MULTIBIOMETRIC TEMPLATE USING IRIS AND FINGERPRINT

1st MRS.R.PRIYA
Applied Mathematics and
Computational Sciences
Coimbatore, India
priyaamcs@gmail.com

2nd T.Gowtham Prasath
Applied Mathematics and
Computational Sciences
Coimbatore, India
prasathgp31@gmail.com

3rd U.Neethu Krishna
Applied Mathematics and
Computational Sciences
Coimbatore, India
neethu52krishna@gmail.com

4th D.Shreenidhiy
Applied Mathematics and
Computational Sciences
Coimbatore, India
shreenidhiydurai@gmail.com

5th V.Akilandaeswari
Applied Mathematics and
Computational Sciences
Coimbatore, India
akilandaeswariv244@gmail.com

ABSTRACT

Biometric technologies are playing a vibrant role in various security applications. It is fundamentally an automatic recognition system. It recognizes a person by determining their specific characteristics possessed by an individual. Since last decade, biometric system continues to provide higher security features for authentication. In the real world application, the unimodal biometric systems are employed for authentication. At the same time they are susceptible to variety of problems and leads to less significance. To reduce the error rate, the multimodal biometric systems is employed .It integrates two or more biometrics systems. In this paper we present a new multi-biometric authentication system using Iris and Fingerprint (IFP) imaging. For matching IFPs, a feature extraction scheme which combines orientation and magnitude information by Canny edge detection and the encrypted images are stored in the database , which consists of 1000 images, is established to verify the efficacy of the proposed system and promising results are obtained. Due to the existence of multiple and independent biometrics, the proposed IFP system achieves much higher recognition rate and it works in real time.

Keywords: Biometric, Authentication, Iris and Fingerprint ,Encryption.

I. INTRODUCTION

In this modern scientific world, technologies are transforming rapidly but along with the ease and comfort they also bring in a big concern for security. Governments and enterprises of all sizes have become much more vigilant regarding security[1]. There is always a need to re-examine and potentially improve security, and biometric is attracting growing interest as fraud increases and the conventional authentication methods PINs, passwords, and identity cards prove inadequate to counter the growing threats.

Biometric systems automatically determine a person's identity based on his anatomical and behavioral characteristics like palm print, fingerprint, face and iris. A method of recognizing the identity of an individual person depends on the physiological and behavioral characteristics is biometric recognition[2]. Multimodal biometric rises correctness by considering other very specific biological traits to limit the no of applicants for an identity. Multimodal biometric systems use over one physiological or behavioral characteristic for enrollment, verification and identification[3].

Unimodal biometric system performs person recognition based on single source of biometric information. These systems have to contend with of number of limitations such as intra-class variations, inter-class similarities, spoof attacks and universality of trait [4]. Apart from these, noisy data resulting from defective sensors, the high failure rates (failure to enroll rate and failure to capture rate) and scalability are other problems associated with these systems. Multimodal biometric system seeks to overcome some of these limitations by merging the characteristics presented by multiple biometric information sources[5]. It combines information from two or more biometric modalities in a single system where information will be in encrypted form. It may fuse information from multiple biometric traits, multiple sensors, multiple representations, multiple snapshots or matching algorithms.

In this paper we present an approach of combining iris and fingerprint (IFP) biometric at feature level in a multimodal biometric system. The main motivation behind this choice of IFP characteristics for a multi-biometric authentication system is that fingerprint is the oldest and most widely adopted biometric technology, as a result is the most mature of all biometric technologies , iris recognition is proved that it is most accurate and hygienic biometric technology among others. As the core of our work revolves around examining whether or not the performance of a biometric-based authentication system may be improved through integrating complementary biometric features that comes primarily from two different and independent modalities.

We propose a multi-modal biometric authentication approach using iris and fingerprint images as biometric traits. We use face detection and feature extraction method to extract iris from an image. Similarly, pre-processing and feature extraction method to extract fingerprint. And encryption algorithms are applied and the encrypted data are stored in IFP database. We demonstrate that this proposed approach achieves high performance on different multimodal biometric databases involving iris and fingerprint modalities. Furthermore, we have analyzed the quality of iris and fingerprint databases. Finally, we show that fusion of uncorrelated modalities such as iris and fingerprint achieves better accuracy and security compared to unimodal biometric systems.

II. LITERATURE SURVEY ON BIOMETRIC SYSTEMS

Authentication is required when it is necessary to know if a person is who they claim to be. It is a procedure that involves a person making a claim about their identity, and then providing evidence to prove it. Biometric refers a technology to demonstrate people by machine controlled means admit anatomical or activity human characteristics. Biometric systems have the potential to try and do the individuals authentication with a high degree of assurance.

In globe application most of the deployed biometric system for authentication relay on the one supply of data (e.g. face, fingerprint, iris etc.). These systems area unit susceptible to sort of issues like non- universality, susceptibility to spoofing , noise in sensed data, intra –class variations, inter-class similarities. Some limitations of the unimodal biometric systems are often eased by using multimodal. A biometric system that mixes quite one sources of data for establishing human identity is named a multimodal biometric system.

A. UNIMODAL BIOMETRIC SYSTEM:

The unimodal biometric employs single biometric attribute (either physical or behaviour trait) to spot the user Physiological life science identifiers embody fingerprints, hand pure mathematics, eye patterns, ear patterns, countenance, etc[6]... Behavioural identifiers embody voice, signature, typewriting patterns etc. whereas recognizing a person's feature, there are a unit probabilities for the system to choose a real person as associate cheater or associate cheater as a real [7].Example: Biometric system supported Iris or Fingerprint or Voice or Gait etc. Here by taking associate example of Iris recognition & fingerprint recognition system, the performance of unimodal system is compared with multimodal biometric system.

IRIS REGONITION SYSTEM:

Iris recognition may be a comparatively new branch of biometric recognition. Iris complex pattern can contain many distinctive features such as arching ligaments, furrows, ridges, crypts, rings, corona and freckles [8]. Iris scanning is less intrusive because the iris is easily visible from several meters away. Responses of the iris to changes in light will offer a vital secondary verification that the iris presented belongs to a live subject. Irises of identical twins are totally different, which is another advantage. Newer systems have become more user-friendly and cost-effective. A careful balance of light, focus, resolution and contrast is important to extract a feature vector from localized image. While the iris looks to be consistent throughout adulthood, it varies somewhat up to adolescence. Iris recognition preferred because of the following reasons:

Uniqueness: The chance of 2 persons' irises being constant is less than 10–35. Although they're twins, their irises square measure quite totally different [9]. This reality is that the reason why we have a tendency to use iris to acknowledge identity.

Reliability: Iris is associate inner organ in our eyes and guarded by lid, lash and tissue layer. Not like finger and palm, it's rarely hurt and therefore the error of recognition caused by scar can never happen during this sense, iris recognition is way higher than fingerprint and palm-print recognition [10].

FINGERPRINT REGONITION SYSTEM:

Fingerprints were used for personal identification for many centuries and the matching accuracy was very high [11]. One of the most publicized and well known biometric is fingerprint identification. Due to their consistency and uniqueness over the time for identification purpose fingerprints are used over the century, and due to enhancement in computing capabilities it has become more automated [12]. The feature values typically correspond to the position and orientation of certain critical points known as minutiae points [13]. The matching method involves comparing the two-dimensional minutiae patterns extracted from the user's print with those within the template. One downside with the present fingerprint recognition systems is that they require a large amount of computational resources.

B. MULTIMODAL BIOMETRIC SYSTEM:

Multimodal biometric recognition systems are estimated to be more reliable due to the presence of multiple, rather independent pieces of facts [14]. Multimodal biometric systems address noisy data downside by providing multiple sensors and multiple traits. Intra-class variations and inter-class similarities can be avoided with multiple samples and multiple instances of same trait. To address the problem of non-universality they provide sufficient population coverage with multiple traits. They also prevent spoof attacks since it would be difficult for an impostor to spoof multiple biometric traits of a genuine user at the same time.

NEED FOR MULTIMODAL BIOMETRIC:

Many biometric systems established to this point in various applications that believe the proof of single supply of data for authentication (e.g. fingerprint, face, voice etc.) area unit unimodal. These systems area unit unsafe attributable to the incidence of kind of issues like clanging information, intra-class variations, inter-class similarities, non-universality and spoofing because it ends up in high false acceptance rate (FAR) and false rejection rate (FRR), restricted discrimination capability, edge in performance and lack of persistence. For establishing identity few limitations exhibited by unimodal biometric systems may be overcome by comprising multiple sources of data [15]. 2 or a lot of biometric systems referred to as multimodal biometric systems area unit allowed to integrate. There responsibleness depends on the presence of multiple, freelance bioscience information and the potency of the general higher cognitive process may be increased by The fusion of multiple modalities .e.g. potency of police investigation events from a team sports video has solely become attainable by fusion of audio-visual options.

RELATED WORK

IRIS AND FINGERPRINT BASED MULTIMODAL BIOMETRICS SYSTEM:

Iris & Fingerprint traits are here combined along for the analysis of multimodal biometric system.
The previous work describes the architecture which uses wavelet & texture based feature extraction method.

The previous system uses two biometrics traits that are iris & fingerprints. For both traits, the process flow is as: first capture the biometric trait sample where no.of samples has been collected for both, pre-processing phase where each sample has been normalized and converted into gray scale as required and feature extraction using hybrid wavelets. Here hybrid wavelets (12bp) are generated from Walsh &Kekre (2bp) transforms [16].The feature vector for the enrolled dataset in given to classifier. The decisions of the classifiers are then fused together using decision fusion.

Feature Extraction Phases

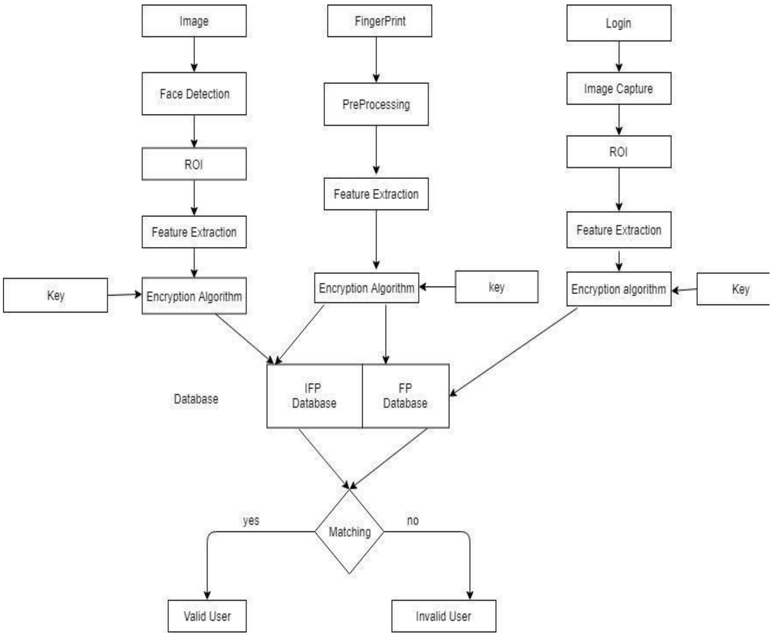
Iris feature extraction: Here first a sample feature has been selected it then converted into grey scale then perform localization and texture features has been extracted. The features values have been saved in .mat file &extrema, centroid and area features has been extracted[17].

Fingerprint feature extraction: Here first a sample feature has been selected it then converted into grey scale then texture features has been extracted. The features values have been saved in .mat file &extrema, centroid, perimeter, convex hull, maxima and minima features has been extracted[17].

III. PROPOSED WORK

In this paper, Iris & Fingerprint traits are here combined together for the analysis of multimodal biometric system. This paper describes the architecture which uses feature extraction method and encryption . This Multimodal Biometric System is practically implemented using MATLAB 7.11.0 environment. In this, a database of 50 Iris & Fingerprint samples consisting of a Training Set & Test Set is used. Each Person contributes 2 samples. The result obtained has been measured by calculating FAR and FRR.

The fig 1. describes the architecture of the proposed system. We proposed a new multi-modal biometric authentication approach using iris and fingerprint images as biometric traits for bank related security purpose. In this system we demonstrated to achieve more security and high performance on different multimodal biometric databases involving fingerprint and iris modalities. Furthermore, we have analyzed the quality of IFP(Iris Fingerprint)database, where the extracted images are in encrypted and to make it more and more secure , key is generated for encryption process. which makes the system more secured . Finally, we show that fusion of uncorrelated modalities such as fingerprint and iris achieves better accuracy and security compared to unimodal biometric systems.



.

Fig. 1. Architecture of Iris and Fingerprint Multimodal Biometric System

IRIS FEATURE EXTRACTION:

As per the architecture diagram , initially an image is considered and from which face detection process has been carried out. In order to segment the iris portion from the detected face , ROI has been demonstrated .Once the Iris portion has been localized to an image of size 256×256 from the detected face , feature extraction takes place on the localized portion. Finally the extracted 256×256 image has been encrypted using appropriate algorithm once the key is generated. The encrypted iris image will not be stored in any database.

Stages In Iris Recognition System

A. Image Acquisition

It is for capturing a number of iris images using a designed sensor. Image acquisition step is one of the most sensitive and important for the quality of image to be processed, data extracted from raw input determines the performance of the entire system to a large extent.

B. Localization/Segmentation

The iris is acquired as a part of a larger image that contains data derived from the surrounding eye region. The inner and the outer boundaries of the iris are calculated. So it is important to localize that portion of the image that corresponds to iris[18].

C. Normalization

It is that process in which there is change in the range of pixel intensity values. It produce iris region which have the same constant dimensions, so that two images of the same iris under different conditions will have same features.In this system normalization of the iris regon by unwrapping the circular region into a rectangular blockof constant dimensions[19].

D. Feature Extraction

The most important step in iris recognition is the ability of extracting some unique attributes from iris, which help to generate a specific code for each individual. Feature extraction is a special form of dimensionality reduction.

To Calculate radius around the iris :

$$r = (\sqrt{\boldsymbol{a}} * b\ ) + (\sqrt{a * \boldsymbol{b}^2}) - (a - (r\_\boldsymbol{iris}^2))$$

$$r = r - r\_pupil$$

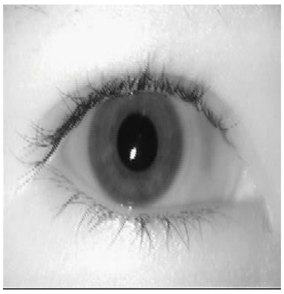


Fig. 2. Localized eye

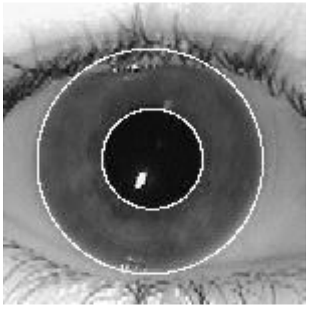


Fig. 3. Extracted Iris

FINGERPRINT EXTRACTION:

Similar to the iris extraction ,an fingerprint image has been preprocessed and specific features have been extracted using Minutiae based extraction method. The extracted image gets shuffled using Henon shuffle method. The shuffled image is encrypted and also key generation has been done prior for more effective encryption.

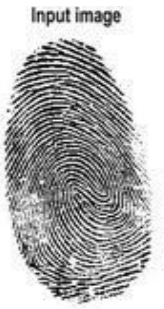


Fig. 4. Input image

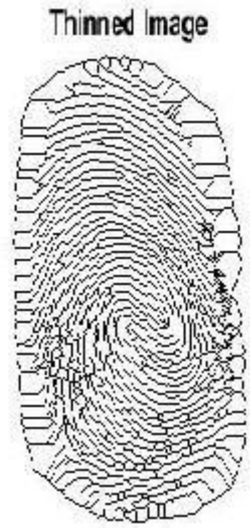
The thinning operation is related to the hit-and-miss transform and can be expressed quite simply in terms of it. The thinning of an image *I* by a structuring element *J* is:

$$\mathbf{thin}(\boldsymbol{I}, \boldsymbol{J}) = \boldsymbol{I} - \textbf{hit-and-miss}(\boldsymbol{I}, \boldsymbol{J})$$

where the subtraction is a *logical subtraction* defined by

$$X - Y = X \cap NOT\ Y$$

Thinning makes it easier to find minutiae and removes a lot of redundant data.



.

Fig. 5. Thinned image

An accurate representation of the fingerprint image is essential to automatic fingerprint identification systems, as a result of most deployed business large-scale systems are captivated with feature-based matching . Among all the fingerprint features, minutiae point features with corresponding orientation maps are distinctive enough to discriminate amongst fingerprints robustly; the minutiae feature representation reduces the complicated fingerprint recognition problem to a point pattern matching problem [20] . In order to accomplish high accuracy minutiae with varied quality fingerprint pictures, segmentation algorithm needs to separate foreground from noisy background that includes all ridge-valley regions and not the background. Image enhancement algorithm must keep the original ridge flow pattern while not fixing the singularity, join broken ridges, clean artifacts between pseudo-parallel ridges, and not introduce false data [21]. Finally minutiae detection algorithm must find expeditiously and accurately the minutiae points.

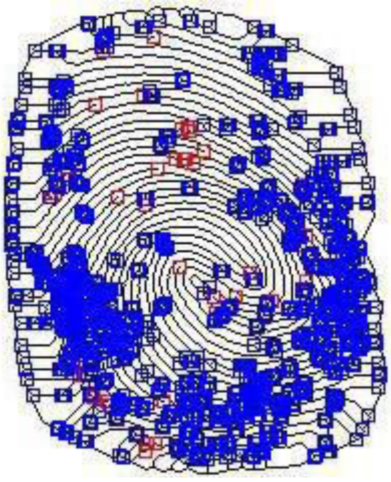


Fig. 6. Minutiae Based Extraction

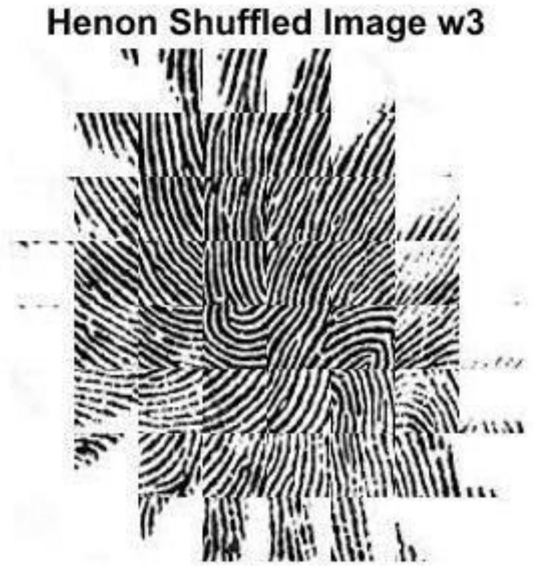


Fig. 7. Shuffled Image

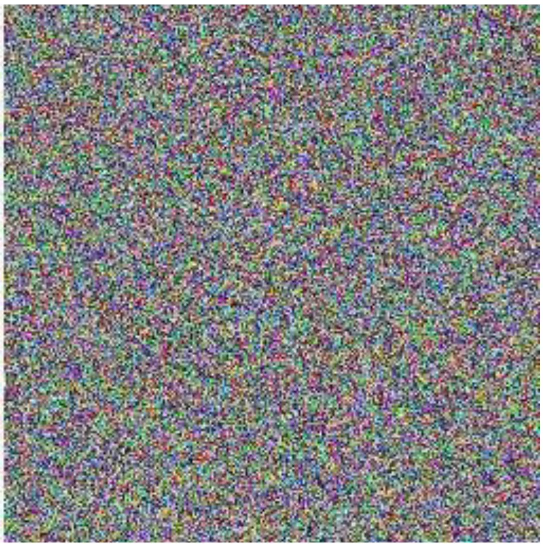


Fig. 8. Encrypted image

Encrypted fingerprint image gets stored in the FP(fingerprint) database .

***KEY GENERATION*:**

The Enhanced Logistic Map(ELM) is used to increase the security of encryption method based chaotic diffusion technique. The equation for ELM is given by the following equations

$$X_{i+1}=-\lambda X_i+\beta Y_i^{2}+\alpha Z_i^{3}+c$$
$$Y_{i+1}=-\lambda Y_i+\beta Z_i^{2}+\alpha X_i^{3}+c$$
$$X_{i+1}=-\lambda Z_i+\beta X_i^{2}+\alpha Y_i^{3}+c$$

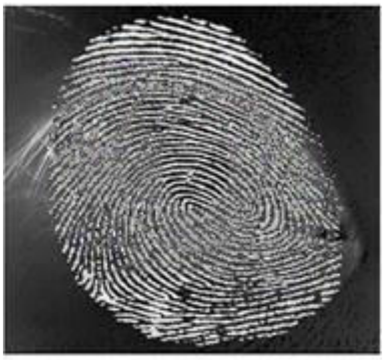


Fig. 9. IFP Image

IV. RESULTS

As a result the encrypted iris image and the encrypted fingerprint image in the FP database are combined applying modulo operations. The final resultant image will be a combined images of iris and fingerprint in IFP database.Once when a user login his/her face will be scanned and iris portion will be extracted . The data stored in the FP database combines with the user's iris and checks for a match from the IFP database.

Different metrics can be used to rate the performance of biometric based authentication system. Here in this proposed system we performed the common metrics - **False Acceptance Rate** FAR and the **False Rejection Rate** FRR[22].

FALSE ACCEPTANCE RATE(FAR):

In biometrics, the instance of incorrectly identifying an unauthorized person is referred to as a type II error or false acceptance. It is considered as the most serious biometric security error as it gives unauthorized users access to systems. Accordingly, the false acceptance rate (FAR) or false match rate (FMR) is the measure of the likelihood that the biometric security system will incorrectly accept an access attempt by an unauthorized user.

FAR is calculated using the following formula:

$$\text{FAR}(\mu) = \frac{\text{No of false successful attempts made in authenticating users}}{\text{Total number of attempts made in authenticating users}}$$

where ' μ' is the security level.

FALSE REJECTION RATE(FRR):

False rejection is a condition in biometric-based system, where an authorized person cannot be identified by the authentication process. False rejection rate (FRR) is the measure to calculate the chance of the biometric based system failing to authenticate a legitimate user and is calculated as the probability of the system to fail in finding a match between an input biometric template and the registered biometric stored in the database. Sometimes it measures a ratio of false rejections and a total number of attempts to do authentication. The term 'rejection' refers to the claim of a user in biometric-based authentication system. It is also known as false non-match rate (FNMR).

$$FRR(\mu) = \frac{\text{No of false reject made in authent icatin g genuine users}}{\text{Total number of attempts made in authenticating users}}$$

where ' μ' is the security level. The lower these FAR and FRR values, the better the biometric trait.

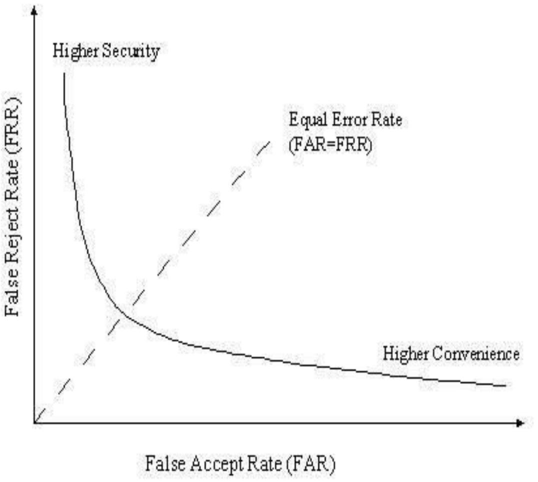


Fig. 10. The representation of FAR, FRR, and EER in receiver operating characteristic (ROC) curve

EQUAL ERROR RATE(ERR):

This error rate is defined as the value obtained at some threshold level of a biometric system where the False Acceptance Rate (FAR) and False Rejection Rate (FRR) are the same. It is also called a crossover error rate. In general, lower the equal error rate, the higher the accuracy of that biometric system. All available biometric systems have the capability of adjusting the sensitivity of these error rates. If the false positive is not desired, the system sensitivity can be set to require (nearly) perfect matches of the enrolment data and the input data of users. If FRR is not desired, the sensitivity value can be readjusted to accept the approximate matches of enrolment data and input data. The following . Fig.10 (ROC curve) illustrates the threshold level to get the desired ERR value.

Traits	(%)	(%)
	FAR	FRR
(Iris &Fingerprint)	4	2

Fig. 11. Result table

Related work	Accuracy (%)
	81.5
Proposed work	84

Fig. 12. Comparison table

V. CONCLUSION

Biometrics refers to an automatic authentication of an individual based on his physiological and/or behavioral characteristics. Some limitations of the unimodal biometric systems will be mitigated by using multimodal biometric systems, that integrate data at numerous levels to boost up the performance. With the objective of improving the performance of biometric authentication systems, works presented in this paper combines two unimodal system to show considerable improvements in the authentication performance. Our future work will continue on login and live image capturing processes.The future of biometrics will so be envisaged to perhaps belong to multimodal biometric systems.

References

[1]. Cavoukian, Ann, and Alex Stoianov. "Biometric encryption: The new breed of untraceable biometrics." Biometrics: Theory, Methods, and Applications (2009): 655-718.

[2]. A. K. Jain, R. Bolle, and S. Pankanti, "Biometrics: personal identification in networked society",vol. 1. 1999, p. 434.

[3]. Arun Ross and Anil K. Jain, "Multimodal biometrics: An overview", appeared in Proc. of 12th European Signal Processing Conference (EUSIPCO), (Vienna, Austria), pp. 1221-1224, September 2004.

[4]. Deepika, C. Lakshmi, and A. Kandaswamy. "An algorithm for improved accuracy in unimodal biometric systems through fusion of multiple feature sets." *ICGST-GVIP Journal* 9.3 (2009): 33-40.

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

[6]. Hassan Soliman,"Feature Level Fusion of Palm Veins and Signature Biometrics," International Journal of Video & Image Processing and Network Security IJVIPNS-IJENS Vol: 12 No: 01 28.

[7]. Jain, K, Anil., Ross, Arun., and Prabhakar,Salil., "An Introduction to Biometric Recognition", Published in IEEE Transactions on Circuits and Systems for Video Technology, Special Issue on Image- and Video-Based Biometrics, Vol. 14, No. 1, pp.1782-1793, 2004.

[8]. J. Daugman, "How Iris Recognition Works", IEEE Trans. on Circuits and Systems for Video Technology, Vol. 14, No. 1, pp. 21-30, January 2004.

[9]. Daugman, John. "Probing the uniqueness and randomness of IrisCodes: Results from 200 billion iris pair comparisons." Proceedings of the IEEE 94.11 (2006): 1927-1935.

[10]. Bansal, Tarsem, and Munish Kumar Dhir. "Analysis of Uni-Modal & Multimodal Biometric System using Iris & Fingerprint." International Journal of Advanced Research in Computer Science 6.7 (2015).

[11]. D. Maio, D. Maltoni, R. Cappelli, J. L. Wayman, A. K. Jain, "FVC2002: Fingerprint verification competition" in Proc. Int. Conf. Pattern Recognition (ICPR), Quebec City, QC, Canada, August 2002, pp. 744-747.

[12]. R. Brunelli, D. Falavigna, "Person identification using multiple cues," IEEE Transactions on Pattern Analysis and Machine Intelligence 1995.

[13]. A. Ross, A. K. Jain, "Information fusion in biometrics", Pattern Recognition Letters 24 (2003) 2115-2125.

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

[15]. S. Ben-Yacoub, Y. Abdeljaoued, and E. Mayoraz, "Fusion of face and speech data for person identity verification," IEEE Trans. Neural Networks, vol. 10, no. 5, pp. 1065-1075, 1999.

[16]. A. Ross, and A. K. JAIN, "Information fusion in biometric," Pattern Recognition Letters, vol. 24, no. 13, pp. 2115-2125, 2003.

[17]. Bansal, Tarsem, and Munish Kumar Dhir. "Analysis of Uni-Modal & Multimodal Biometric System using Iris & Fingerprint." International Journal of Advanced Research in Computer Science 6.7 (2015).

[18]. Liu, Xiaomei, Kevin W. Bowyer, and Patrick J. Flynn. "Experiments with an improved iris segmentation algorithm." *Fourth IEEE Workshop on Automatic Identification Advanced Technologies (AutoID'05)*. IEEE, 2005.

[19]. Proenca, Hugo, and Luis A. Alexandre. "Iris recognition: An analysis of the aliasing problem in the iris normalization stage." *2006 International Conference on Computational Intelligence and Security*. Vol. 2. IEEE, 2006.

[20]. F. Chen, J. Zhou and C. Yang, “Reconstructing Orientation Field from Fingerprint Minutiae to Improve Minutiae Matching Accuracy”, IEEE Transactions on Image Processing, vol. 18, no. 7, 2009, pp. 1665-1670.

[21]. H. Choi, K. Choi and J. Kim, “Fingerprint Matching Incorporating Ridge Features With Minutiae”, IEEE Transactions on Information Forensics and Security, vol. 6, no. 2, 2011, pp. 338-345.

[22]. Maltoni D, Maio D, Jain AK, Prabhakar S. Handbook of fingerprint recognition. Springer Science & Business Media; 2009 Apr 21.