]. In any case, they face the downside of high exactness of iris recognition and the comfort of face recognition [10]. So as to exploit the recognition framework, it is basic to execute a decent strategy for combining distinctive wellsprings of biometric data [11, 12]. Hence in this paper we propose a multibiometrics cryptosystem with numerous element extraction strategies and encoded utilizing RSA (Rivest-Shamir-Adleman) algorithm for iris and unique finger impression. The paper is sorted out as pursues. An average report about the past writing is examined in Section 2, proposed multimodal biometric framework and distinctive preprocessing and extraction methods are delineated in Section 3. The section 4 and 5 outlines the reenactment result and ends are introduced in the last area of the paper.

II. LITERATURE SURVEY

A. Submission of the paper

In this area ongoing exploration works of the creators were portrayed.

The previous two decades have seen the improvement of an extensive number of biometric and multi biometric cryptosystems which was talked about for the acknowledgment of a person for security reason. Maneet Singh et al [13] have exhibited an outline of biometric combination with explicit spotlight on three inquiries: what to fusion, when to wire, and how to interlink. A complete survey of methods fusing auxiliary data in the biometric acknowledgment pipeline was additionally introduced. Here they talked about the consolidating (I) information quality in the biometric recognition pipeline; (ii) joining delicate biometric characteristics with essential biometric identifiers; (iii) using relevant data to improve biometric recognition exactness and (iv) performing nonstop validation utilizing auxiliary data. These Multi biometric frameworks use the rule of combination to consolidate data from various sources so as to improve acknowledgment exactness while tending to a portion of the restrictions of single biometric frameworks. At long last, a portion of the exploration challenges in biometric combination were identified.Sandip Kumar Singh Modak et.al [14] have contemplated on multibiometric (multimodal, multialgorithm, multi-test, multi-sensor and multi-occasion) combination methodology and its distinctive applications. Furthermore, they talked about the diverse strategy utilized in a combination procedure (Sensor, Feature, Score, Decision, Rank) of multibiometric frameworks from most recent three decades and looks at the techniques utilized, to investigate their victories and disappointment.AnilK.Jain et al. [15] have reported a significant advancement that has been accomplished in the field of biometric recognition in the previous 50 years. This advancement empowered the present best in class biometric framework to precisely perceive the people dependent on biometric characteristic obtained under controlled natural condition. There second target was to enroll the difficulties and break down the arrangements proposed to conquer them and feature the analysis openings in this field. One of the chief difficulties was to plan a strong calculations for representing and coordinating biometric tests acquired from uncooperative subjects under unconstrained ecological conditions(e.g., perceiving faces in a group). Also, central inquiries, for example, the peculiarity and diligence of biometric qualities need more prominent consideration. Issues identified with the security of biometric information and heartiness of the biometric framework against caricaturing and muddling assaults likewise stay unsolved. At long last, bigger framework level issues like convenience, client security concerns, coordination with the end application, and rate of profitability have not been sufficiently tended to. Opening the maximum capacity of biometrics through between disciplinary research in the above territories won't just prompt broad selection of this promising innovation, however will likewise result in more extensive client acknowledgment and societal effect.Ajita Rattani et al [16] have dragged in huge consideration on Face biometrics technology for secure access to cell phones. This is on the grounds that practically all cell phones have RGB cameras appropriate for catching countenances, and the required client association was worthy given the notoriety of selfies. The majority of the conventional techniques for face biometrics may not be managable to local execution on versatile equipment because of their constrained memory and registering power. Thus, various calculations explicitly planned or adjusted to the versatile condition have been proposed for face biometrics. Nonetheless, the best in class identified with face biometrics in a versatile situation was not outstanding. The paper altogether and basically studies face biometrics regarding face identification and standardization, acknowledgment, and hostile to mocking techniques proposed for cell phones. The general point was to improve understanding and talk about the favorable circumstances and confinements of the current strategies. Further, difficulties and future research bearings are recognized for further innovative work.TimVanhamme et al. [17] have tended to the security chance brought about by these choice combination plans making invalid suspicions, for example, a fixed likelihood of (in) right acknowledgment and a fleeting consistency of behaviometrics. To relieve this hazard, the paper displays a formal trust show that drives the behaviometrics decision and piece. Our trust show embraces a half and half methodology consolidating arrangement and notoriety based learning portrayal systems. Our model and structure externalizes trust learning from the confirmation rationale to accomplish inexactly coupled trust the board, and formalizes this information in depiction rationale to reason upon and merchant complex circulated trust connections to settle on hazard versatile choices for multi-modular verification. The assessment of our verification of-idea outlines a worthy act overhead while lifting the weight of manual trust and behaviometric the board for multi-modular confirmation Rajkumar Saini et al [18] have proposed a novel multimodal client distinguishing proof and check conspire joining two between connected biometric qualities. Mounding manually written strokes for mark invigorates EEG motions in the cerebrum.

The reaction of the mind signals amid marking was exceptional for every client and this cerebrum flag signature connection was used in the proposed plan. To the best of our insight, there exists no confirmation approach joining these two between connected biometric characteristics. The proposed multimodal plot utilizes Hidden Markov Model (HMM) based consecutive classifier to demonstrate highlights removed from marks and EEG flags independently. Pyramid Histogram of Orientation Gradients (PHOG) highlights are extricated from the mark pictures and next PHOG highlights are utilized to manufacture client explicit mark HMM models. At long last, a score consolidating grouping scores of mark HMM and EEG-HMM models is utilized to perform client distinguishing proof and check. To assess the viability of the proposed plan, we have built up a dataset gathering these two attributes all the while utilizing the Emo tiv Epoc+ gadget and pen-paper for 70 singular subjects. From that point, client's recognizable proof is performed with people's mark and EEG motions just as their joined attributes. The ID exactness of the proposed multimodal approach has been accomplished upto 98.24%. The adequacy of the check conspire was approved Meriem Dorsaf Bounneche et al [19] have proposed a coding-based methodology utilizing multi-phantom palm print pictures are alluring inferable from their high acknowledgment rates. Intending to additionally improve the execution of these methodologies, the paper introduces a novel multi-otherworldly palmprint acknowledgment approach dependent on situated multiscale log-Gabor channels.

The proposed strategy intends to improve the acknowledgment exhibitions by proposing novel arrangements at three phases of the acknowledgment procedure. Propelled by the bitwise aggressive coding, the element extraction utilizes a multi-goals log-Gabor sifting where the last element map was created by the triumphant codes of the most reduced channels' bank reaction. The coordinating procedure utilizes a bitwise Hamming separation and Kullback-Leibler dissimilarity as novel measurements to empower an effective catch of the intra-and between likenesses between palmprint highlight maps. At last, the choice stage was conveyed utilizing a combination of the scores produced from of various unearthly groups to decrease covering. Moreover, a combination of the element maps through two proposed novel element combination procedures to enable us to dispense with the natural excess of the highlights of neighboring unearthly groups was likewise proposed. The test results got utilizing the multi-ghostly palmprint database MS-PolyU have demonstrated that the proposed strategy accomplishes high exactness in mono-otherworldly and multi-ghastly acknowledgment exhibitions for both confirmation and distinguishing proof modes; and furthermore beats the best in class techniques.
Hadi Habibzadeh et al [20] have displayed a concise planar review of savvy city framework design by presenting the application, detecting, correspondence, information, and security/protection planes. Fitting existing correspondence conventions and frameworks to connect enormously conveyed sensors and information handling/stockpiling assets presents special correspondence challenges for savvy urban areas. Moreover, concurrence, reconciliation, and control of committed and non-devoted sensors was a fabulous test while IoT sensors ceaselessly drive tangible information through the correspondence medium towards information handling and examination planes. While inescapability and universality of brilliant city administrations were guaranteed by the connection of correspondence and detecting advances, their heartiness and versatility call for modified security and protection arrangements. In view of these, we center on detecting/activation, correspondence, and security planes of a savvy city framework and present an extensive study of the difficulties and best in class arrangements in each plane. Moreover, we give bits of knowledge to open issues and openings in these planes.

III. PROPOSED MULTI-BIOMETRIC CRYPTOGRAPHIC RECOGNITION SYSTEM

Multimodal Biometric framework utilizes numerous reliant or pitifully related biometric templates from a person, for instance, Fingerprint and retina of a similar individual, or fingerprints from two distinct fingers of an individual. Multi-biometric cryptosystems are arranged into two dependent on fusion modes

- Biometric level fusion,
- Cryptographic level fusion

The biometric level fusion is the fusion associated at the feature level and the fusion associated at the decision level is known as cryptographic level fusion. Here, we intend propose a feature level system to all the while secure different layouts of a client utilizing biometric cryptosystems. To demonstrate the viability of this framework shown in fig.1, the entire procedure of the proposed check framework can be isolated in to five stages. These steps are depicted in the accompanying segments
Step 1: Input as Fingerprint and iris image
Step 2: Perform preprocessing and extract the feature for fingerprint and iris image
Step 3: Minutiae features were extracted for feature enhancement
Step 4: Reduction of extracted features using kernel principal component analysis (KPCA)
Step 5: Fusion process
Step 6: Apply encryption and utilize cryptographic algorithm for the templates
Step 7: Decryption for the templates
Step 8: Compare the generated template with template available in the database.
Step 9: Verification process
Step 10: Final decision, if it is matched then the user is allowed otherwise will be rejected.

A. Acquisition process

The acquisition process is totally fundamental in a Multi-biometric confirmation framework, here instead of execution, it is supplanted by a trivial database of images, and this database comprises of unique finger impression and iris pictures from numerous subjects.

B. Preprocessing

The fingerprint and iris image is first preprocessed by using the following methods,

- Gray scale conversion,
- Gaussian Filtering
- Gamma Intensity Correction (GIC) and
- Histogram Equalization (HE)

These methods were associated to the input picture, to lessen data misfortune in the image so as to improve its appropriateness for ensuing system performance.

- **Gray Scale Conversion**

The gray-scale image contains every one of the sensitivities of data; it is less demanding to get it. This procedure of color transformation incorporates adding color to the gray scale pictures utilizing reference picture alone. Contingent upon the reference picture taken, the output picture is colorized. At first, the gray scale pictures transformation method check whether the original picture is a gray scale picture or not. In the event that it is a color picture, at that point it ought to be changed over into a grey scale picture. The source picture which is taken for reference is bought to be a color picture. At that point the extent of the original picture and the source picture ought to be taken to change over it into color space. Next the standardization procedure is done and lastly luminance is analyzed. In the wake of looking at the luminance the coloring mind-set is taken from the source picture and added in like manner to the original picture to frame the goal picture

- **Histogram Equalization**

Histogram equalization is to extend the pixel esteem dispersion of a picture in order to expand the perceptional data.

The histogram equalization out possesses all the range from 0 to 255 and the perception impact is upgraded. It is a graphical portrayal of the standardized number of pixels versus different estimations of intensity of image. It is a nonlinear transformation that adjusts brightness of the picture giving a high contrast picture which is outwardly recognizable from the original picture.

- **Gaussian Filtering**

This linear filter is generally used to obscure the picture or to diminish noise. The Gaussian filter in equation 1 alone will obscure edges and lessen contrast. The principle destinations of the filters are to improve the nature of picture by upgrading is to improve interoperability of the data present in the pictures for human visual. The Gaussian function is represented as

$$G(x) = \frac{1}{\sqrt{2\Pi\sigma^2}} e^{\frac{-x^2}{2\sigma^2}} \quad (1)$$

Where, σ is the standard deviation of the distribution. The dispersion is expected to have a mean of 0. This filter constricts the variety of light force in the area of a pixel. It smoothen the general state of the picture.

- **Gamma Intensity Correction (GIC)**

The Gamma Intensity Correction (GIC) in equation 2 redresses the general splendor of picture to a pre-characterized sanctioned picture. Consequently the impact of differing lighting is debilitated and it upgrades the finger print and iris features.

$$I_{xy} = G(I_{xy}; \gamma) \quad (2)$$

Where, the γ represents the degree of brightness, by changing the gamma parameter the general brightness of a picture can be controlled.

C. Feature Extraction

- **Fingerprint**

There are numerous varieties in finger situation and pressure applied on the sensor, here initially an sample feature has been chosen and afterward it is changed over into grey scale then surface features has been separated. For better feature extraction Minutia-based algorithm is utilized and it analyze a few minutia focuses (edge consummation, bifurcation, and short edge) extricated from the original picture put away in a layout with those separated from a optimistic finger impression. The minutia focuses extracted from the template and query fingerprints must be adjusted, or enrolled before coordinating.

- **Iris**

The iris is the annular area of the human eye limited by the pupil and the white of the eye (Sclera) on either side. The mind boggling iris surface conveys interesting data valuable for individual recognizable proof. At that point template generation is finished by utilizing various strategies.

The techniques used for fingerprint and iris template generation of feature extraction are as follows

- Gray level co-occurrence matrix (GLCM)
- Local binary pattern (LBP),
- Triplet half-band filter bank (THFB) and
- Dynamic features (DF).

These filter result gives two outcomes, at that point we analyze these two outcomes and greatest directional features are observed as the final template. This template is the contrasted and template of the input picture. On the off chance, that includes feature count check is less, at that point the picture does not coordinate, and if feature count is high the individual is distinguished compared with remaining samples.

- **Gray level co-occurrence matrix (GLCM)**

A co-occurrence matrix is a framework that is characterized over a picture to be the distribution of co-occurrence pixel esteems (dark scale esteems, or shades) at a given counterbalance.

- **Local binary pattern (LBP)**

LBP is the specific instance of the Texture Spectrum model has since been observed to be an amazing feature for texture classification; it improves the detection execution impressively on some datasets. Local Binary Pattern (LBP) is a straightforward yet extremely effective texture administrator which names the pixels of a picture by thresholding the area of every pixel and thinks about the outcome as a binary number.

- **Triplet half-band filter bank (THFB)**

This filter removes successful and minimized iris features and an adaptable post-classifier in order to deal with conceivable ancient rarities particularly segment error like incorrect identification of inward and external limits of iris and unique finger impression, impediment of eyelids/eyelashes, reflection on iris, shadow of upper/lower eyelid on iris, non-linear distortion, and so forth.

- **Dynamic features**

The spatial control of the filter coefficients can't be all around safeguarded. It can majorly affect the state of the output signal which can prompt reduction the texture discrimination capacity. In this way, DF extraction assumes an imperative job for finger print and iris feature extraction. The feature extracted within pupil contraction and dilation can be utilized proficiently in biometric recognition by utilizing the human iris. We examined these features one by one to check the separation potential among various divided unique finger impression and irises.

D. Kernel principal component analysis (KPCA)

The features extracted utilizing the above strategies will have high dimensionality, which will build up the calculation time of the multi biometric framework. So to decrease the dimensionality of the separated features we make utilization of KPCA [21] method. Kernel PCA (KPCA) is one of the productive and as often as possible strategy and the motivation behind KPCA is to decrease the substantial dimensionality of the extracted features to the smaller inherent dimensionality of feature space, which are expected to depict the information economically.

By arranging of minor parts, the KPCA viably lessens the quantity of features and shows the feature data set in a low dimensional subspace.

Step 1: Find the mean value of the extracted features in the dataset

Step 2: Form a matrix by reducing the mean value from the dataset
Step 3: Apply transpose to the obtained matrix to form a covariance matrix
Step 4: Calculate Eigen vectors for the covariance matrix
Step 5: Finally low dimensionality data set is obtained from the largest Eigen vectors

E. Fusion at the Feature Extraction Level

The Feature Extraction Level fusion is difficult since connection between features was not known and fundamentally contradictory features are normal and the scourge of dimensionality. The data extricated from wellsprings of various modalities is put away in vectors based on their methodology. These feature vectors are then consolidated to make a joint component vector which is the reason for the matching and recognition process. Coordinating execution of a biometric framework is estimated with the assistance of false acceptance rate (FAR) and false rejection rate (FRR).

F. Encryption based on RSA

Here, the features of finger print and iris are melded and encoded during verification process utilizing a standard encryption algorithm. Here, the templates are scrambled and secured utilizing a conventional RSA (Rivest-Shamir-Adleman) cryptographic calculation utilized for encoding the pictures. It gives better security because of expense of figuring substantial numbers. The steps included in RSA algorithm are,
Step 1: Key generation
Step 2: Cipher text using public key (to lock) is produced by encrypting the plain text
Step 3: In order to obtain plain text using private key (to open) cipher text is decrypted

G. Decision

At this stage the multi biometric cryptosystem finishes every one of the procedures of feature extraction, matching and recognition. Choices are made by utilizing Boolean functions. The recognition output is the major choice among every single present subsystem. In this stage, the fused single vector is compared and the vector which is put away in the database and key is generated. On the off chance that the key which isn't open matches, at that point the client is legitimate or it is chosen that client is invalid

IV. RESULT AND DISCUSSION

The proposed technique displayed here gives security to the disseminated framework and feature level fusion framework simulation outcome is described here in this section. Execution of the multi biometric crypto frameworks is estimated by their accuracy in person ID. The proposed methods utilized for preprocessing, feature extraction and encryption/decoding referenced in paper has been tried on 25 pictures stored in database. The performance of proposed method has been assessed regarding false acceptance rate (FAR) and false rejection rate (FRR). The FRR and FAR is characterized as a rate of authentic clients dismissed and acknowledged by the biometric framework and this has been demonstrated in table 1 and accuracy is determined for iris, finger print recognition and for both.

Table 1: Performance evaluation

Accuracy in %		FAR (False acceptance rate in %)	FRR (False rejection rate in %)
Finger print recognition	90.1%	1.12	8.94
Iris Recognition	91.5%	0.25	0.34
Multi biometric Crypto system	97.33%	0.11	0.15

False Acceptance rate is the likelihood that the framework mistakenly approves a non-approved individual, due to inaccurately coordinating the biometric contribution with a template. The FAR and FRR are typically expressed in percentage, following the FAR definition is that the level of invalid sources of information which are erroneously acknowledged. The False Rejection Rate is the likelihood that the framework mistakenly rejects access to an approved individual, because of neglecting to coordinate the biometric contribution with a format. The FRR definition this is the level of substantial information sources which are erroneously dismissed. FAR and FRR are especially very much subjected to the biometric factor.

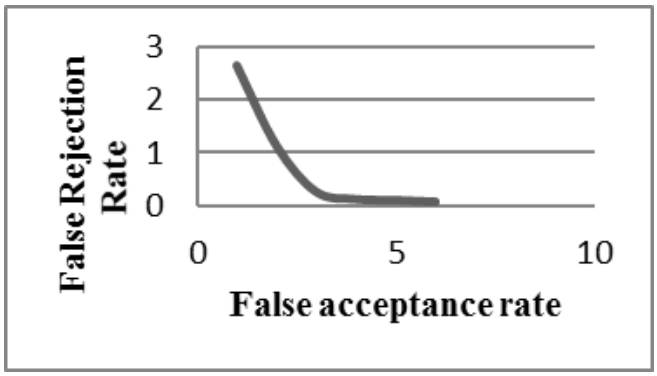

Fig 2: FRR Vs FAR

FRR may increment because of natural conditions or wrong use, for instance when utilizing grimy fingers on a finger print reader. Generally the FRR brings down when a client acquires involvement in how to utilize the biometric gadget or programming. At the point when biometrics is utilized for consistent or physical access control, the target of the application is to deny access to unapproved people under all conditions. Obviously an extremely low FAR is required for such an application as portrayed in the above table and fig 2. For the false acceptance rate of 0.25 which is low and have the false rejection rate of about 0.34.And FRR expanding quickly than FAR, which does not influence the finger impression and iris recognition.

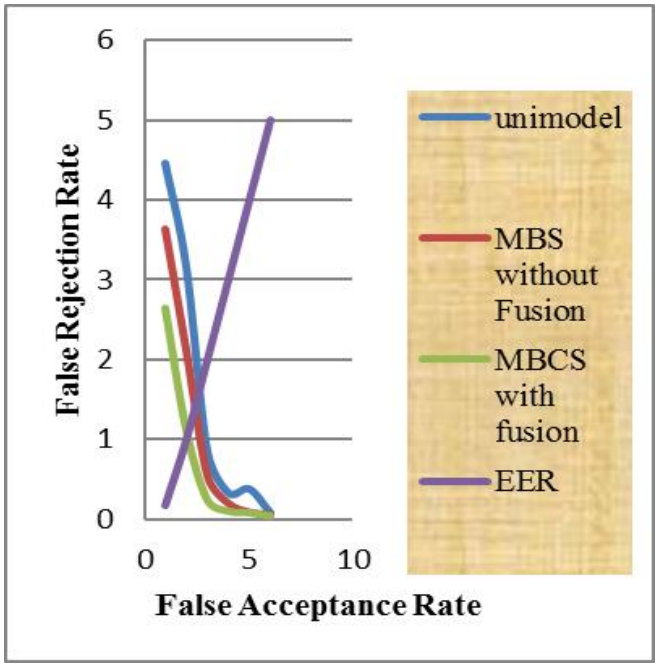

Fig 3: Comparative performance analysis

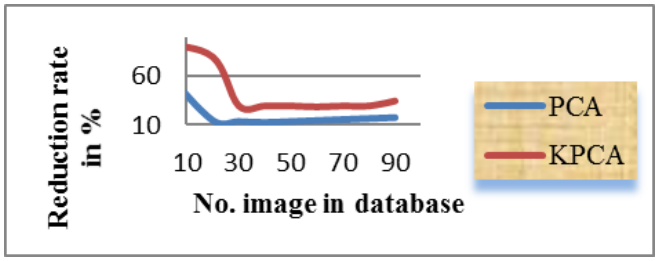

Fig 4: Performance evaluation of KPCA with PCA

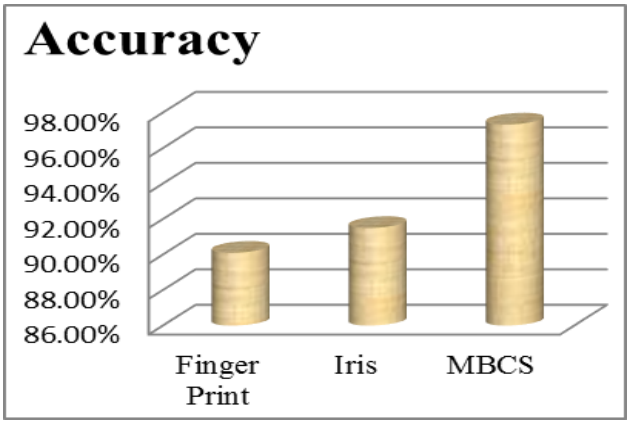

Fig 5: Accuracy analysis of Multi biometric crypto system (MBCS

In fig 3, our proposed work is compared with the existing unimodel biometric and multimodal biometric system without fusion. The proposed work in shows the better FRR vs FAR as depicted above in the table 1. Superimposing the equal error rate (EER) guide, comparing to the point where the FAR is equivalent to the FRR, it relates to EER is of about 0.18%. In fig 4the performance evaluation rate of PCA and KPCA is done, the results indicate that recognition rate achieves 93% while images in the dataset are used as the training sample. If the testing samples are increased, the recognition rate will improve, but the training time will be also greatly extended. In order to establish the person's identity with a high degree of reliability, the accuracy of our proposed multi biometric crypto system is shown in fig 5. The accuracy of the finger print is of about 90.1 %, iris is of about 91.5 % and our proposed work shows the accuracy level of about 97.33%.However, our experimental results show that our feature level fusion based cryptographic algorithm outperforms and has every low average errors with high accuracy and standard acceptance and rejection rate

V. CONCLUSION

Biometrics assessment reports and other autonomous examinations show that the execution of numerous conditions of Finger print and iris recognition techniques falls apart with changes in lighting, pose, and different elements. With biometric fusion at extraction, both sheltered and elite outcomes can be accomplished. Multi biometric frameworks consolidate the data introduced by multi biometric sensors, calculations and tests so as to build up the identity of a person. In this work we check the effectiveness of the multimodal biometric framework. Here, various systems based features are separated for Iris and unique finger impression. Here feature extraction level fusion is utilized in multimodal framework after minutia extracted features and the dimensionality of the extracted features were reduced using KPCA. The exactness of given framework is 97.33% for multimodal framework with a database of 25 pictures. This implies a multimodal biometric framework works effectively than unimodal framework. The Feature level fusion have the issue of extensive dimensionality of feature, which prompts the excess data and inconsequential information, Therefore future works could go toward utilizing increasingly powerful strategies against these downsides and half breed combination level can be utilized. Likewise, the framework ought to be tried on a bigger database with noisy samples to esteem the power of the multi biometric model.

REFERENCES

1. Sheena and Sheena Mathew, "Multimodal Biometric Authentication: Secured Encryption of IRIS using Fingerprint ID", International Journal on Cryptography and Information Security (IJCIS), Vol. 6, No. 3/4, pp. 39-46, 2016
2. P. Subramanian, K. Nithin krishna, Rinku Marya Sebastian and Najeeb ur Rahman,"Multibiometric Systems ", International Journal on Chemical Science, Vol. 14, No.3, pp. 805-808, 2016
3. O. Kurban, T. Yildirim and A. Bilgic, "A multi-biometric recognition system based on deep features of face and gesture energy image", IEEE International Conference on Innovations in Intelligent systems and Applications (INISTA), pp. 1-4, 2017.
4. A. Jain and A. Ross, "Multibiometric systems", Communications of the ACM, vol. 47, no. 1, p. 34, 2004.
5. Ahmad Tasnim Siddiqui,"An Enhanced Multi-Modal Biometric System for Secure User Identification", Asian Journal of Technology and Management Research (AJTMR), Volume 06 – Issue 01, Jun 2016
6. Massimo Tistarelli, Stan Z. Li, Rama Chellappa,"Handbook of Remote Biometrics", Advances in Pattern Recognition, pp. 64-381, 2009.
7. Tarsem Bansa, Er. Munish Kumar Dhir,"Analysis of Uni-Modal & Multimodal Biometric System using Iris & Fingerprint", International Journal of Advanced Research in Computer Science,Vol. 6, No. 7, pp.88-92, 2015
8. Wang, Z, Wang, E, Wang, S, Ding, Q, "Multimodal Biometric System Using Face-Iris Fusion Feature", Journal of Computers, Vol. 6, pp. 931–938., 2011
9. Liau, H. F., Isa, D, "Feature Selection for Support Vector Machine-based Face-iris Multimodal Biometric System", Expert Systems with Applications, Vol. 38, 2011
10. Wang, Z, Wang, S, Ding, Q, "Security of Multimodal Biometric Fusion System" Vol. 5, pp. 264–270, 2011

11. R. Rodrigues, L. Ling and V. Govindaraju, "Robustness of multimodal biometric fusion methods against spoof attacks", Journal of Visual Languages & Computing, vol. 20, no. 3, pp. 169-179, 2009.
12. J. Fierrez-Aguilar, J. Ortega-Garcia, J. Gonzalez-Rodriguez, J. Bigun, “Discriminative multimodal biometric authentication based on quality measures”, Journal on Pattern Recognition, Vol. 38, No.5, pp. 777–779, 2005
13. M. Singh, R. Singh and A. Ross, "A Comprehensive Overview of Biometric Fusion", Journal on Information Fusion, pp. 1-25, 2019
14. S. Modak and V. Jha, "Multibiometric fusion strategy and its applications: A review", Information Fusion, vol. 49, pp. 174-204, 2019.
15. Anil K. Jaina, Karthik Nandakumar, Arun Ross, "50 years of biometric research: Accomplishments, challenges, and opportunities", Journal on Pattern Recognition Letters, Vol. 79, pp.80–105, 2016
16. A. Rattani and R. Derakhshani, "A Survey Of mobile face biometrics", Journal on Computers & Electrical Engineering, vol. 72, pp. 39-52, 2018.
17. T. Van hamme, D. Preuveneers and W. Joosen, "Managing distributed trust relationships for multi-modal authentication", Journal of Information Security and Applications, vol. 40, pp. 258-270, 2018
18. R. Saini et al., "Don’t just sign use brain too: A novel multimodal approach for user identification and verification", Journal on Information Sciences, vol. 430-431, pp. 163-178, 2018
19. M. Bounneche, L. Boubchir, A. Bouridane, B. Nekhoul and A. Ali-Chérif, "Multi-spectral palmprint recognition based on oriented multiscale log-Gabor filters", Journal on Neurocomputing, vol. 205, pp. 274-286, 2016.
20. H. Habibzadeh, T. Soyata, B. Kantarci, A. Boukerche and C. Kaptan, "Sensing, communication and security planes: A new challenge for a smart city system design", Journal on Computer Networks, vol. 144, pp. 163-200, 2018.
21. A. Jade, B. Srikanth, V. Jayaraman, B. Kulkarni, J. Jog and L. Priya, "Feature extraction and denoising using kernel PCA", Journal on chemical Engineering Science, Vol. 58, pp. 4441 – 4448, 2019.

AUTHORS PROFILE

P Jayapriya completed B.Sc., (CS), M.C.A and M.E Computer science (2016) and doing full time research in Department of Information Technology at PSG College of Technology, Coimbatore, Tamil nadu. She has 10 years teaching as teaching experience. She is a member of Indian Society for Technical Education. She presented paper in more than 15 national international conferences and two Scopus indexed journal. Her area of research are image processing, pattern recognition, and biometrics

Dr. K. Umamaheswari is currently working as professor and Head the department of Information technology of PSG College of Technology. She has rich experience in teaching for about 20 + years. Her area of research is classification of various types of data like text, image etc. using data mining. The applications related are gene expression analysis, review analysis in social media, multimodal biometrics and cognitive networks. She published more than 75 papers in international, national journals and conferences publication to her credit. She is a life member in ISTE, ACS and fellow member in IE. She is the editor of National journal of technology, PSG college of Technology and reviewer for many national and International journals