

A Multi Model Biometric System Based On Feature Fusion Method For Secure Entrance System

Shashank Tripathi¹, Jai Mungi², Dr. Kalpana Rai³, Sneha Soni⁴, Rajdeep Singh⁵

¹M.Tech Scholar, ^{2,4,5}Assistant Professor, ³Professor,

^{1,2,3,4,5}Department of Computer Science Engineering

^{1,2,3,4,5}Sagar Institute of Research & Technology Excellence, Bhopal [M.P.]

Abstract : Multi biometric system used to enhanced accuracy of the authentication process and also reduce error rates. Person identification required in many systems such as area-access control, PC login, e-commerce etc. The biometric system is most probably used for security purpose. Uni modal biometric and multimodal biometric are the two frameworks of biometric systems. A single biometric trait is used in uni modal system, where more than one biometric traits are used in multimodal system. Multimodal framework is more precise as contrast with uni modal biometric framework. During this proposed work discuss the various sort of biometric systems i.e., uni modal and multimodal. Conjointly discuss the comparison of various previous modal in biometric system and its comparative analysis. The comparison of receptive technique relies on multi modal system. In day to day the demand of biometric system will increase. Drawbacks are also shown of uni modal system, that why demand of multimodal is additionally will increase. During this analysis work principally discuss the uni modal and multimodal based mostly previous work. In proposed multi biometric system two traits are combined such as fingerprint, iris. The standard database is used to evaluate the proposed system. Various features are taken from every trait by using different features extraction algorithms. Matching score of these extracted features are calculated separately. These individual scores are combines together by using weighted fusion technique. As per the observation 96 % accuracy is achieved, which overcome the limitations of present system.

Index Terms - Multi-modal Bio-metrics, Weighted Score Level Fusion, Minutia Point and Extraction Algorithm.

I. INTRODUCTION

Biometric technology is the one among technologies in the scientific area. Nowadays, biometric technologies are applied in various areas, from the work entrance organization to the person identification among the payment transactions Biometrics are an active area of research in pattern recognition and machine learning community. It is an integral component of identity science, and biometric modalities such as the face, fingerprint, iris, and voice are being applied to recognize an individual. It offers a very convenient and secure mode of identification and verification solutions. It is used in several applications like computer network login, electronic data security, e-commerce, Internet access, ATM, credit card, physical access control, cellular phone, PDA, medical records management, distance learning. In this technology,

biometric systems rely on particular data about unique biological traits to unique work effectively. There are two types of biometric systems such as the uni modal biometric system and the multimodal biometric system. In this, uni modal biometric systems that use only one biometric trait for recognition often affect issues such as biometric data variation, lack of distinctiveness, low recognition accuracy, and spoof attacks. To discover the problem, multimodal biometric systems are used. Cloud computing is an advanced technology, which deliver services without direct management of user, based on the demand of resources. It is highly scalable, robust and provides access to the data anywhere at any time. It supports performing complex, high-scale operations over cloud environment. The key advantage of this technology is in ensuring better resource management, access control and security. Biometrics refers to physical measurement and its related calculations of human body. These metrics can be directly related to the characteristics, otherwise modalities of the human. Also, these metrics are used in most of the authentication schemes via access control systems. Some traits are said to be fingerprint, iris, palm print, retina, DNA, voice, gait etc. The traits of every individual are collected, processed, stored in a database and this process is called as enrollment. Then during verification process, the user is authenticated via an access control scheme such as fingerprint authentication. The importance of biometrics lies in its uniqueness in the pattern of every individual. Uni-modal biometric systems are fairly outdated, have many drawbacks and used only in some scenarios where the security is not a big concern. Fusing more than a trait is called a Multimodal biometric system. The robustness of the system is high with multimodal authentication process.

II. LITERATURE SURVEY

Purohit, et.al., [2021], "Optimal feature level fusion for secured human authentication in multimodal biometric system." In this paper, we suggested an effective feature level fusion method for multimodal biometric recognition system. We considered the multimodal biometric feature level fusion like a fingerprint, ear, and palm. In our proposed method, we did four main processes such as preprocessing, feature extraction, optimal feature level fusion, and recognition. We used a modified region growing algorithm for extract the shape features and we used HMSB operator for extracting texture features. Moreover, we selected the relevant features with the help of the optimization technique. For selecting the optimal feature, we used the OGWO + LQ algorithm. In final we proposed recognition, for the recognition we used the multi-kernel support vector machine (MK SVM) algorithm. The performance of our suggested method is evaluated in terms of evaluation metrics such as sensitivity, specificity, and accuracy. The experimental results and comparative analysis demonstrates that our proposed method effectively gives better sensitivity, specificity, and accuracy results than other existing methods. So, the efficiency of our proposed method is very helpful for the multimodal biometric recognition system effectively. Convolution neural network based person authentication modelling is efficient way to implement a multimodal biometric system on hardware. CNN based Implementation of our proposed work would be a future task to accomplish. [01]Leghari, et. al, [2021], "Deep Feature Fusion of Fingerprint and Online Signature for Multi

modal Bio-metrics.", In this paper, deep learning models based on the CNN architecture have been proposed for the feature level fusion of online signatures and fingerprints. Two feature fusion techniques, that is, early and late have been developed where the features extracted from both biometric modalities are fused together at convolution and fully connected layers. The size of the input image for the fingerprint is fixed to $150 \times 150 \times 1$ and the size of the online signature file is 1×17 . To fuse the features of fingerprint and online signature, the size of the signature was reshaped to $1 \times 17 \times 1$ before passing to the online signature network. To fuse the features of fingerprint image and online signature, different approaches were tried. However, the accuracy and other values for other evaluation metrics for the proposed system did not improve because of the width of the online signature's feature vector which was equal to 1. The problem was addressed and the accuracy and the values for other evaluation metrics for the system was increased by adding two zero-padding layers in the signature network. By this zero-padding technique, the extra zeros were added at all four sides of the feature vector, that is, top, bottom, left and right. In this way, the dimensions of the final feature vector became 4×4 in size. Similarly, the size of final feature vector of fingerprint was 4×4 . These features have been fused by concatenation and passed the fully connected layers for more abstract feature extraction and classification. The model was trained and tested on the new collected data set and finally, the overall system achieved an accuracy of 99.10% with early fusion scheme and 98.35% with the late fusion scheme. In future, low level characteristics or level 3 features of the fingerprint like ridge contours and active sweat pores may also be used for the fusion to ensure more accuracy and liveness of a user. In future one of the different-state-of-the-art cryptography techniques for bio-metrics may also be applied to the proposed system to further ensure the security of the fused biometric template.

[02]Conti,et.al., [2021], "A multi modal retina-iris biometric system using the Levenshtein distance for spatial feature comparison." IET Bio-metrics 10, no. 1. This work aimed to investigate a system that leverages the best performing biometric features, namely, retina and iris. The proposed multi modal system exploited iris and retina, as well as the an innovative way, allowing us to overcome the typical issues in spatial approaches, often due to misalignment of the templates to be compared. The tests aimed at evaluating the performance of the multi modal retina-iris system on multiple retina and iris database configurations. The authors used publicly available databases accessible by the scientific community allowing for result re productivity and comparability. In order to provide comprehensive results, the authors plotted the DET curves, as well as calculated the AUC, EER and FMR1000 metrics. The best FAR and FRR values achieved by our multi modal biometric approach were 0% and 3.33%, respectively. The multi modal retina-iris approach out performed the corresponding uni modal systems, so drawing out its potential in authentication systems. Therefore, these experimental findings showed that our multi modal solution can guarantee a high level of reliability and be beneficial to computer security applications. Adaptive weights for the comparison score-level fusion might be employed to cope with the variability of the environmental conditions that could affect the quality of the traits acquired by the biometric sensors. For this reason, it might be useful to consider variable weights in order to dynamically manage this variability, as proposed in [03]. Since the authors analyse biometric images acquired in 'controlled' environments, the use of dynamic weights is not mandatory. The authors are currently attempting to increase the size of the tested 'virtual' multi modal retina-iris database to validate our approach on a large-scale database. With the goal of keeping result re productivity and comparability, more public available databases might be combined to achieve larger datasets, such as in the particular case of retina data bases. However, it is worth noting that the majority of retina databases were collected for the research and analysis in clinical scenarios tailored to anomaly or disease detection (e.g. diabetic retinopathy, glaucoma) and are not suitable for biometric purposes. In the near future, the authors aim to extend the same multi modal approach with other static biometric features that allow for identifying and extracting the minutiae in the spatial domain. As a matter of fact, The authors plan to develop a multi modal framework with a fusion scheme at the template-level to combine and standardize multiple biometric approaches into one system in order to obtain a novel universal approach for any type of static biometric features.

[03]Joseph,et.al,[2020], "A multi modal biometric authentication scheme based on feature fusion for improving security in cloud environment" Authentication is an important factor on ensuring security for various applications. Cloud computing is an internet based model for providing service to various end users related to information technology. It provides high flexibility for the users, so the usability of cloud services is increasing gradually. Also, it makes the concern about data security to some extent. Multi modal biometric system enhances the robustness of the authentication mechanism because of its inherent unique biological patterns. It accurately discriminates the individuals based on the captured pattern from their traits. Moreover, this concept can be applied in various applications to improve the robustness of the system such as securing human genetic code and health information for future reference using Electronic Health Record (EHR) management, digital ledger management, etc. In this work, a multi modal biometric authentication mechanism is proposed to make data in cloud environment more secure. A secret key is generated by fusing the features extracted from fingerprint, iris and palm print in multiple stages and finally converted into hash of strings and numbers using MD-5 hashing algorithm. The data to be secured is then encrypted by the secret key with three symmetric key encryption algorithms DES, AES and Blowfish. Among them DES takes less execution time, but AES has better performance when compared with other two algorithms based on the strength of encryption process. This model proved its robustness in data security due to the fusion of human modalities as a part of framing the security mechanism.

[04]Mustafa,et.al.,[2020], "Multi modal Biometric System Iris and Fingerprint Recognition Based on Fusion Technique." The advancements in sensing & multi modal communication technologies have increased the complexity of multi modal biometric recognition (MBR); the existence of high dimensional richer input biometric data information has also contributed to this complexity of MBR. In this paper, multi modal fusion techniques system was proposed based on the combination of features extracted from iris and fingerprint images using the GLCM algorithm. The existing works related to iris and fingerprint were reviewed before recommending the proposed recognition system. The decision on the fusion technique depended on the AND gate to make the final decision. The results of the study showed that the proposed system achieved high accuracy rate based on the suggested threshold of up to 90% with KNN classifier. The evaluation of the system was based on the FAR, FRR, and total accuracy rate.

[05]Chanukya, et.al,[2019] "Multi modal biometric cryptosystem for human authentication using fingerprint and ear." An innovative optimal neural network based biometric image classification method with three diverse phases such as the Pre processing, Feature Extraction and classification is elegantly launched in this document. The novel technique commences with the task of pre processing involving the median filters. It is followed by the feature extraction stage in which various features are effectively extorted from the biometric images. The extracted features include the shape and texture feature like the fingerprint and ear feature. The ONN technique admirably classifies the images. The efficiency metrics such as the False Positive Rate, False Negative Rate, sensitivity, specificity and accuracy are successfully estimated for the new-fangled technique, which comes out in flying colors in classifying the images with superlative efficacy, thereby accomplishing sterling efficiency in the task of classification of images and turning out cheering outcomes of amazing

accuracy.[6] Elhoseny,et.al,[2018] "Multi modal biometric personal identification and verification." Most Security systems can be considered as one of these three types; knowledge based; "What you know" like PIN, passwords, or ID however it may be guessed, forgotten, or shared. Another type is token "What you have" like cards, or key; it may be lost or duplicated and it can be stolen. Last type is the use of bio-metrics; "What you are" like fingerprint, IRIS, face etc. Biometric identification systems have the ability to recognize individuals by measuring and analyzing physiological or behavioral characteristics and comparing them against template set stored in the database. Uni modal biometric systems suffer from some problems like noise in sensed data, non-universality, spoof attacks, intra -class variations, and inter-class similarities. Multi modal biometric system is the use of a combination of two or more biometric types to increase the security of a system (like: Fingerprint and Iris) to increase security for user identification or verification. Five levels of fusion in multi modal biometric systems: sensor level; in which raw data captured by the sensor are combined, feature level; in this level, features created from each user biometric process are combined to make a single feature set, score level; in which match scores provided by difference matches representing degree of similarity between the input and stored templates, are fused to reach the final decision, 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, and decision level; the final result for every biometric subsystem are combined to obtain final recognition decision. Multi biometric systems categorized into six different types: multi sensor; uses more than one sensor to capture biometric trait to extract various data, multi algorithm; in which more than one algorithm applied to the same biometric data, multi instance; use more than one instance of the same biometric (for example, left and right index fingers or left and right irises), multi sample; more than one sample of the same biometric are captured using the same sensor to acquire a more complete representation of the underlying biometric, multi modal; combine evidence of two or more biometric traits, and hybrid; refers to systems using two or more of the other five mentioned categories. In this chapter a proposed system using Fingerprint and Iris recognition is presented based on minutiae extraction for fingerprint recognition and hamming distance for IRIS Recognition. The proposed system is implemented with MATLAB 7.8.0.347(R2009a) using data set from CASIA Iris V1 for Iris recognition and FVC 2000 and 2002 DB1 A for fingerprint recognition. The experiment results carried on datasets from CASIA Iris V1 for Iris recognition and FVC 2000 and 2002 DB1 A for fingerprint recognition. It compares FAR, FRR, and accuracy metrics for Fingerprint standalone recognition system and the multi modal biometric system based on Fingerprint and Iris and shows that the multi modal system results of FAR and FRR are decreased and accuracy is increased compared to the fingerprint standalone system [07] Kim,et.al,[2018] "Multi modal biometric recognition based on convolution neural network by the fusion of finger-vein and finger shape using near-infrared (NIR) camera sensor." In this study, finger-vein and finger shape multi modal bio metrics based on a deep convolution neural network (CNN) were proposed. Following are the details about what we achieved, the scientific contributions, how much important, and from which point of view, our results are different from the state of the art. First, convex polygons were generated using the algorithm that finds the coordinates of the outermost pixels of finger ROI s to calibrate the empty spaces of the images. Then, the robust finger ROI s for misalignment were extracted after conducting in-plane rotation compensation based on the angle of tilting measured based on the boundaries of the upper, lower, left, and right pixels. Second, two-dimensional spectrogram images that express finger-thickness frequency-component changes depending on the horizontal position of fingers were obtained and used as CNN inputs for finger shape recognition. Third, matching distances calculated based on the features of finger-vein and finger shape obtained using Res Net models were score fused using various fusion methods, such as the weight sum, weighted product, and perceptron. Fourth, trained CNN models and algorithms developed in this study were open through so that other researchers can use them in fair performance evaluations. Through an experiment conducted using two open databases, the accuracy of the method proposed in this study was confirmed to be higher than the state of the art, and those of existing methods and other CNN models. The experimental results revealed that most false rejection cases occurred because of misalignment between finger-vein images due to finger position changes between the enrolled and recognized images, and because of the difference between finger shape spectrogram images due to finger rolling. False acceptance cases occurred because the regions of finger were so dark or bright, and the correct boundary of finger shape could not be extracted by the highly saturated region inside of finger. To solve these problems, the study on compensation method of severe finger rolling and illumination variation is necessary as the future work. Moreover, in future study, the possibility of performance improvement by combining the multi modal recognition method proposed in this study with scattering blur-restoration methods to reduce the blurring effects in finger-vein images shall be investigated.. [8].

III. PROPOSED METHOD

The proposed multi model biometric system is design to improve the bio metric based security system enhancements. The proposed system is used to detect the unauthentic access of fake persons. Authentication is the most common problem in the secured places. For improve the security system multi model biometric system play an important role, first create the data base of the authentic persons present in secured of both Biometric finger print and iris. In the proposed work calculate the matching percentage of biometric properties from one person to other person. For the calculation of accuracy required both data training and testing data sets. In the first part of proposed method create training data set and in the second part apply image processing for authentic access and unauthentic access.

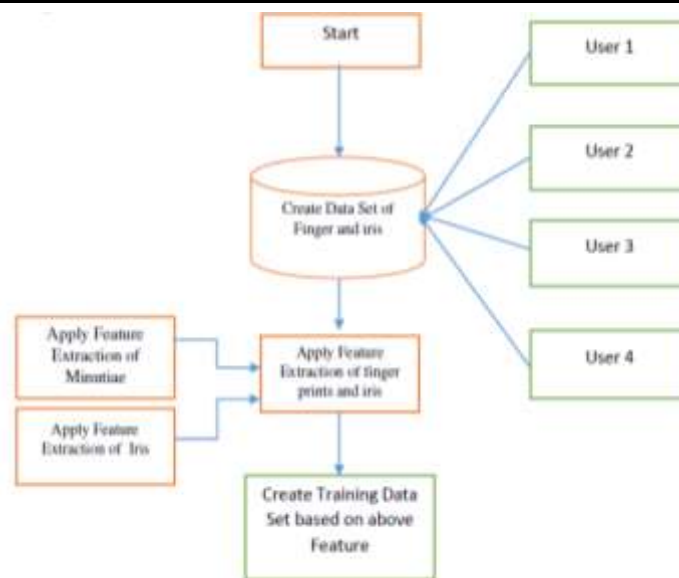


Fig .1 Training and Data set Creation

The above figure 4.1 shows the data set creation and feature extraction of different user biometric information also the take some unauthentic persons for checking the false detection.

Steps of Training Data Set creation

Step 1 – First collect the different user finger print biometric and iris images biometric which contain different properties.

Step 2 – Apply feature extraction techniques of these biometric information of different user and create a training data set. Which is used to detection the person in the authentication system. The diagram of above steps also explained in the above figure 1

Biometric Based Finger Print and Iris Matching Proposed Algorithm.

Step 1 – Query Image Selection:

First select the biometric information in the form of image from different data sets of users. The data set is the combination of the different type of biometric finger print images. There are different type of images in the data set. For selecting the image form data set using a matlab function that is uigetfile. Uigetfile is the predefined function in matlab for selecting dataset of the image. Also select the directory of image with the help cd command.

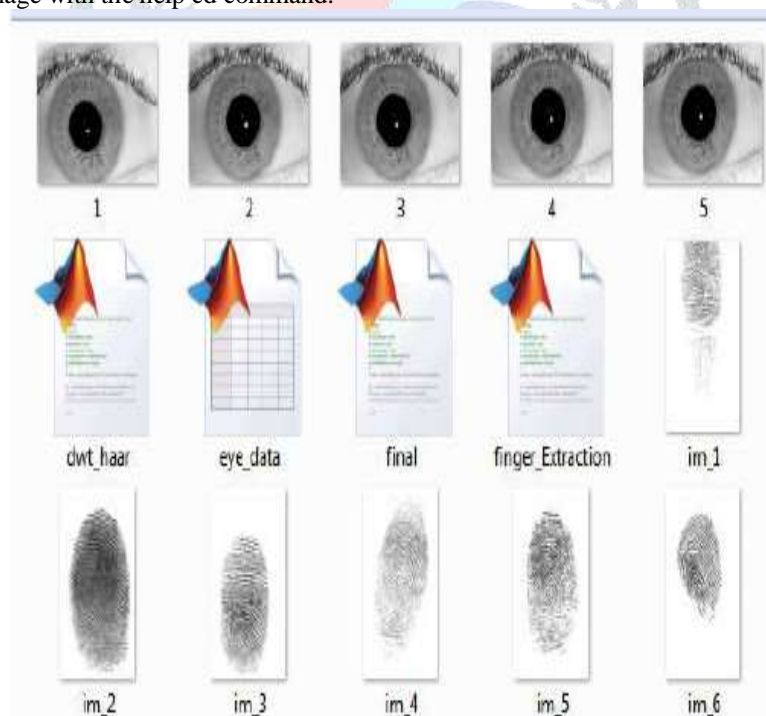


Fig. 2 Select of Biometric Based Finger Print from the different users

Step 2 – Calculate the Minutiae of the query image

After the select of image, apply this image into the pre-processing block. In this step calculate the –
Begin -

1. Binary form of the image. // `im2bw(input image)`
2. Apply Morphological Operation // `bwmorph(binary_image,'thin',Inf);`
For obtain the thin image that is shown in the below figure 3 (a).
3. Now search the ridge end finding of the thin image
4. after that find out the bifurcation finding –
5. Store the Minutiae of the image of memory. // Create .mat file
`Figure;imshow(outImg);title('Minutiae');`

Desire = bifurcation;

End

Apply the above algorithm for all the images and store all the points in the mat file for matching purpose.

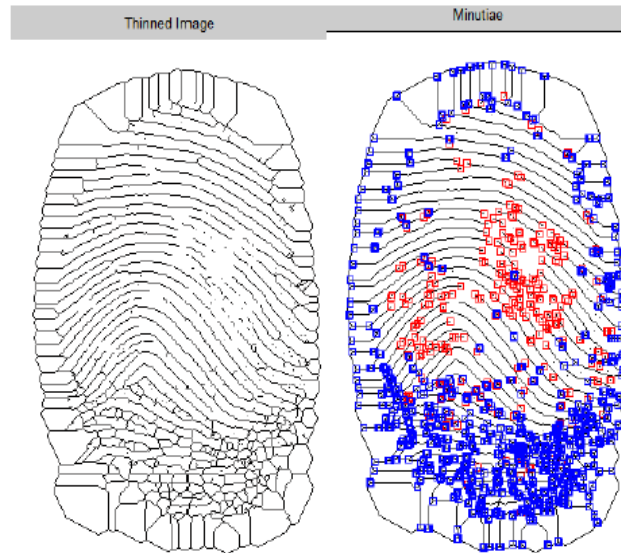


Fig.3 (a) and (b) Shows the Minutiae of the query image

Above figure 3 shows the thinned image, for the thinned image calculate the binary image of the query image used by morphology processing functions.

Step 3- Algorithm the Iris Matching – First Load testing image – Click on the load image then open this window for selected the iris print. Click on testing image and further proceed on the image

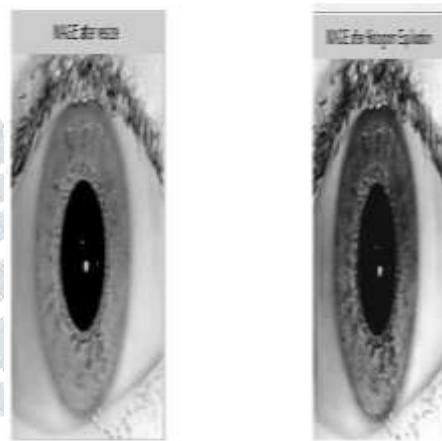


Fig Input Iris Image Fig. 4.Enhanced Query image

Fig. 4 shows the output of the test image for iris recognition

Begin

Start – 1. Take iris image // imread(input images)

2. Convert into the gray scale // rgb2gray

3. Take histogram

4. Apply edge detection

Extraction of patterns from different traits

Fingerprint

IRIS

Iris is a highly significant part of human eye. The structure inside the human eye varies between everyone. This is one of the robust ways to authenticate a user in highly secure processes (Zhang and Parhi 2002). Many approaches are successful in extracting region of interest from iris. In this system, some methods are followed, which are given below. Figure 3 shows theiris feature point extraction method.

(i) Binarization: As an initial processing of iris image, the data is binarized using Otsu thresholding technique.

(ii) The edges of the image curve are traced out by using canny edge detection method.

(iii) Boundaries of edge detected image are identified using Hough transform.

(iv) Features from the iris part is extracted using Gabor filtering technique

IV. RESULTS AND DISCUSSION

There are different result parameters in finger print matching and iris detection like percentage of matching with other person. Therefore correct person identification is the major task of the proposed work. Second result parameter is affected regions matching from different person and the last one is accuracy for that perform features matching between different iris images with the help of features matching

Classification –

The major task of proposed work is separate by machine learning the iris and finger print recognition and classification method by using image processing and soft computing techniques. Methods/Analysis: The proposed method examined the two different types of data sets of plant and iris in different images.

Finger Print Region (Area) Matching –Finger Print Region (Area) Matching of different humans calculated with the help of miniature. In the whole world each and every person having different finger prints with the help of finger print detect the person identification.

Accuracy –Multi model bio matrix system is the tedious task for researchers. Finger Print Region Matching detection a detected is a true positive (TP) whereas a real negative (TN) is unmatched detection of the person detected.

$$\text{Accuracy} = (\text{TP} + \text{TN}) / S \quad (5.1)$$

V. CONCLUSION

In this presented work, presented a multi model detection of user in this work. The multi biometric system used to overcome the problems of uni biometrics. Here the accuracy of single modal biometric system using fingerprint, and iris, obtained is higher respectively. The accuracy of the proposed system obtained is 96.4%. Proposed system develops a fusion at matching score level, which is a fastest fusion. The proposed system demonstrates the scores of three traits. These scores measure the similarity among the traits. Scores are combined to gether using weighted fusion technique. By results it can be concluded that multimodal system is precise than Single modal system. Also discuss the need of multi model and its need in the current scenario for enhancing the current single model system. Also discuss the comparison of different multi model system in last decade in multi model system.

REFERENCES

- [1] [1] Ali, Purohit, Himanshu, and Pawan K. Ajmera. "Optimal feature level fusion for secured human authentication in multimodal biometric system." *Machine Vision and Applications* 32, no. 1 (2021): 1-12.
- [2] Leghari, Mehwish, Shahzad Memon, Lachhman Das Dhomeja, Akhtar Hussain Jalbani, and Asghar Ali Chandio. "Deep Feature Fusion of Fingerprint and Online Signature for Multimodal Biometrics." *Computers* 10, no. 2 (2021): 21.
- [3] Conti, Vincenzo, Leonardo Rundo, Carmelo Militello, Valerio Mario Salerno, Salvatore Vitabile, and Sabato Marco Siniscalchi. "A multimodal retina-iris biometric system using the Levenshtein distance for spatial feature comparison." *IET Biometrics* 10, no. 1 (2021): 44-64.
- [4] Joseph, Teena, S. A. Kalaiselvan, S. U. Aswathy, R. Radhakrishnan, and A. R. Shamna. "A multimodal biometric authentication scheme based on feature fusion for improving security in cloud environment." *Journal of Ambient Intelligence and Humanized Computing* (2020): 1-9.
- [5] Mustafa, Ahmed Shamil, Aymen Jalil Abdulelah, and Abdullah Khalid Ahmed. "Multimodal Biometric System Iris and Fingerprint Recognition Based on Fusion Technique." *International Journal of Advanced Science and Technology* 29 (2020): 7423-7432.
- [6] Mustafa, Ahmed Shamil, Aymen Jalil Abdulelah, and Abdullah Khalid Ahmed. "Multimodal Biometric System Iris and Fingerprint Recognition Based on Fusion Technique." *International Journal of Advanced Science and Technology* 29 (2020): 7423-7432.
- [7] Chanukya, Padira SVVN, and T. K. Thivakaran. "Multimodal biometric cryptosystem for human authentication using fingerprint and ear." *Multimedia Tools and Applications* 79, no. 1 (2019): 659-673.
- [8] Elhoseny, Mohamed, Ahmed Elkhateb, Ahmed Sahlol, and Aboul Ella Hassanien. "Multimodal biometric personal identification and verification." In *Advances in Soft Computing and Machine Learning in Image Processing*, pp. 249-276. Springer, Cham, 2018.
- [9] Kim, Wan, Jong Min Song, and Kang Ryoung Park. "Multimodal biometric recognition based on convolutional neural network by the fusion of finger-vein and finger shape using near-infrared (NIR) camera sensor." *Sensors* 18, no. 7 (2018): 2296.
- [10] Elhoseny, Mohamed, Ehab Essa, Ahmed Elkhateb, Aboul Ella Hassanien, and Ahmed Hamad. "Cascade multimodal biometric system using fingerprint and Iris patterns." In *International conference on advanced intelligent systems and informatics*, pp. 590-599. Springer, Cham, 2017.
- [11] Gavrilova, M. L., F. Ahmed, S. Azam, P. P. Paul, W. Rahman, M. Sultana, and F. T. Zohra. "Emerging trends in security system design using the concept of social behavioural biometrics." In *Information Fusion for Cyber-Security Analytics*, pp. 229-251. Springer, Cham, 2017.
- [12] Kazimov, T., Mahmudova, S.: The role of biometric technology in information security. *Int. Res. J. Eng. Technol. (IRJET)* 2(03), 1509–1513 (2015)
- [13] George, A., Routray, A.: A score level fusion method for eye movement biometrics. *Pattern Recogn. Lett.* 82, 207–215 (2016).
- [14] Singh, R., Ross, A., Bowyer, K.W.: Special issue on information fusion in biometrics. *Inform. Fusion* 32, 1–2 (2016)
- [15] Panchal, T., Singh, A.: Multimodal biometric system. *Int. J. Adv. Res. Comput. Sci. Softw. Eng.* 3(5), 1360–1363 (2013)
- [16] Yang, W., Hu, J., Wang, S., Chen, C.: Mutual dependency of features in multimodal biometric systems. *Electron. Lett.* 51(3) 234–235 (2015)
- [17] Mai, G., Lim, M.-H., Yuen, P.C.: Binary feature fusion for discriminative and secure multi-biometric cryptosystems. *Image Vis. Comput.* 58, 254–265 (2017)

- [18] Peng, J., El-Latif, A.A.A., Li, Q., Niu, X.: Multimodal biometric authentication based on score level fusion of finger biometrics. *Optik Int. J. Light Electron. Opt.* **125**(23), 6891–6897 (2014)
- [19] Geethanjali, N., Thamaraiselvi, K.: Feature level fusion of multimodal biometrics and two tier security in ATM system. *Int.J. Comput. Appl.* **70**(14), 17–23 (2013)
- [20] Bhardwaj, S.K.: An algorithm for feature level fusion in multimodal biometric system. *Int. J. Adv. Res. Comput. Eng. Technol. (IJARCET)* **3**, 3499–3503 (2014)
- [21] Jacob, A.J., Bhuvan, N.T., Thampi, S.M.: Feature level fusion using multiple fingerprints. *Comput. Sci. New Dimens. Perspect.* **4**(1) 13–18 (2011)
- [22] Ahmad, M.I., Woo, W.L., Dlay, S.: Non-stationary feature fusion of face and palmprint multimodal biometrics. *NeuroComput.* **177**, 49–61 (2016)
- [23] Mondal, A., Kaur, A.: Comparative study of feature level and decision level fusion in multimodal biometric recognition of face ear and iris. *Int. J. Comput. Sci. Mob. Comput. (IJCSMC)* **5**(5) 822–842 (2016)
- [24] Xin, M., Xiaojun, J.: Correlation-based identification approach for multimodal biometric fusion. *J. China Univ. Posts Telecommun.* **24**(4), 34–50 (2017)
- [25] Veluchamy, S., Karlmarx, L.R.: System for multimodal biometric recognition based on finger knuckle and finger vein using feature level fusion and k-support vector machine classifier. *IET Biom.* **6**(3), 232–242 (2016)
- [26] Nagar, A., Nandakumar, K., Jain, A.K.: Multibiometric cryptosystems based on feature-level fusion. *IEEE Trans. Inform. Forens. Secur.* **7**(1), 255–268 (2012)
- [27] Yang, W., Wang, S., Hu, J., Zheng, G., Valli, C.: A fingerprint and finger-vein based cancelable multi-biometric system. *Pattern Recognit.* **78**, 242–251 (2018).
- [28] □ Pranay Yadav – “Color Image Noise Removal by Modified Adaptive Threshold Median Filter for RVIN” in National Institution of Technology (NIT - Shilong) Conference date 28 – 29 Jan. 2015. (Scopus)
- [29] □ Pranay Yadav and Parool Singh – “Color Impulse Noise Removal by Modified Unsymmetric Trimmed Median Mean Filter for FVIN” in PARK College of Engineering and Technology, Coimbatore-641659, Tamilnadu, India. IEEE International Conference on Computational Intelligence and Computing. 17 – 19 Dec. 2014 (Scopus) <http://ieeexplore.ieee.org/document/7238369/>
- [30] □ Shachi Sharma and Pranay Yadav “Removal of Fixed Valued Impulse Noise by Improved Trimmed Mean Median Filter” in PARK College of Engineering and Technology, Coimbatore-641659, Tamilnadu, India. International Conference on Computational Intelligence and Computing. 17-19 Dec 2014. (Scopus) <http://ieeexplore.ieee.org/document/7238368/>
- [31] Pranay Yadav and Vivek Kumar– “Image De-noising for Salt and Pepper Noise by Robust Mean Filter “ fourth international conference on Advances in Engineering and Technology –AET -2013 AET2013AEE547RE. http://searchdl.org/index.php/book_series/view/1521
- [32] Kumar V, Yadav P, Samadhiya A, Jain A, Tiwari P, Comparative Performance Analysis of Image De-noising Techniques, International Conference on Innovations in Engineering and Technology (ICIET) Bangkok, Thailand 2013, <http://dx.doi.org/10.15242/IIE.E1213576>