IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2320-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 9, Issue 11, November 2020

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.512

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

||Volume 9, Issue 11, November 2020||

Alleviating the Challenges of Unimodal Biometrics using Multimodal Biometrics for Authentication

Sidra Shaikh

Academic Research Student, Department of Information Technology, B.K. Birla College of Arts, Science & Commerce (Autonomous), Kalyan, Maharashtra, India

ABSTRACT: Biometrics is a way of identifying or recognizing people based on their physical or behavioral characteristics. The use of biometrics for authentication purposes has skyrocketed in the recent years. It is the most secure way of authentication as it uses an individual's physical or behavioral traits which are unique to everyone. However, as it is being used extensively, the potential risks for security and privacy of our data increases. This paper focuses on the security threats of using single biometric modality such as fingerprint, voice, facial and iris recognition for authentication. It also talks about howmultimodal biometrics can help in building more robust and secure biometric systems. As the world has seen a new pandemic in the face of Covid-19, it has posed new challenges for contact-only biometric technologies as they can contribute to the transmission of the disease. Thus, forcing people to adapt to contactless biometric technologies.

KEYWORDS: Unimodal biometrics, security vulnerabilities, multimodal biometrics, impact of Covid-19, contactless biometrics.

I.INTRODUCTION

Traditionally, passwords and PINs were used as means of authentication but it was difficult to maintain them. They could get hacked or stolen easily which poses a threat to data security. Also, identification using passwords and PINs was time consuming in order to match that data with the database. Today, we are living in the era of technology and we cannot expect things to be slow. Everything is automated and so should be our authentication system. Biometric technology is the solution for this. Biometrics is the measurement of people's unique physical or behavioral characteristics. Biometric authentication uses unique biological characteristics of an individual to verify his identity. It is more convenient and secure as it cannot be stolen and provides high accuracy of recognition. Due to this, it is being widely accepted as the only means of authentication across the globe.

Biometric authentication processes generally involves three steps – enrollment, verification and identification [10]. Enrollment is the stage where the biometric data of an individual is captured and stored in the database in the form of templates. During verification, the live-captured biometric data is compared with the data stored in the database.The system basically verifies, "Are you indeed, who you claim you are?"Identification is the process in which the system checks the biometric presented against all the templates stored in the database in an attempt to find out the identity of an unknown individual. This process answers the question, "Who are you?"Two broadly classified categories of biometric systems are – Unimodal biometric systems and Multimodal biometric systems.Unimodal biometric system uses single biometric trait of an individual for verification and authentication. But as biometrics are used extensively by the government organizations, law enforcement agencies, in border control and by the people across the globe for the purpose of authentication, the security risks associated with the use of single biometric trait increases. Some factors affecting the accuracy of unimodal biometric systems are – Noise in sensed data, intra-class variations, inter-class similarities, non-universality, interoperability issues and spoof attacks [4]. Hence, using multimodal biometrics will help overcome the limitations of unimodal biometrics. Multimodal biometric systems combines two or more biometric traits or modalities to identify an individual. It provides more security as there are multiple levels of authenticationso even if one of the biometric traits is compromised, the remaining traits will still be able to secure the system.

1. Security threats of using Unimodal Biometric systems:

Although fingerprint recognition is studied and used most extensively, there are issues related to security of these systems. A fingerprint sensor can be fooled by presenting fake biometric data in an attempt to circumvent the biometric system [11]. These attacks are called as spoofing attacks where an adversary presents a fake fingerprint film or an artificial fingerprint with an intent to intrude the system. Attacks on biometric template databases can take place where

the template data in the database can be hacked by an adversary, thus providing unauthorized access to the system. Voices are unique since they are comprised of countless elements. Thus, even the slightest change in a user's voice can impact the typical scoring model and can lead to false acceptances or rejections [12]. There are two major types of attacks- replay attacks and impersonation attacks. In replay attacks, the adversary pre-records and playbacks the voice sample of the person while in impersonation attacks, the adversary simply mimics the voice and speaking habit of the person [14]. Deep Neural Networks (DNN) are frequently used in the field of facial recognition. These classifiers can be fooled by adversarial attacks involving adding perturbations in an original image. A backdoor attack also targets DNN wherein the attacker poisons training data which causes the model to misclassify an input with a specific trigger [16]. Contact lenses can pose a threat to iris recognition systems where an adversary wears a contact lens with the iris pattern of a target individual printed on it. The system can also be fooled by presenting a photograph of an iris or a fake iris.

2. Multimodal Biometrics:

Multimodal biometric systems consolidates two or more biometric traits of an individual for authentication. Along with enrollment, verification and identification, the authentication process using multimodal biometrics involves an additional phase called fusion which defines how the information from different modalities is fused. The fusion of information can be done before matching (at sensor level and feature level) or after matching (at score level, decision level and rank level) [21]. Using multimodal biometrics provides enhanced verification accuracy and higher security against spoofing than unimodal biometrics as it is difficult for an impostor to spoof the multiple biometric traits simultaneously. As the system analyses patterns from multiple biometric factors, it addresses the problem of non-universality i.e. even if a person doesn't possess a required factor, the system will still be able to authenticate using other factors [10]. Multimodal biometric systems provides liveness detection i.e. it detects whether the acquired sample comes from a genuine living user or not.

II. OBJECTIVES

- To study whether biometrics are more secure than traditional IT security methods.
- To study the security vulnerabilities of unimodal biometrics and overcoming it using multimodal biometrics.
- To study the new and emerging challenges facing biometric technology due to Covid-19.

These objectives shall be attained through analysis of a survey conducted based on the hypothesis as under:

Multimodal biometrics are more secure, reliable and accurate than Unimodal biometrics as it uses multiple physiological or behavioral traits for verification and identification and is less vulnerable to spoofing.

III. RELATED WORK

The use of biometrics for authentication purpose has increased in the recent years. Memon[1] talked about the dangers associated with the frequent use of biometric authentication and how technology is becoming an avenue for the companies to invade our privacy. In [2], [3],the authors reviewed all the biometric techniques along with their potential risks and challenges for security and privacy.Bhable [4] focused on the accuracy of multimodal biometric systems and about various adversarial attacks. Carlaw [5] discussed about the significant impact of Covid-19 on biometrics leading to a rise in contactless technologies. Yang et al. [6] provided a comprehensive review on fingerprint-based biometrics and provided various solutions for improving security and accuracy. Kaur and Khanna [7] focused on two major template protection techniques- Cancelable Biometrics &Visual Cryptography. Dabouei et al. [8] portrayed the negative impact of distortions of fingerprint on the authentication systems and proposed a distortion rectification model using Deep Convolutional Neural Networks. Gaubitch [12] talked about how the ageing in voice affects the effectiveness of current authentication solutions. Vaidya and Sherr [13] discussed about how the increase in use of voice based services by people have posed an increase in voice synthesis attacks and introduced techniques for locally sanitizing voice inputs before processing. Alparslan et al. [15] experimented with different adversarial attack approaches on CNN in facial recognition domain. Wenger et al. [16] presented results of a detailed study on DNN backdoor attacks in the physical world focusing on facial recognition. Nguyen et al. [17] reviewed the state-of-the-art design and implementation of iris-recognition-at-a-distance (IAAD) systems along with the significance and applications of IAAD systems.Minaee, Abdolrashidiy and Wang [18] investigated the application of deep features extracted from VGG-Net for iris recognition. In [20], Jagadiswary and Saraswady proposed a fused multimodal system based on feature extraction and key generation using RSA. Loey et al. [22] proposed a hybrid deep learning model for face mask detection consisting two components. The authors have used decision trees, Support Vector Machine (SVM) and ensemble algorithm. Leila et al. [23] proposed a system based on the score level fusion of face and fingerprint recognition using three normalization methods: Min-Max, Z-scores and Hyperbolic Function. Hammad, Liu and Wang [25] proposed a multimodal biometric system using CNN and QG-MSVM based on feature and decision level fusion of

ECG and fingerprint. Sireesha and Reddy [27] presented an innovative technique for multimodal biometric authentication using iris and fingerprint modalities based on two level fusion.

IV. METHODOLOGY

To find out the people's perceptions about various biometric authentication techniques, a survey was conducted using questionnaire. This survey was aimed to find out whether multimodal biometrics are more secure than unimodal biometrics. It was also aimed to find out people's awareness regarding the security threats associated with using biometrics and how reluctant they are towards using it for authentication. The survey consisted of Likert scale-based and multiple choice questions. The questionnaire was sent to people at random and a total of 33 responses were obtained.The data was analyzed using Excel. It was coded to perform statistical analysis. We used a chi-square goodness of fit test for data analysis.

In the survey, the respondents were asked what do they think is more secure-using single biometric trait or using multiple or combination of biometric traits. As shown in fig. 1, 78.8% people said that using combination of biometric traits is more secure than using single biometric trait for authentication. Thus, we performed a chi-square goodness of fit test for evaluating and analyzing the obtained data. It measures the goodness of fit between the observed frequencies and the frequencies expected under the null hypothesis.

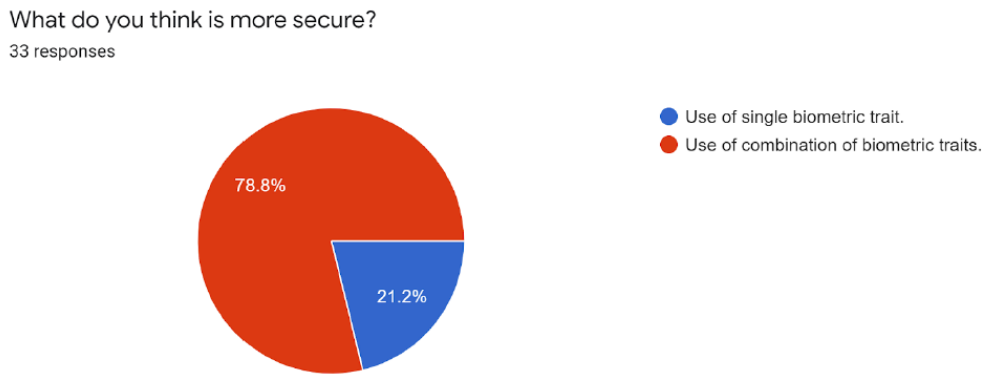

Fig. 1 Pie chart of the responses collected

Null hypothesis (H_0): Multimodal biometrics is less secure and reliable than unimodal biometrics.

Alternative hypothesis (H_a): Multimodal biometrics is more secure and reliable than unimodal biometrics.

Chi-square test statistic is given by the following equation-

$$\chi^2=\sum [(O_i-E_i)^2/E_i] \qquad (1)$$

Where $O_i$and E_i are the observed and expected frequency count respectively for the categorical variable at *i*th level. We performed this test with significance level (α) of 0.05 and degrees of freedom (ν) equal to 1.

V. EXPERIMENTAL RESULTS

Based on our null hypothesis, we predicted the expected frequency count for single and multiple biometric traits to be 18 and 15 respectively. The observed and expected frequency count is shown in the fig. 2.

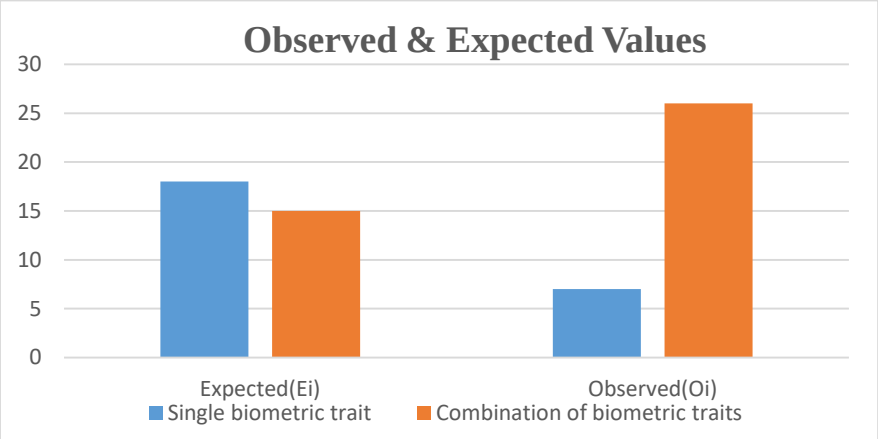

Fig. 2 Observed & Expected Frequency chart

	Expected(E_i)	Observed(O_i)	(O_i-E_i)	(O_i-E_i)^2	(O_i-E_i)^2/E_i	χ^2
Single biometric trait	18	7	-11	121	6.72	**14.79**
Combination of biometric traits	15	26	11	121	8.07	

Table. 1 Chi-square test statistic

The calculated value of chi-square test statistic is 14.79. The p-value for the given chi-square statistic having 1 degree of freedom is calculated to be 0.0001. Since the p-value (0.0001) is less than the significance level (0.05), we reject the null hypothesis. The result is significant at $p<0.05$. Hence, this proves that multimodal biometrics are more secure and reliable than unimodal biometrics.

In the survey conducted, 69.7% people think invasion of personal privacy as the major security concern relating to the use of biometrics. 57.6% people fear the theft of identity by using biometrics. 33.3% people consider tracking by the government and law enforcement agencies as a security concern. 18.2% people worry about their biometric data being used by the advertisers for marketing. This is shown below in fig. 3.

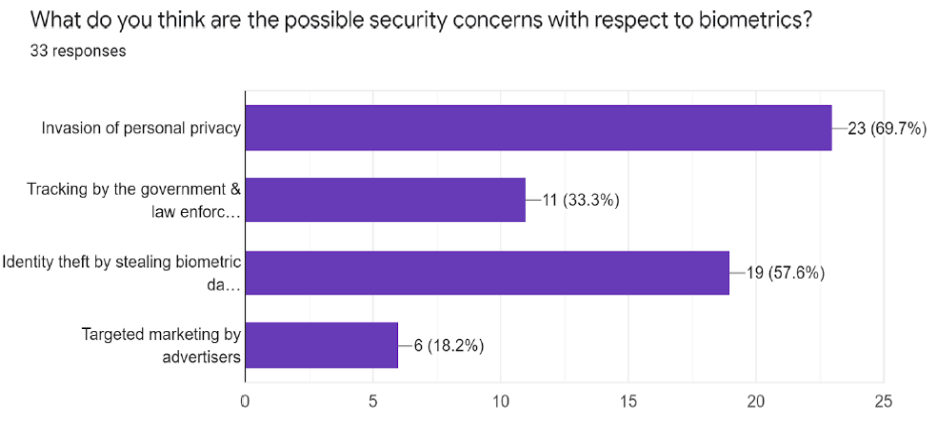

Fig. 3 Bar chart highlighting security concerns

1. Impact of Covid-19 on biometrics:

Covid-19 has significantly impacted the biometric systems which rely on contact-only sensing technologies such as fingerprint and finger vein recognition systems as they can pose great health concerns and contribute to the spread of virus. We surveyed the people regarding whether contact-only biometric technologies such as fingerprint scanning can potentially increase the risk of transmission of the virus.Among the respondents, the percentage of people saying that fingerprint authentication can contribute to the transmission of the virus and the percentage of people not sure whether it can is same and equals to 42.4% for both the cases. The remaining 15.2% people were with the view that fingerprint authentication does not contribute to the transmission of the virus. Thus, the data has a bimodal distribution.

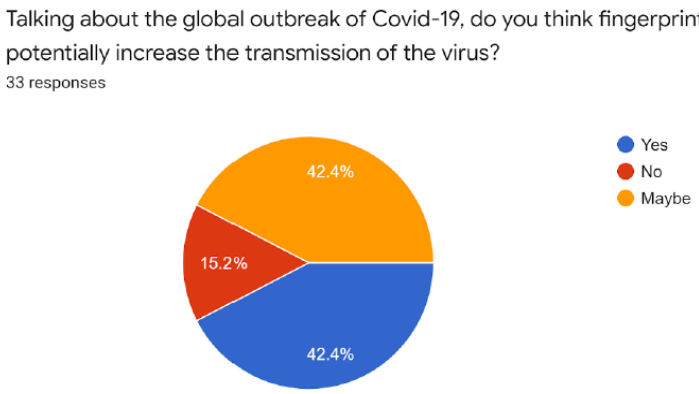

Fig. 4 Pie chart of the responses collected

Due to Covid-19, there is a rise in use of contactless biometric technologies such as face and iris recognition as they do not involve any contact with the surfaces thus, eliminating the risk of potential transmission of the virus [5]. Many companies have started using AI facial recognition as sanitary alternatives to fingerprint scanners. With people starting to wear face masks, the facial recognition algorithms have been pushed to new heights to tackle the emergent threat.

VI. CONCLUSION

Biometrics are one of the most widely used means of authentication. It started with simple unimodal biometrics but with the rise of the use of biometric authentication by the people globally, it posed a challenge to the security provided by unimodal biometrics. Thus, a more robust and secure form of authentication using multiple biometric traits was developed called as multimodal biometrics. It has a higher accuracy and recognition rate compared to unimodal biometrics and is nearly spoof-proof. But designing and implementation of these systems is a complex and exorbitant process. With the world fighting with Covid-19, the pandemic has posed new challenges for biometric technologies such as people wearing face masks which obstructs the detection and recognition of faces by the facial recognition algorithms thereby leading to unsuccessful or false identifications. Future work can include developing algorithms that works with only on the data around the eyes and forehead.

ACKNOWLEDGEMENT

Sincere thanks and gratitude to Prof. Swapna Augustine Nikale, Department of Information Technology, B.K. Birla College of Arts, Science & Commerce (Autonomous), Kalyan for her continuous guidance and encouragement at every stage which helped in preparingthe research paper. Also thanking everyone who directly or indirectly helped in the successful completion of the research.

REFERENCES

[1] Memon, N. (2017). How Biometric Authentication Poses New Challenges to Our Security and Privacy. *IEEE*, *34*(4), 194–196. https://doi.org/10.1109/MSP.2017.2697179

[2]Rui, Z., & Yan, Z. (2018). A Survey on Biometric Authentication: Toward Secure and Privacy-Preserving Identification. *IEEE*, *7*, 5994–6009. https://doi.org/10.1109/ACCESS.2018.2889996

[3] Bhatia, S. (2019). Systematic review of Biometric Advancement and Challenges. *International Journal of Electronics Engineering*, *11*(1), 812–821. http://www.csjournals.com/IJEE/PDF11-1/135.%20Sakshi.pdf

[4] Bhable, S. (2015). A Survey of Security of Multimodal Biometric Systems. *International Journal of Engineering Research and Applications*, *5*(12), 67–72. https://pdfs.semanticscholar.org/57b1/0d7e3507d24e2258aa62fe356df2a9023e4f.pdf

[5]Carlaw, S. (2020). Impact on biometrics of Covid-19. *Biometric Technology Today*, *2020*(4), 8–9. https://www.sciencedirect.com/science/article/pii/S0969476520300503

[6]Yang, W., Wang, S., Hu, J., Zheng, G., & Valli, C. (2019). Security and Accuracy of Fingerprint-Based Biometrics: A Review. *Symmetry*, *11*(2), 141. doi:10.3390/sym11020141

[7]Kaur, H., Khanna, P. Biometric template protection using cancelable biometrics and visual cryptography techniques. *Multimed Tools Appl* 75, 16333–16361 (2016). https://doi.org/10.1007/s11042-015-2933-6

[8]A. Dabouei, H. Kazemi, S. M. Iranmanesh, J. Dawson and N. M. Nasrabadi, "Fingerprint Distortion Rectification Using Deep Convolutional Neural Networks," *2018 International Conference on Biometrics (ICB)*, Gold Coast, QLD, 2018, pp. 1-8, doi: 10.1109/ICB2018.2018.00012.

[9] S. Mil'shtein and A. Pillai, "Perspectives and limitations of touchless fingerprints," *2017 IEEE International Symposium on Technologies for Homeland Security (HST)*, Waltham, MA, 2017, pp. 1-6, doi: 10.1109/THS.2017.7943479.

[10]Kumar, K., & Farik, M. (2016). A Review Of Multimodal Biometric Authentication Systems. *International Journal of Scientific & Technology Research*, *5*(12), 5–9. https://www.researchgate.net/profile/Mohammed_Farik/publication/311714564_A_Review_Of_Multimodal_Biometric_Authentication_Systems/links/585b69e108ae329d61f17b64.pdf

[11]Joshi, M., Mazumdar, B., & Dey, S. (2018). Security Vulnerabilities Against Fingerprint Biometric System. *ArXiv*, *abs/1805.07116*.

[12]Gaubitch, N. (2017). How voice ageing impacts biometric effectiveness. *Biometric Technology Today*, *2017*(6), 8–9. https://doi.org/10.1016/S0969-4765(17)30115-7

[13]T. Vaidya and M. Sherr, "You Talk Too Much: Limiting Privacy Exposure Via Voice Input," *2019 IEEE Security and Privacy Workshops (SPW)*, San Francisco, CA, USA, 2019, pp. 84-91, doi: 10.1109/SPW.2019.00026

[14]Q. Wang et al., "VoicePop: A Pop Noise based Anti-spoofing System for Voice Authentication on Smartphones," IEEE INFOCOM 2019 - IEEE Conference on Computer Communications, Paris, France, 2019, pp. 2062-2070, doi: 10.1109/INFOCOM.2019.8737422.

[15]Alparslan, Yigit & Keim-Shenk, Jeremy & Khade, Shweta & Greenstadt, Rachel. (2020). Adversarial Attacks on Convolutional Neural Networks in Facial Recognition Domain.https://arxiv.org/ftp/arxiv/papers/2001/2001.11137.pdf

[16]Wenger, Emily & Passananti, Josephine & Yao, Yuanshun & Zheng, Haitao & Zhao, Ben. (2020). Backdoor Attacks on Facial Recognition in the Physical World. https://arxiv.org/pdf/2006.14580.pdf

[17]Nguyen, K., Fookes, C., Jillela, R., Sridharan, S., & Ross, A. (2017). Long range iris recognition: A survey. *Pattern Recognition*, *72*, 123–143. https://doi.org/10.1016/j.patcog.2017.05.021

[18] S. Minaee, A. Abdolrashidiy and Y. Wang, "An experimental study of deep convolutional features for iris recognition," 2016 IEEE Signal Processing in Medicine and Biology Symposium (SPMB), Philadelphia, PA, 2016, pp. 1-6, doi: 10.1109/SPMB.2016.7846859.

[19]N. Kohli, D. Yadav, M. Vatsa, R. Singh and A. Noore, "Synthetic iris presentation attack using iDCGAN," 2017 IEEE International Joint Conference on Biometrics (IJCB), Denver, CO, 2017, pp. 674-680, doi: 10.1109/BTAS.2017.8272756.

[20]Jagadiswary, D., & Saraswady, D. (2016). Biometric Authentication Using Fused Multimodal Biometric. *Procedia Computer Science*, *85*, 109–116. https://doi.org/10.1016/j.procs.2016.05.187

[21]Kaur, G., et al. "Fusion in Multimodal Biometric System: A Review." *Indian Journal of Science and Technology*, vol. 10, 2017, sciresol.s3.us-east-2.amazonaws.com/IJST/Articles/2017/Issue-28/Article9.pdf.

[22]Loey, Mohamed, et al. "A Hybrid Deep Transfer Learning Model with Machine Learning Methods for Face Mask Detection in the Era of the COVID-19 Pandemic." *Measurement*, vol. 167, 2021, p. 108288. *Crossref*, doi:10.1016/j.measurement.2020.108288.

[23]Leila, Hellal & Naceur-Eddine, Boukezzoula & Mohamed, Cheniti & Halima, Saadi. (2020). Multimodal biometric authentication based on score level fusion of face and fingerprint recognition.

[24]Hung, T. C., Tri, N. T., & Minh, H. N. (2016). An Enhanced Security for Government Base on Multifactor Biometric Authentication. *International Journal of Computer Networks & Communications*, *8*(6), 55–72. https://doi.org/10.5121/ijcnc.2016.8605

[25]M. Hammad, Y. Liu and K. Wang, "Multimodal Biometric Authentication Systems Using Convolution Neural Network Based on Different Level Fusion of ECG and Fingerprint," in IEEE Access, vol. 7, pp. 26527-26542, 2019, doi: 10.1109/ACCESS.2018.2886573.

[26]Mahendar, G., & Batta, M. (2020). Enhanced Security in ATM by IRIS and Face Recognition Authentication. *International Journal of Scientific Research & Engineering Trends*, *6*(3), 1074. https://ijsret.com/wp-content/uploads/2020/05/IJSRET_V6_issue3_328.pdf

[27]Sireesha, V., & Reddy, S. (2016). Two Levels Fusion Based Multimodal Biometric Authentication Using Iris and Fingerprint Modalities. International Journal of Intelligent Engineering and Systems, 9(3), 21–35. https://doi.org/10.22266/ijies2016.0930.03

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor:
7.512

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर
NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details