http://www.jctjournals.com ISSN(ONLINE):2278 – 3814

Volume-10, Issue-02, February 2021
JOURNAL OF COMPUTING TECHNOLOGIES (JCT)
International Journal
Page Number: 01-05

A Literature Survey On Multi Model Bio-Metric System

Shashank Tripathi[1], Jay Murgi[2], Dr. Kalpana Rai[3] Sneha Soni[4], Rajdeep Singh
[1]M.Tech Scholar, [245]Assistant Professor, [2]Professor,
[12345]Department of Computer Science Engineering
[12345]Sagar Institute of Research & Technology Excellance, Bhopal [M.P.]
[1]shashanktripathi73@gmail.com, [2]jaimsirt@gmail.com, [4]khusoni14@gmail.com

***Abstract*— In this survey paper discuss the different methods for bio metric authenticate system. In the last decade there are various research work on going related to bio metric authentication system. In this survey paper presented the various method. Bio metric authenticate system divided into two parts, uni model system and multi model system. In the uni-model system single features are used for person identification and in the multi model system use two or more then two feature to bio metric.**

***Keywords*— Multimodal Biometrics, Weighted Score Level Fusion, Minutia Point Extraction Algorithm and**

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. The service provided by cloud is expanding in different form such as Platform as a Service (PaaS), Infrastructure as a Service (IaaS), Software as a Service (SaaS) etc. (Armbrust et al. 2010). So, day by day, the number of users consuming the services of cloud is increased.The data can be stored in different cloud services where it can be accessed remotely by the user, whenever it is needed. But the major concern is in maintaining data security Since the data is in remote server, it is prone to any malicious 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 BACKGROUND STUDY

Multimodal biometric authentication system is an integral part of multiple domains such as cryptography, image processing and computer networks. A multimodal biometric system based authentication system is developed by fusing fingerprint and palm print. Histogram equalization is made to normalize the pixel intensity. For feature extraction, PCA is used and fusion of features is carried out by Gabor wavelet method. This model is developed to strengthen up the security on user authentication process A hash key based cryptographic algorithm is proposed by combining the features extracted from multimodal biometrics to enhance cloud security. Fingerprint, iris and face modalities are incorporated in this system. Features of independent modalities are extracted using various image processing techniques. To optimize the extracted features, a swarm intelligence technique called Artificial Fish Swarm (AFS) algorithm is used. The data to be stored in cloud is encrypted by AES algorithm with the generated hash key A multimodal biometric-based cloud security enhancement technique is developed by fusing three modalities. The fused vectors are bin arized, then XOR is performed between the transformed feature vectors. The final resultant key is used to encrypt the data before storing in the cloud using AES A robust authentication system for user verification is framed from face and iris modalities. Machine Learning algorithms are employed to detect the feature vectors from the image. Multilayered Perceptron and Self Organized Map neural networks are used in this process Multifactor authentication system on cloud environment is deployed with multimodal biometric scheme (MFAMB) Password-based user verification makes the data security on cloud as incomplete. This system enhances the security with multiple levels of user authentication such as password and multimodal biometric data In a similar way, a two-step verification scheme is proposed to improve cloud security on mobile communication. Iris and fingerprint modalities are used in this system for authentication of the user A biometric-based cloud authentication system is depicted to provide access control and ensuring data security using various schemes for different cloud architectures To preserve privacy in cloud, a multimodal biometric system is introduced to resist hill climbing attacks. Two-way encryption is performed in this A multimodal biometric authentication scheme based on feature fusion for improving security uni-modal or multimodal biometric encryption is performed for first level of authentication. The successor step follows the process of calculating the overlapping information on the data using Euclidean distance measure as next level A decision level fusion mechanism for multi-biometric cryptosystem is proposed to perform secure file upload in cloud. This system provides high security over authentication and integrity on access control to handle the data Context-aware models to secure cloud empowered systems are deployed using multimodal biometric methods. Three level of process is done in this system, first is to integrate class association rule into MFA-MB. Then a new metric is developed to evaluate the user experience on this system and finally to enhance the authentication on PaaS and SaaS provided by cloud An entropy-based Local Binary Pattern technique is developed in this work to extract the features from multimodal traits. The extracted features are highly robust to verify the users with low FAR and high FRR. This mechanism is embedded in cloud scenario to enhance data security The feasibility factor for generating key using different modalities is investigated in this work. Fingerprint, keystrokes and face modalities are used to test the model and achieved a fair result as an outcome. A transparen kegeneration technique is introduced to frame a key of length 256 bits.

III 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 fifingerprint, 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 modifified 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 fifinal we proposed recognition, for the recognition we used the multi-kernel support vector machine (MKSVM) algorithm. The performance of our suggested method is evaluated in terms of evaluation metrics such as sensitivity, specifificity, 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.[1]

Leghari ,et. al, [2021], "Deep Feature Fusion of Fingerprint and Online Signature for Multi modal Biometrics.", 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 × 150 × 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 × 17 × 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[2].

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 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 vali date 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 bio metric purposes. In the near future, the authors aim to extend the same multi modal approach with other static bio metric 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 an universal approach for any type of static biometric features [3].

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 Blowfsh. 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 [4].

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[5].

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 captu red 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 [7].

IV.CONCLUSIONS

In this survey paper, discuss the different presented a multi model based bio metric authentication system. In the last decade there are many research work presented related to bio metric system. In this survey paper discuss the different multi model system.

REFERENCES

[1] 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.:Ascore 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 featurelevel 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)

