Enhancement with Data Encryption Method in Multi-Model Biometric System

Nancy Gupta[*], Sandeep Kumar Singla[**], Dr. Anu Bala[***]
Research Scholar, GNDEC Ludhiana[*], Assistant Professor, GNDEC Ludhiana[**],
Assistant Professor, NIT Jalandhar[**]
Department of Computer Science and Technology, Guru Nanak Dev Engineering College,
Ludhiana,Punjab, India,
nncgupta92@gmail.com[*], sandeepkumar.singla@gmail.com[**],
anu_singla13@yahoo.com[***]

Abstract— Biometric Systems are the major concept of deployment, today information is used from a single biometric technology for identification and verification. The large-scale biometric systems have to address additional requirements like as larger population coverage and various deployment environments, etc. Nowadays, single modality biometric systems are finding, it difficult to meet these requirements and a solution is to integrate additional sources of data to strengthen the decision procedure. Biometric authentication is a main challenge for accessing dissimilar web-based applications, data exchange, communicating users, conducting e-business and performing financial operations, System accessible like as ATM and WI-FI etc. Multi-model biometric system combines data from various biometric traits, methods, sensors and some other components to create a recognition process. Most biometric systems that are typically use a single biometric trait to establish identity have some challenges like Noise in sensed data which increases False Acceptance Rate (FAR) of the system, Non-universality which reduces Genuine Acceptance Rate (GAR). Hence the security afforded by the biometric system mitigates its benefits. In this existing work, it proposed a Fused Multi-modal system which also has several advantages over uni-biometric systems such as, enhanced verification accuracy, larger feature space to accommodate more subjects and higher security against spoofing. In the multi-modal biometric system used for mainly to enhance the security issues with encryption techniques. In uni-modal biometric system trait to verify have some challenges like distortion in sensed data which increase the FAR (False Acceptance Rate) of the system and non-universality which reduces the GAR (Genuine Acceptance Rate).The proposed work, an enhanced multimodal authentication system is based on feature extraction (using fingerprint, retina and finger vein) and key generation (using 3DES encryption algorithm).

Keywords— **3DES (Triple Data Encryption System), PCA (Principal Component Analysis), RSA *(R*ivest Shamir Adleman*)*, SLF (Score level Fusion).**

I. INTRODUCTION

In the world of technology, privacy becomes a major issue in the automatic security systems. The privacy required several things as the Confidentiality, Authentication, Integrity, Non-Repudiation and a lot of availability on the network. Confidentiality is the authentication for accessing the data. The users who have confidentiality can extract the data and information. Non-Repudiation relates to the confirmation about the message sent or receives in case of false replies. The enhanced systems allot availability to the users with improved services. Another term is integrity, which refers to the security of data that are without modification in the process of sending and receiving data [1]. Authentication is a main concept of any trustworthy computing system. It confirms that only the identified and recognized users should be allowed to access the system resources [2].

The term biometric derived from the Greek word bios which refer to the life and metrics which describes the measures. These are the methods generated for identification of humans in the automatic security system. Another work of biometrics is for the verification of new data with the existing data. It contains several measurements about the person's face, fingers, length, head, feet's etc.

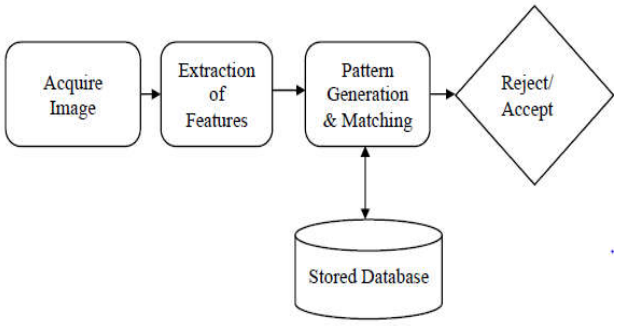

Fig.1 Biometric System

A. Classification of Biometric Systems

Biometric systems are classified in various fields of recognition that based on the person's behavior and physical properties.

1) *Iris Recognition*: It is a kind of biometric system. Iris recognition is used for identification and verification of the human identity.
2) Face Identification: This recognition process based on the features of the face that includes nose, eyes, smile, lips, and head. It is a system for computer vision applications for verification of existing data with the new images or the person.
3) *Finger Prints:* Usually, finger prints are seen in every automatic security system. The recognition takes place with the loops ridges, arches, furrows on the finger tips.
4) *Voice Recognition:* The primary factor for detection of voice is frequency of the person's voice, tone of speaking, cadence and inflection. On the basis of these factors the detection processed [3].

B. Multi-Modal Biometric System

This kind of biometric systems acquired the source information form the different images and process for all of them, called multi modal system. The working of multi-model is based on the three kinds of the operators, namely, serial mode operator, parallel mode and the hierarchical mode. One operator is always required for the procedure of multimodal system. There are further basic biometric systems that came under the multi modal category of biometric systems as shown as in fig.2 [4].

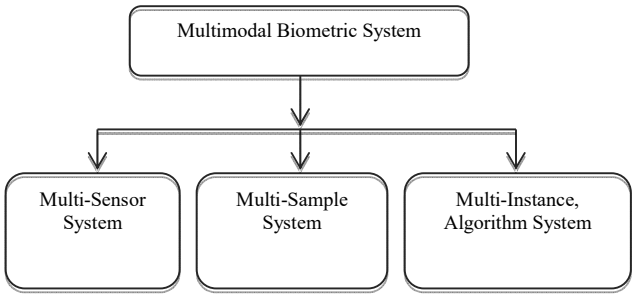

Fig. 2 Multimodal Biometric Systems

C. Architecture of Multi-Modal System

The multimodal architecture described with the working process of multimodal system. Firstly, sensor mode, which is used to capture the input samples, second part is the feature extraction method that extracted the all similar and dissimilar features of input image., next to it Matching module takes place which refer to the matching process that compares the new data with the existing data stored in the database, then fusion module taken that have certain levels and the new data must be pass through these levels.

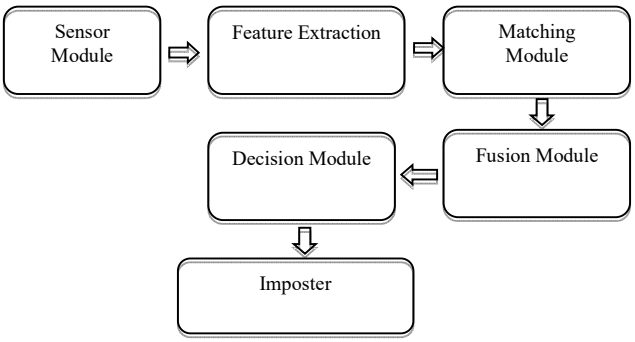

Fig.3. Architecture of Multimodal System [5]

Different Modules of Multi-Modal Biometric: There are primary four modules of multimodal biometric which are given below-

1) *Sensor Module:* These are the modules used for the feature extraction. All these modalities given for the input image.
2) *Feature Extraction Module:* All the features are captured from the different modularity's. After feature extraction these modularity's given to the matching module for the comparisons of features.
3) *Matching Module*: The new modularity's is compared with the previous data stored at the database.
4) *Decision Making Module:* A final modularity is selected in this part. A decision is based on the matching modules.

D. Fusion in Multi-Modal System

Fusion is basically preferred for the combination of data that have certain levels for the processing of captured data of image that are given below.

1) *Sensor Level Fusion*: This level 1 fusion which collects the raw data or information from the multiple sources with the multiple sensors. From the raw data a vector is created that have direct access to the feature extraction module.
2) *Feature Level Fusion:* The most common and useful level is feature level fusion. This level is used for extract the data from the same modularity's. It combines the multiple data into a single vector. The selection of features done using techniques. It is highly efficient for Euclidean distance.
3) *Matching Level Fusion:* This level is related to the normalization of score matches which are from the similar domain. It prefers some methods like- minimum, maximum particularly trained for the Score value in the form of binary as 0 or 1.
4) *Decision Level Fusion:* The acceptance and the rejection take place in this scheme, where the multiple biometric fusion performed with each classifier used for the decisions. Ranks are given according to the winner electric method in which candidates receive points related to the position. Eventually, the winner is declared who had the highest number of points in the Board approach [5].

5) *Ranking Level Fusion:* In this level, all the data is sorted in the descending order. These rankings are more relevant than the verification. A rank is allotted to each dataset [4] [6].

E. Characteristics of Multi-Modal System

There are various advantages over the uni-modal system. Multi modal overcomes the weaknesses of uni-modal and have some other features that are effective outcome, deter to spoof attack, higher reliability, better indexing, more privacy and better performance in matching.

F. Applications of Multi Modal Biometric System

Automatic security systems are also in need of highly efficient biometric system. Multimodal biometric system outcomes are higher efficient and reliable in the real time applications. The fields of applications of this system are as below-

1) Defence and intelligence community
2) A home land Security
3) Law enforcement community
4) Border management and civil applications.
5) Government applications
6) Business transactions.
7) Personal information
8) Online customer verification [7].

The entire research work is explained in different sections. Section I consists the basic information about the biometric systems as well as the multi-modal biometric system with different modules. Section II explained to describe the existing work done in the same research topic as multi-modal system. Section III represents the proposed work and the most important section IV which is the experimental section that improved the performance of multimodal system. The last sections are V and VI that gives the overall summary and future purposes of current research.

II. LITERATURE REVIEW

Jagadiswary et al., (2016)[8] proposed a Fused Multimodal system that had various benefits with respect to uni-biometric framework like improved verification accuracy, bigger space to coordinate with more subjects. Biometric were an extension of the pattern recognition framework. Recently, optical sensors such as scanning devices and cameras used to record images and unique features. Biometric framework generally used biometrics to create a unique identity that maximizes the FAR (False Acceptance Rate) and non-universality minimizes GAR (Genuine Acceptance Rate). The proposed and improved multimodal confirmation framework depends upon a feature extraction by using retina, fingerprint, etc. and key generation. MATLAB was used to evaluate and illustrate the importance of upgraded framework. The performance of framework improved with RSA had genuine acceptance Rate of 95.3% and false acceptance rate of 0.01%.

Barbu et al., (2015) proposed a multimodal biometric framework based on iris, voice and faces identifiers. They explained various biometric recognition techniques for human irises, voice and face and united them in a multimodal framework. The recognition methods utilize same classification methods, but a unique method for feature extraction.

The text based speaker identification model utilizes DDMFCC dependent speech analysis; facial identification a method establishes SIFT dependable feature vectors, whereas iris verification system utilizes LAB color features. There was initialization of specific metrics to compute distances among them. The biometric fusion performed at decision level results in an enhanced recognition rate.

Dinca et al., (2017) [10] surveyed on Multi-biometric, including fusion methods and security. Fusion was a main prerequisite in multi-biometric frameworks, being the technique used to consolidate numerous biometric strategies into a solitary framework. The combination segment overviews late multi-biometric plans arranged from the point of view of combination strategy. The security area was an exhaustive audit of current issues, for example: format security, sensor satirizing, and biometric encryption. Latest trends and challenges like: contextual-based biometrics, etc. were discussed.

Kim et al., (2012) [11] reviewed several multi-biometric techniques along with the fusion of biometrics and several feasible scenarios. Biometrics were becoming most encouraging technologies in the previous few years that utilized physiological features like face, voice, fingerprint, iris, etc. for individual identification. Combinations of two or more techniques furnish better performances compared to uni-modal. Lastly, discussed few applications of smart TV domain depend upon multi-modal biometric.

Omran and Maryam, (2014) [12] proposed a multimodal system using iris and finger-print recognition framework to create a series of identification system. The fingerprint identification formula was revised to create Delaney triangulation framework in which neighbouring triangles were compared among stored template and input. Whereas, iris recognition system was revised segmentation method based on correlation filter. Such method was applied to lower part of the iris region, which is least influenced by noise. The suggested multimodal system provides high accuracy and less error rate that equals (0.9%).

TABLE I

LITERATURE SURVEY COMPARISON

Author's Name And Year	Technique Used	Performance Parameters	Research Gap
Jagadiswary et. al., (2016)	Fused multi-modal system	Accuracy, False acceptance rate, genuine acceptance rate	Increased noises while capturing of images.
Barbu et. al., (2015)	SIFT (Scale invariant feature transform)	-	Uni-modal deals with vast error rates,
Dinca et. al., (2017)	Discuss various multi-model methods,	-	Contextual based issues
Kim et al., (2012)	Review of different techniques.	Comparison of uni-modal and multi-modal	-
Omran and Maryam, (2014)	Finger print and iris recognition	Accuracy Error rates	Noise

III. PROPOSED WORK

In this section, the process of collecting the images such as retina image, fingerprint and Vein Image required for the training and testing, preprocessing, feature extraction and parameter evaluation has been discussed.

A. Image Acquisition

It defines the biometric category i.e.; Fingerprint, Finger vein and Retina (CASIA) from the UCI repository Dataset .The multi-modal biometric system need to convert the original input image to the corresponding gray scale image.

B. Pre-Processing

Pre-processing step is considered to identify the noise level i.e. Salt and Pepper form and filtration methods used to remove the interference in the retina, finger vein and fingerprint images and detect the RGB components.

C. Principal Component Analysis (PCA)

Principal component algorithm is used for feature extraction to determine the uniqueness of an image and to develop eigenvalue and vector. In principle component analysis algorithm used to extract the features.

D. Feature Extraction

The extraction of features in fingerprint (Munitia Algorithm): Minutiae algorithm used for feature extraction. Fingerprint image of an each person is measureable as distinctive and it also un-changed over the life-time. Even the Image fingerprints of twins are also unique. An impression of the Fingerprint may be produced by the ridge and valley model on a finger-tip hide. A ridge may be defined as a signal curve part and a valley is the edge between twin's adjacent ridges. Valley and ridges model banks on every fingerprint image create some different aspects which are portrayed minutiae feature extraction was carried out using the cross number method.

E. 3DES (Triple Data Encryption System)

3DES stands for the triple data encryption process the encryption is a method to change the plain text in the form of hidden patterns as cipher text. This procedure used to save the data from the hackers. This procedure started by National Institute of Standards and Technology (NIST), the whole part of DES based on the IBM. It was invented in 1974. 3DES is the similar algorithm for encryption, to increase the security and to save the data from attackers the encryption applied three times, so it named as 3DES [13].

F. Score Level Fusion (SLF)

Score Level fusion after matching the features of different biometrics like fingerprint, finger veins and retina recognition. Compute the overall performance of the system i.e. Genuine acceptance rate and False acceptance Rate and compared with the existing one (RSA).

IV. EXPERIMENTAL RESULTS

An important part of the design and development of a biometric authentication system is the process of evaluating and determining system performance, which is an indication of the system accuracy before the system is used in real-life application. The most commonly used methods of evaluating the performance of multi-model biometric authentication systems are described. It also provides information on one of the currently available multi-modal databases used in evaluating the proposed methods.

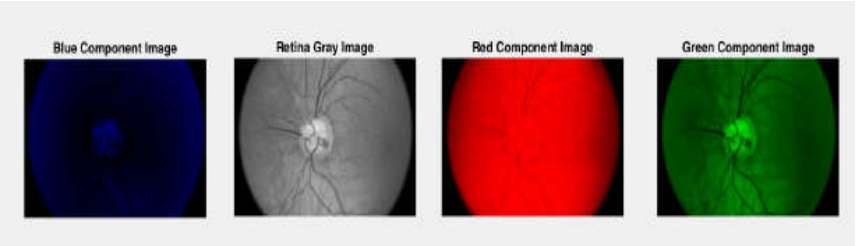

Fig.4 Retina Framework

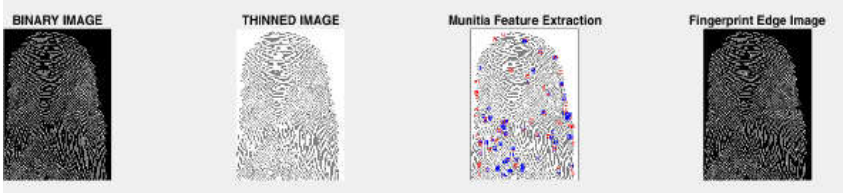

Fig.5 Fingerprint Framework

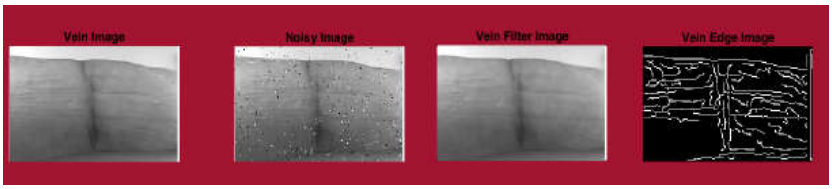

Fig.6 Finger Vein Recognition Framework System

The description of above three figures as namely as the retina, fingerprints and vein recognition are as below-In the retina framework, it uploads the image from the dataset which is downloaded from the online site. Artificial Noise adds in original image. Filtration methods used to remove the noise in the retina image. Edge detection is used to detect the regions in the image. Apply feature extraction method to identify the key-points which is unique features in the original image. Figure represents that the Fingerprint recognition graphical user interface i.e., shows that the upload the original image. Gray scale form, edge detection using canny Technique and feature extraction using Minutia algorithm.

A. Performance with Graphical Representation (FAR, FRR & GAR)

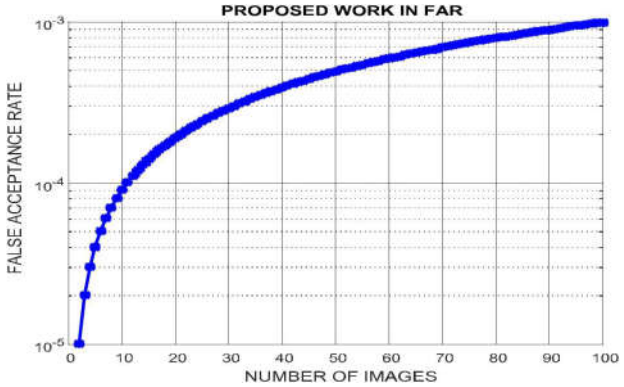

Fig.7 Parameters in FAR (False Acceptance Rate)

Fig.7 shows that the FAR, which is used to evaluate the performance, related to the possibility of the biometric system will incorrectly allow false access attempt by an unauthorized person.

False Rejection Rate (FRR) is the measure of the likelihood that the biometric security framework will inaccurately dismiss an entrance endeavor by an approved user as given by the fig.8. A framework's FRR, normally is expressed as the proportion of the quantity of false dismissals partitioned by the quantity of recognizable proof endeavors.

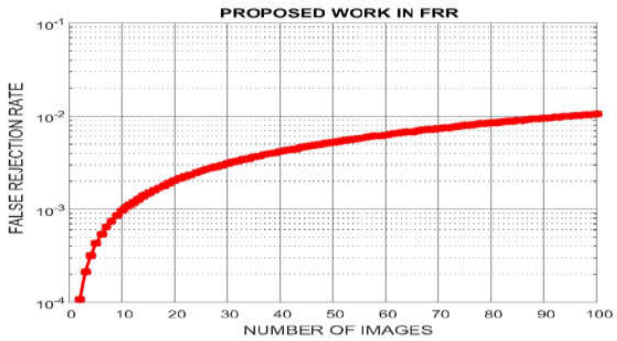

Fig. 8 Parameters in FRR (False Rejection Rate)

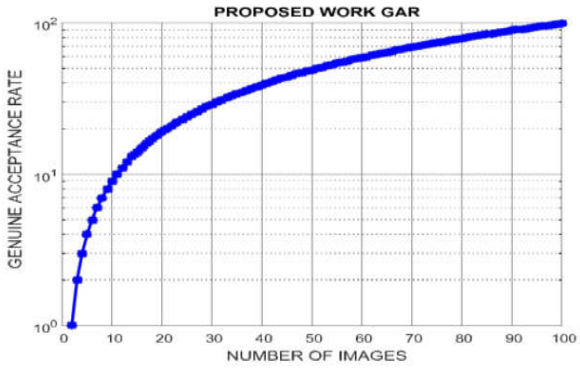

Fig.9 Proposed Parameters in GAR (Genuine Acceptance Rate)

Genuine Acceptance Rate (GAR) is defined as a percentage of genuine and approved users accepted by the biometric system. It is given by GAR=100-FRR.

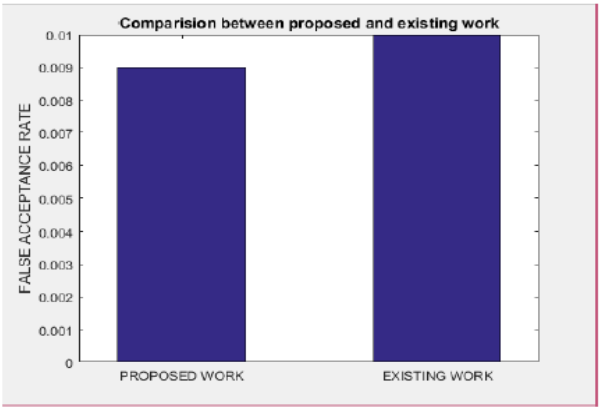

Fig. 10 Comparison between Proposed and Existing Work (FAR)

Fig.10 shows that the comparative assessment between proposed (3DES) and Existing (RSA) algorithm with False Acceptance Rate. In FAR parameter value decreases in the proposed work and existing work has high rate of the wrong data acceptable in the biometric system with fusion. In existing work FAR value is 0.01 and proposed work value is 0.00099.

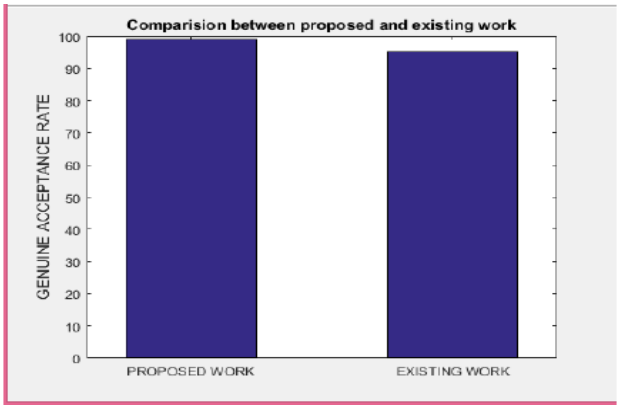

Fig. 11 Comparison between Proposed and Existing Work (GAR)

Fig.11 shows that the comparative assessment between proposed (3DES) and Existing (RSA) algorithm with Genuine Acceptance Rate. In GAR parameter value decreases in the proposed work and existing work high rate of the original data acceptable in the biometric system with fusion. In existing work GAR value is 95.3 and proposed work value is 98.6.

TABLE IIV
PROPOSED PARAMETERS

Biometrics Traits	**FAR**	**FRR**	**GAR**
Fingerprint, Retina and Vein	0.00099	0.0105	0.99
Fingerprint, Retina and Vein	0.00098	0.0104	0.98
Fingerprint, Retina and Vein	0.00089	0.010	0.97

TABLE II described that the proposed parameters False Acceptance Rate, False Rejection Rate and Genuine Acceptance Rate. In proposed work, the performance metrics are improved with 3DES with Fused the three biometric traits (Retina, Fingerprint and Finger Vein) system.

TABLE IIIV

COMPARISON (FAR) WITH PROPOSED AND EXISTING WORK

Biometrics Traits	**FAR (Proposed Work)**	**FAR (Existing Work)**
Fingerprint, Retina and Vein	0.00099	0.01
Fingerprint, Retina and Vein	1.023	2.06
Fingerprint, Retina and Vein	1.90	2.2

TABLE IVV

COMPARISON (GAR) WITH PROPOSED AND EXISTING WORK

Biometrics Traits	**GAR (Proposed Work) %**	**GAR (Existing Work) %**
Fingerprint, Retina and Vein	98.5~0.98	98.3~0.95
Fingerprint, Retina and Vein	98.3~0.983	80.52~0.802
Fingerprint, Retina and Vein	97.0~0.97	84.2~0.842

Cavernous study of the Tables III and IV revealed that, the performance of the proposed multimodal biometric (fusion of finger vein, fingerprint and retina) which is based on the fused matrix values and by using 3DES has a GAR value of 0.98% and FAR is 0.00099 and RSA value in existing work has a GAR value of 95.3% and FAR of 0.01%**,** whereas without RSA. The comparative curves were shown in Fig. 4.12 and 4.13. However, in order to increase the accuracy of multimodal biometric as a whole, fusion at score level fusion, and encrypting using security algorithm has been performed. The overall performance of a multi-modal system has reduced FAR of 0.00099 and increases GAR of 98.5% with 3DES, respectively, and its performance compared to uni-modal biometric systems such as fingerprint, retina and finger vein with RSA. The performance of multimodal biometric based on fused matrix values using 3DES has a GAR of 97.3% and FAR of 1.023, RSA with fingerprint have GAR of 0.97 and FAR 1.90.

V. CONCLUSIONS AND FUTURE SCOPE

The score level fusion method is used for the design of multi-modal biometric traits such as fingerprint, retina and finger vein, which protects the multiple templates using 3DES and PCA has been implemented using MATLAB R2016a.

A realistic security analysis of the multimodal biometric crypto-system has also been conducted using fingerprint, finger-vein and retina, which provide a significant improvement performance in a multi-modal biometric crypto-system using 3DES. Finger vein, Finger Print and Retina based recognition resulted in different performance parameters of using databases collected by features i.e., texture format and shape based feature (Eigen Values and Vectors). After, in research work completed the retina, fingerprint and finger vein experiment and attained like as a distinction performance it has conducted retina image, finger print and vein databases, particular, enhance the contrast and accuracy and reduce the false accepted Data and Rejected Data in the multi model System. The overall performance of multi-modal system has increased with 3DES algorithm GAR 99% and reduced with FAR of 0.0009, which is compared to uni-modal biometric using RSA. The experimental results define that in most of the cases fused performance (Retina + Fingerprint and Finger Vein) was importantly enhanced to uni-model biometric performance Retina, Fingerprint and Vein respectively. It is to be concentrate that the famous multi-model biometric fusion by Score Level fusion methods and 3DES encryption approach used.

REFERENCES

[1] *Nie, T., and Zhang, T. (2009). A study of DES and Blowfish encryption algorithm. In Tencon 2009-2009 IEEE Region 10 Conference, pp. 1-4.*

[2] *Sui, Y., Zou, X., & Du, E. Y. (2011, July). Biometrics-based authentication: A new approach. In Computer Communications and Networks (ICCCN), 2011 Proceedings of 20th International Conference on (pp. 1-6). IEEE.*

[3] *Vats, S., & Kaur, H. (2016). A Comparative Study of Different Biometric Features. International Journal of Advanced Research in Computer Science, 7(6).*

[4] *Taouche, C., Batouche, M. C., Berkane, M., & Taleb-Ahmed, A. (2014, April). Multimodal biometric systems. In Multimedia Computing and Systems (ICMCS), 2014 International Conference on (pp. 301-308). IEEE.*

[5] *Veluchamy, S., & Karlmarx, L. R. (2013). Technical Review of Multi Model Biometrics System. International Journal of Computer Technology and Applications, 4(3), 537.*

[6] *Telgad, R. L., Deshmukh, P. D., & Siddiqui, A. M. (2014, May). Combination approach to score level fusion for Multimodal Biometric system by using face and fingerprint. In Recent Advances and Innovations in Engineering (ICRAIE), 2014 (pp. 1-8). IEEE.*

[7] *Shobana, D., Logeshwari, A., & Maheswari, S. U. (2017). A Study on Multimodal Biometrics System.*

[8] *Jagadiswary, D., & Saraswady, D. (2016). Biometric authentication using fused multimodal biometric. Procedia Computer Science, 85, 109-116.*

[9] *Barbu, T., Ciobanu, A., & Luca, M. (2015, November). Multimodal biometric authentication based on voice, face and iris. In E-Health and Bioengineering Conference (EHB), 2015(pp. 1-4). IEEE.*

[10] *Dinca, L. M., & Hancke, G. P. (2017). The fall of one, the rise of many: a survey on multi-biometric fusion methods. IEEE Access, 5, 6247-6289.*

[11] *Kim, Y. G., Shin, K. Y., Lee, W. O., Park, K. R., Lee, E. C., Oh, C., & Lee, H. (2012). Multimodal Biometric Systems and Its Application in Smart TV. In Computer Applications for Database, Education, and Ubiquitous Computing (pp. 219-226). Springer, Berlin, Heidelberg.*

[12] *Omran, S. S. and Maryam A. S. (2014). Design and Implementation of Multi-Model Biometric Identification System. International Journal of Computer Applications, 99 (15), pp.14-21.*

[13] *Singh, S. P., & Maini, R. (2011). Comparison of data encryption algorithms. International Journal of Computer Science and Communication, 2(1), 125-127.*