WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

A Multimodal Biometric Verification System using Traits

V.Dharani[1], T. Sushmitha[2], B. Ganesh[3], K. Venkata Lalitha Bhavani[4]

[1,2,3,4]Department of Electronics and Communication Engineering, AITAM, College, Tekkali, Srikakulam, Andhra Pradesh,532201.

ABSTRACT :

Generally Password, pin and signature are used as single source for identification of persons. There is a chance to lost or stolen. In Biometric system a person can be identified through traits .they may be physical or biological. These traits are fingerprint, Voice, Face, Iris and so on . Biometric system is more robust. The main advantage is when a person is identified with trait cannot be forgotten or guessed easily. Main aim of this paper is to develop a new biometric authentication system with different modalities like face, voice and fingerprint.

Keywords : Traits, Multimodal biometric.

1. Introduction:

A Biometric Authentication System is essentially a means of measuring unique characteristics of human beings[1]. There are two types of authentication system. They are physiological Mode are behavioural characteristics. The physiological characteristics are Fingerprint, Palm print, Face, iris etc. and behavioural characteristics are voice andsignature etc. .It involves two mode of operation one is verification Mode and another one is identification mode. In verification mode used for capturing the data and comparing the and the biometric with template which is already kept in system databaseif it matched then person gets verified it is based on one to one search basis. In the identification mode the biometric trait data is acquired and compare with existing biometric trait data of several other persons which are stored in data base. It is one to many search basis. Multimodal Biometric System includes two or more biometric modalities in an authentication system. By using various modalities recognition accuracy can be enhanced and overcome the limitations of uni-modal[2] . In this model, input traits like fingerprint, face and voice information are acquired and these are combined with various combinations of two traits like face and voice, fingerprint and voice.

The implementation of this model can be done in various steps as follows. Features are extracted individually from the pre-processed traits of face, fingerprint and voice. The individual features are distributed and then classified using Gaussian mixture model where classified into vectors and these are integrated using by score level fusion which is based on maximum score value among the traits[3]. Fusion of biometric traits improves recognition performance and reduces false access. After that a new fusion vector is generated and stored as a training database. Similarly the same procedure implemented for generating testing dataset. Using correlation method testing dataset is compared with existing training dataset which decides whether the person is genuine or an imposter.

2. Literature Survey

A review of multimodal biometric system with Fast Fourier Transform (FFT)by Gualberto Aguilar, gabor Filters combination to enhance the image and later a novel stage of recognition using Local Features and Statistical Parameters[4]. The reason to use Gabor Filters is to eliminate the problem of handle high curvature regions, since the enhancement by means of FFT presents a very robust even near regions of high curvature but marked by large storage requirements. The results by them show an elevated percentage of recognition for an application of regular size.

A review of multimodal biometric system based on fingerprint and iris recognition by Feten Besbes[13].This proposed system is tested with database of grayscale fingerprints and eye images. The final decision of their system uses the operator "AND" between decision coming from the fingerprint recognition step and that coming from the iris recognition one. Their results have shown that the method given by them performs well.

A multimodal recognition system by using feature- level fusion of normalized features by Gaurav Jaswal[9].The mined palm ROI samples go through some rotation and illumination effects that bound the matching performance. ROI samples are geometrically arranged first and then changed into illumination invariant structure using CS-LBP. Additionally, local key points of transformed ROI images are mined using SURF descriptor. The performance of this multimodal recognition system is established to be better to each and every individual modality in addition to the reported state of the art systems.

K. Rajesh P. Kartik S. R. Mahadeva Prasanna J.S. Sahamb The recognition of individuals through automated means based on a feature vectors that are derived from their physiological and/or behavioural characteristics is known as biometric recognition[1].For the purpose of confirming or establishing

the identity of an individual, biometric recognition systems must offer dependable personal recognition protocols. Such systems have diverse applications, including the security of computer systems, electronic banking, mobile phones, credit cards, building access control, and access to health and social services

Elhoseny et al. (2018) proposed a method for multi-modal biometric personal identification and verification, which involves five levels of fusion in multimodal biometric systems[8].The first level of fusion is the sensor level, in which the raw data captured by the sensor are combined. At the feature level, the features created from each user biometric process are combined to create a single feature set. The score level involves the fusion of match scores provided by different matches which represent the degree of similarity between the input and stored templates, to reach the final decision. At the rank level, each biometric subsystem assigns a rank to each enrolled identity, and the ranks from the subsystems are combined to obtain a new rank for each identity

3. Methodology:

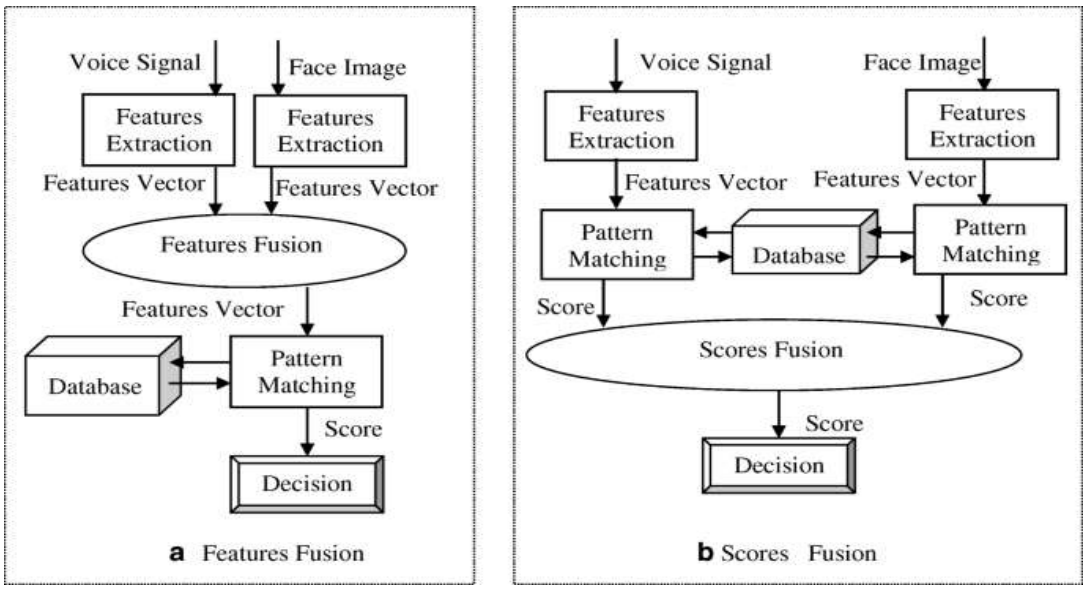

Fig 1 Block diagram of Proposed system

Fig 1 Displays the block diagram of the authentication Multimodal System using the traits face, voice and finger print. The majority of biometric systems used in practical applications rely on a single source of information for authentication, making them unimodal. For example, such sources of information can be fingerprints, faces, voices, and so on. Despite the advantages of biometric systems, While biometric authentication systems offer many benefits, they are not perfect and can be susceptible to various issues. In addition, these systems may have performance upper bounds and lack permanence, meaning that they may become less accurate over time as people's faces and voices change. Spoofing attacks, where an attacker attempts to impersonate a legitimate user, can also be a concern. To address these limitations, multimodal biometric systems have been developed that integrate multiple sources of information for identity verification. These systems combine two or more types of biometric systems to enhance their reliability, as they rely on multiple independent biometrics for identification. As a result, multimodal biometric systems are more dependable and robust compared to unimodal systems. the system in question appears to be discussing methods of preventing spoofing in biometric authentication. By requesting a random subset of biometric traits from the individual during the authentication process, it becomes more challenging for fraudsters to impersonate them, as they would need to replicate multiple biometric traits simultaneously. This technique helps to enhance the security of biometric authentication systems and improve their resistance to attacks, such as spoofing, where an attacker attempts to use fake biometric data to gain unauthorized access to a system. This approach also allows for a challenge-response type of authentication, which confirms that the live individual is indeed present at the time of the data accession. Facial recognition technology is the term used to refer to the process of identifying or confirming an individual's identity through their facial features. This technology captures, assesses, and matches facial attributes to identify individuals by analysing patterns in their facial features. The way fingerprint recognition technology works is by obtaining a person's fingerprint and identifying its unique patterns, measurements, and textures. In order to capture a trait the captured fingerprint image is compared to data base in which the image is already stored that is shown in Fig1.0 Voice authentication is also useful for speech-recognition devices such as Google Home or Amazon’s Alexa. In the voice authentication the cost is less to integrate into other devices such as automobiles and home appliances. Voice is a type of speech recognition system which is convenient and familiar for most users. Voice authentication can have training mode and the recognition mode.

4. Implementation of Single Trait

4.1 Face Authentication System:

In this section, face trait biometric authentication system is discussed. Face images are acquired by using webcam and then pre-processed. Feature extraction is done on pre- processed images and then distributed data for classification. Finally, results are obtained by comparing the input trait with existing dataset. The entire process of face recognition is divided in various phases which are shown in Fig 2.

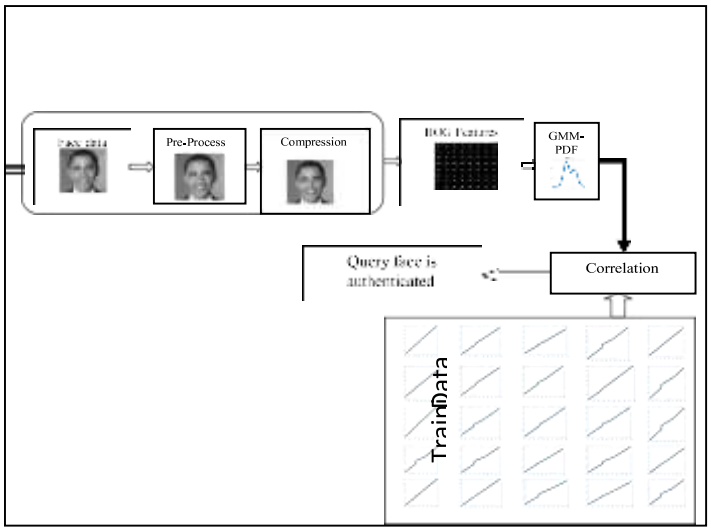

Fig 2. Face recognition system

If the correlation value is less than the threshold value then query image is not authenticated. If the correlation value is greater than or equal to the threshold value, then the query image is authenticated.

4.2 Fingerprint Authentication System

In this authentication system fingerprint recognition is a type technology, which extracts features like minutiae from impressions made with the more ridges on the finger tips [4] and [5]. The fingerprints should be flat or rolled. A flat print include only an impression of the central area between the finger tip and the first knuckle, whereas a rolled print takes ridge on both

sides of the finger which is used in our biometric system. The process which involves an optical scanner capturing an image of a fingerprint, which is then improved and transformed into a template, as illustrated in the figure.

Fingerprint recognition is an automated process of verifying a match between two human fingerprints, which is one of the many biometric methods used to identify and verify individuals. Fingerprint recognition algorithms primarily extract the unique characteristics of the fingerprint images in order to establish their distinctiveness. It is known that every individual has a unique and unchangeable set of fingerprints shown in Fig 3.

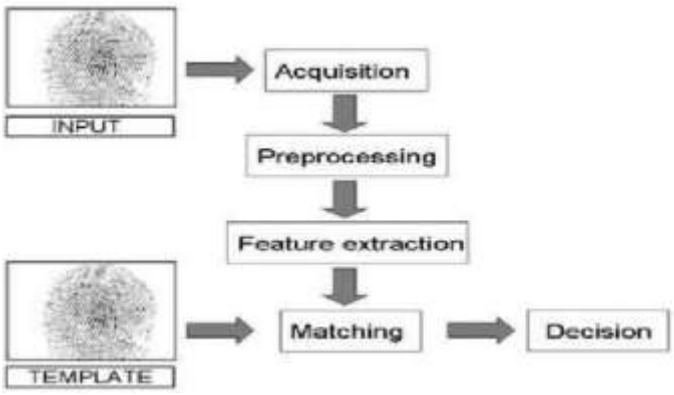

Fig 3.Fingerprint recognition system

4.3 Voice Authentication System

In this section, Voice trait biometric authentication system is discussed. Voice images are acquired from and then pre-processed. Feature extraction is done on pre-processed images and then distributed data for classification. Finally, results are obtained by comparing the input trait with existing dataset. The entire process of voice recognition is divided in various phases which are shown in Fig 4 .

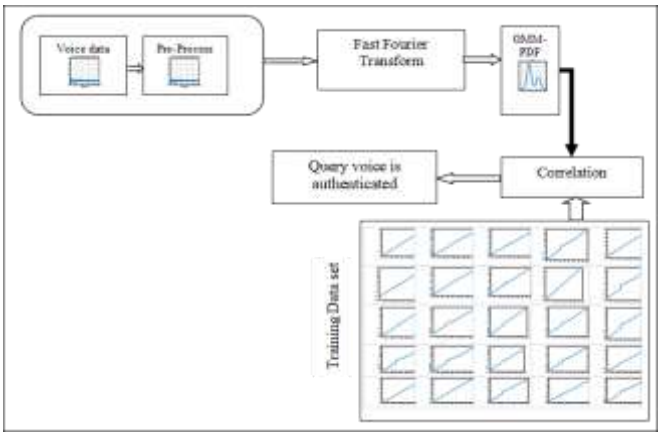

Fig 4. Voice recognition system.

If the correlation value is less than the threshold value then query image is not authenticated. If the correlation value is greater than or equal to the threshold value, then the query image is authenticated.

5. Fusion of Traits

5.1 Fusion of Face and voice

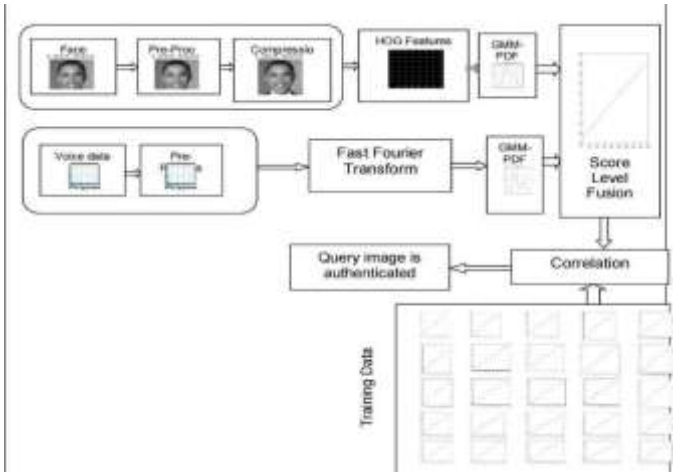

Fig 5. Face and Voice recognition system

Fig 5 shows recognition systems of face and voice. In this section a new biometric authentication system by using face and voice traits is experimented. These traits are integrated by using score level fusion. Feature vectors are extracted individually from the pre-processed traits of Face and voice [6]. The individual feature vectors are distributed and then classified using Gaussian Mixture model. The individual classified vectors are integrated based on maximum score between both the traits. Finally, a new fusion vector is created and stored in training database. The correlation method declares whether the person is genuine or an imposter . The individual recognized by this systemis more reliable than the uni-modal biometric systems. Fusion of two biometric traits improves recognition performance and reduces false access.

To overcome the troubles faced in single trait biometric recognizers like voice signal, palm print, fingerprint, or face based models; a new combination is projected for the recognition system. The integrated system provides anti-spoofing measures, high efficiency, robustness, and more security. The proposed model is divided into six phases. In the first phase, traits of each user are acquired by using appropriate device and then pre-processed. In the second phase, feature extraction is implemented. In third phase, the data is distributed based on weights. In the fourth phase, fusion of the Gaussian values using score level fusion is done. In fifth phase, testing data is compared with trainee data by using correlation. Finally, in sixth phase, the result to know whether user is genuine or an imposter is obtained.

5.2 Fusion of Face and Finger Print

The integration of information at feature and decision levels leads to more accurate and reliable identification of individuals, with enhanced security and reduced risk of spoofing attacks[7]. Moreover, the proposed system can be applied in various applications, such as access control systems, e-commerce transactions, and secure identification for financial transactions. The use of multimodal biometric systems in such applications enhances the security and reliability of the system, providing a more robust and effective mechanism for identity verification. Recognition system of both Face and Fingerprint shown in Fig 6

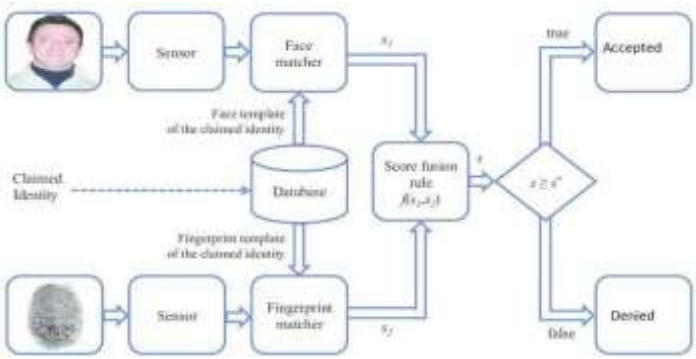

Fig 6. Face and Finger print recognition system

6. Implementation of Multimodal Authentication System

The system may either accept an imposter or reject a genuine user. To overcome these limitations, multi-modal biometric systems have been developed, which combine multiple sources of information for authentication [8] and [9]. These systems are more reliable as they use independent biometric traits, and the likelihood of an imposter having multiple matching traits is significantly lower. The integration of multiple sources of information at different levels of the system, such as feature level and decision level, can also improve the overall accuracy and robustness of the biometric system limited discrimination capability, upper bound in performance and lack of permanence. Multimodal biometric systems, which integrate multiple sources of biometric data such as fingerprints, face, voice, iris, etc., can improve the accuracy and reliability. These systems are more dependable because they make use of multiple, independent biometric sources. Multimodal biometric systems can improve the performance of biometric combining multiple sources of biometric information[8].This can help overcome some of the limitations faced by unimodal biometric systems, such as noisy data, intra-class variations, inter-class similarities, lack of universality, and spoofing. The integration of multiple biometric traits makes it more difficult for an attacker to spoof or deceive the system, thus enhancing its security and accuracy. These systems are able to meet the stringent performance requirements imposed by various applications. They address the problem of non- universality, since multiple traits ensure sufficient population coverage. They also deter spoofing since it would be difficult for an impostor to spoof multiple biometric traits of a genuine user simultaneously. Furthermore, they can facilitate a challenge – response type of mechanism by requesting the user to present a random subset of biometric traits thereby ensuring that a ‘live’ user is indeed present at the point of data acquisition.

Fused multimodal biometric system is the recorded biometric data is pre-processed to enhance the quality of the data, which is then processed to extract features that represent the biometric trait [9]. This feature extraction process is specific to the type of biometric trait being used, such as fingerprint or face recognition. In the verification module, the user provides their biometric data through the same sensor or reader as used in the enrolment phase. The raw biometric data is again pre-processed and the features are extracted. The extracted features are then fused using a suitable fusion technique, such as feature level fusion or decision level fusion. The fused features are compared with the previously stored template to verify the user's identity. If the fused features match the template within a specified threshold, the user is granted access. Otherwise, the system rejects the user's identity and denies access.

The feature extraction of three biometric traits fused using feature level fusion and encrypted using RSA and stored in a database for desired authentication and verification[9].This then facilitates the next process of verification module, in which the user claims an uniqueness and the scheme verifies whether the claim is genuine or in poster. By combining the different biometric indicators, the system can increase accuracy and security by making it more difficult for an impostor to fake or spoof both indicators simultaneously[10].

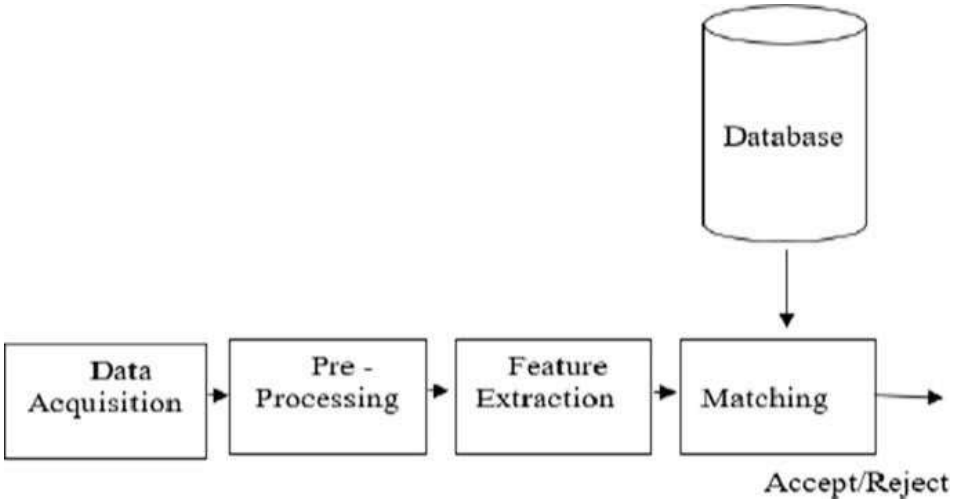

Fig 7. Block diagram of the Multimodal Biometric Authentication System

Fig 7. Displays the block diagram of the Multimodal Biometric authentication System

6.1 Gaussian Mixture Modal

In this stage, after extracting the features from face image trait and voice signal, the result is in the format of vector with length 1 x 34536 [14]. These vector values are random values and need to classify the data using Gaussian Mixture model. Then classify entire feature vector is classified and the result is given as2 x 434 vector.

6.2 Score Level Fusion

Score level fusion is also known as measurement or confidence level fusion[14]. Using score level fusion, the results of GMM vectors of both face and voice are compared, then integrated into a new single vector by using SCL based on maximum score. The result of new vector size is 2x434 after the fusion. This process is also repeated for remaining traits and makes a new training dataset. This is achieved by considering (x_{ij}, y_{ij}) and (x_{ik},y_{ik}) as pixels of two different images, where *i* indicate position of pixel and *j, k* indicates image number. A new fused image (x_n, y_n) is formed by fusing above two images based on the following conditions.

7. Conclusion

Compared to unimodal biometric systems, a multimodal biometric recognition system is typically more reliable and efficient for real-time authentication systems. By combining multiple biometric traits, such as fingerprint, face, voice, etc., a multimodal system can achieve higher accuracy. Additionally, multimodal biometric systems can offer better security and confidentiality by utilizing fusion strategies to arrive at a final decision. In the experiment the results have shown that utilizing convolutional neural networks for training, bracketing, and testing in a proposed system has improved the performance of biometric authentication. The system exhibited better sensitivity, which is suitable for an access control system. Utilizing convolutional neural networks for feature extraction, training, bracketing, and testing can reduce complexity and dimensionality in multimodal biometric recognition systems, resulting in improved recognition sensitivity. Moreover, it is both efficient and effective to integrate this approach for specific identification purposes. Future studies should explore the impact of similar optimization learning algorithms on a multimodal system that incorporates different biometric traits and experiments with datasets containing a smaller number of subjects. A multimodal biometric system can enhance the security and confidentiality of stored data. A multimodal biometric system employs fusion strategies to combine inputs from each subsystem and arrive at a final decision. This improves the accuracy of a multimodal system.

7.1 Results:

The comparison of query image with existed image shown in Fig 8. below

Fig 8. correlated Images

Fig 9 It shows that when the given password is correct and input and existed traits are same, it displays that the output accepted**.**

Fig 9. Access is accepted

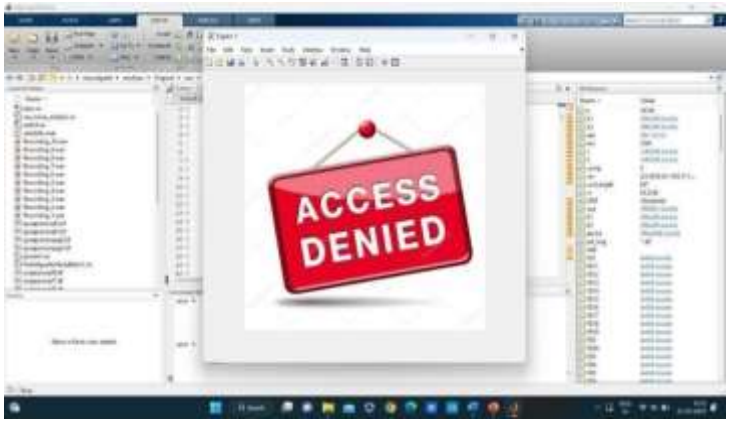

Fig 10. Unmatched traits

Fig 10. It shows that when the given password is incorrect and both input and existing traits are different, it displays that output is denied.

References:

1. K. Jain, A. Ross and S. Prabhakar, “An introduction to biometric recognition”. IEEE Transaction son Circuits and Systems for Video Technology, vol. 14, pp. 4–20, Jan 2004.
2. Roohie Naaz Mir, A Survey on “Biometric Recognition Techniques” January 2015
3. Kabir W., Ahmad M. O., and Swamy M. N., “A multi-biometric system based on feature and score level fusions,” IEEE Access, vol. 7, pp. 59437-59450, 2019, doi: 10.1109/ACCESS.2019.2914992.

4. Aguilar G, Sánchez G, Toscano K, Nakano M, Pérez H., "Multimodal biometric system using fingerprint", International Conference on Intelligent and Advanced Systems, pp. 145-150, 2007.
5. D. Maltoni, D. Maio, A.K. Jain, and S. Prabhakar, Handbook of Fingerprint Recognition. Springer,2003.[9] Sasidhar, K., Kakulapati, V.L., Ramakrishna, K., Kailasa, R.K., Multimodal biometric systems – studyto improve accuracy and performance, International Journal of Computer Science and Engineering Survey, vol. 1,no. 2, 2010, p. 54-61.
6. S. Ben-Yacoub, Y. Abdeljaoued, and E. Mayoraz, "Fusion of Face and Speech Data forPerson IdentityVerification," IEEE Trans. Neural Networks, vol. 10, no. 5, pp. 1065- 1075,1999.
7. L. Hong and A.K. Jain, "Integrating Faces and Fingerprints for Personal
8. Identification," IEEE Trans.Pattern Analysis and Machine Intelligence, vol. 20, no. 12, pp. 1295-1307, Dec. 1998.
9. Elhoseny,et.al,[2018] "Multi modal biometric personal identification and verification." Jaswal G, Kaul A, Nath R., "Multimodal Biometric Authentication System Using Hand Shape, Palm Print, and Hand Geometry", Computational Intelligence: Theories, Applications and Future Directions, pp. 557-570, 2019.
10. S. Aruna Irani, R. Gobinath "Literature review on multimodal Biometrics" International Journal of Engineering & Technology, 7 (2.26) (2018) 31-34
11. M. Indovina, U. Uludag, R. Snelick, A. Mink, and A. Jain, "Multimodal Biometric Authentication Methods: A COTS Approach,"
12. R.Frischholz, U. Dieckman. "A Multimodal Biometric Identification System", IEEE Computer, 33(2): pp. 64- 68, 2000
13. Besbes F, Trichili H, Solaiman B., "Multimodal biometric system based on fingerprint identification and iris recognition", International Conference on Information and Communication Technologies: From Theory to Applications, pp. 1-5, 2008.