iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** XI **Month of publication:** November 2023

DOI: https://doi.org/10.22214/ijraset.2023.56728

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue XI Nov 2023- Available at www.ijraset.com

An In Depth Survey on Biometric ATM Handling through Fingerprint and Face Recognition using Deep Learning

Prof. Archana R. Ghuge[1], Ms. Jayshri Avhad[2], Mr. Vijay Burkul[3], Ms.Pallavi Shewale[4], Ms.Priya Warungase[5]
IT Department, SVIT College, Chincholi.

Abstract: ***The achievement of greater ease and dependability has been made possible by India's technical advancements. The banking industry has also prospered, achieving notable improvements that have benefited the consumer. Automated Teller Machines (ATMs) have transformed transaction capabilities and decreased the likelihood of human error. Cash can always be dispensed and deposited via ATMs. This can be done with the bank-issued cards, which make integration considerably simpler. However, there has been a rise in card theft and fraudulent transactions, which compromises the dependability and security of ATMs. Consequently, rather than recognizing the card as is the case with the current model, a methodology that identifies the person during the transaction is required to increase the security and dependability of Automated Teller Machines. Implementing a biometric authentication system will be necessary to realize user identification through a virtual ATM strategy. In order to create a very reliable and secure virtual ATM, this method covers the usage of face recognition in addition to fingerprint recognition using live streaming, Channel Boosted Convolutional Neural Networks, and One Time Password implementation. The research directives to come will provide a detailed explanation of the strategy.***

Keywords: Biometric ATM, Biometric recognition. Face recognition, Fingerprint Recognition, Channel Boosted Convolutional Neural Networks.

I. INTRODUCTION

India's technology advancements have resulted in the introduction of many types of machinery aimed at enhancing customer satisfaction. The ATM was one such gadget that simplified financial transactions for account holders. Early in the 20th century, automated teller machines were created to encourage self-service in consumer banking. Originally intended to handle money transfers for the bank's customers, ATMs were later linked into the central bank system, enabling anyone to obtain an automated teller machine from any bank and conduct a transaction. This made it possible for people to send, receive, and transfer money from machines that belonged to other banks.

ATMs require both an EMV chip card and approval from the card company or another authorizing body for money transfers via the telecoms network. Several banks charge their customers fees to use their ATMs. ATMs have advantages and disadvantages. An article looks into and discusses different ways to mitigate ATM danger. To reduce the risk of unethical activity, ATM systems can be equipped with a number of protections. However, regulations shouldn't be seen as a cure-all. When a card is lost, the current ATM authentication processes fall short because it can be used for dubious transactions. Facial recognition technology can dramatically reduce the incidence of misconduct.

Over the last few decades, a great deal of research has been done on face recognition, which is possibly one of the best methods for identifying someone. Facial recognition from photographs is a popular primary biometrics research topic. One of the most useful applications of face detection and identification technology is comprehension image evaluation. Psychiatrists, cognitive psychologists, and machine vision experts have all expressed interest in face recognition due to its unique problems, since advancements in this field can shed light on human brain functioning. While there are a number of biometric technologies available for identifying individuals, such as retinal and fingerprint scanning, they still need human assistance. However, if facial images are used, person verification does not require them. A major part of identifying a person is done by face recognition software, which has a distinct benefit over other biometrics techniques in that it doesn't actually require human involvement.

Despite the fact that there are numerous technologies available for facial recognition in images. Several investigations will reveal more efficient components that increase efficiency and accuracy. The efficiency is essentially dependent on factors such as alignment, illumination, and so on, and a large amount of processing power is needed to retrieve the images from the large database.

It might lead individuals to focus on massive image databases and novel approaches that improve the accuracy and efficiency of solving challenging mathematical issues. The ultimate goal is to accurately identify human faces using image collections. Research has been done in the field of biometric face identification to determine an individual's identity based on facial features from an image of a group of people. Face recognition is widely used in biometric and access control technologies and has many applications. The three primary building blocks of a facial recognition system are biometric authentication, face identification, and training of detected faces.

Automation is the application of technical advancements to machinery and its operations through the use of computer software. The modern era's precision has increased thanks to technical advancements, which have also improved living standards. The requirement for labor is substantially reduced by these kinds of developments. One technological advance is the Automated Authentication system, which takes the place of antiquated and traditional authentication methods. The objective of our system is to provide a face and fingerprint recognition based virtual ATM authentication system with a reduced false positive rate when recognizing new users.

H. Qi et al. describes in [1] about LBAS_Resnet50, a real-time face identification technique based on blink detection, to address the issues of lighting and expression variations during real-time face recognition. To increase the recognition process's tolerance to lighting, the model uses ResNet50 as the foundational network structure and feeds the texture information that the LBP method extracts into the base network. Then, it is straightforward to extract time series features in order to increase the accuracy of real-time recognition by using BiLSTM to collect context information. In order to extract crucial feature information and give weights, the channel attention mechanism is included at the same time that SPP pooling is utilized to increase the model's robustness. Lastly, eye blink detection is used to assess the true face. The experimental findings show that the strategy suggested in this paper significantly improves real-time facial recognition accuracy against spoofing. Cameras capture distinct information about brightness and illumination in their facial photographs because paper, screens on electronic devices, and real faces have different structures. To further enhance model performance, System will look into effectively extracting features related to brightness and reflected light from RGB photos in the upcoming study. Additionally, the system will think about using face recognition-based deep learning with sparse representation.

M. Ibsen et al. states in [2] that with the development of deep learning and the availability of big face databases, face recognition has become more common. In spite of this, it is evident that these systems are susceptible to presentation assaults, which need for strong detection techniques in order to prevent a facial recognition system's security from being compromised. The field of presentation assault detection has recently shifted toward generalizable techniques that can identify a wide range of attacks, including ones that are not visible to the trainer during training. In order to progress the field and precisely assess the capabilities of these presentation assault detection techniques, benchmarks incorporating fresh and innovative attack kinds need to be implemented. In this study, a novel multi-channel T-shirt Face Presentation Attack (TFPA) database with 1,608 T-shirt impersonation attacks and 100 distinct T-shirt PAIs were introduced. By first examining the viability of launching the assaults and then assessing the success rate of the T-shirt attacks, the vulnerability of facial recognition systems to the attacks was assessed. The outcomes demonstrated that if the true face was hidden, the attack might be initiated. Both an open-source and a commercial face recognition system had attack success rates more than 92.6% in terms of IAPMR in these situations where the face on the T-shirt was identified.

[3] The work of M. O. Alassafi et al., proposes a hybrid face PAD approach that combines the Mobile NET CNN's transfer learning with the idea of interpolation-based image diffusion. On the Replay-Attack, Replay-Mobile, CASIA-FASD, and ROSE You datasets, the suggested architecture has demonstrated encouraging results, achieving the highest accuracy and HTER of 99.93% and 0.09%, 99.04% and 1.14%, 99.90% and 0.09%, and 95.04% and 4.92%, respectively. Additionally, the suggested approach performed better in cross-domain evaluation. Such face PAD approaches have a wide range of applications. In order to maximize System's future prospects, System plans to integrate System's face PAD method with a facial recognition and gesture recognition system for monitoring student attendance and exams in an educational setting. This will create a deep learning-based framework that will support daily operations in schools. In addition, System hopes to enhance the suggested method's cross-domain performance in subsequent studies by using it in an unsupervised learning scheme to carry out domain adaptation for face PAD across a variety of intricate face PAD databases.

Part 2 of this literature survey article is divided into a literature review, which evaluates earlier work, and part 3 offers suggestions for more research.

II. RELATED WORKS

N. M. Alnaim and other in [4] discusses the modern Deepfakes are becoming harder to detect, which makes the issue more crucial to address. Large-scale politics, crime, personal safety, security, and society are all impacted by this technology.

The COVID-19 virus outbreak in 2020 led to the widespread adoption of face masks, which enable users to cover their faces. This has greatly facilitated the creation of Deepfake films and increased the difficulty of identifying them. With the use of its dataset of face mask Deepfakes, this study intends to facilitate research in Deepfake identification by examining several deep learning models for Deepfake detection on the suggested dataset. Ultimately, the study's findings show that the deep-fake dataset can be detected with considerable accuracies of 77.48%, 99.25%, and 99.81 using CNN, InceptionResNetV2, and VGG19 approaches. One of the limitations that the system encountered in this research study was the absence of video resources featuring people wearing masks; this will be addressed in the next research investigation. In order to enhance the ensuing experimental work, the system will employ additional deep learning techniques for detection in future work.

In the study by J. M. Singh [5], this introduced a brand-new kind of digital attack known as Composite Face Image Attack (CFIA), which is based on facial features. The proposed CFIA will first separately segment the face photos into six different attributes using the facial images from the two contributory data participants. Next, a transparent mask based on both single and multiple face traits is used to mix these parts. In order to produce the final early portions of the papers, which are typical of low, moderate, and high vulnerability combinations, these qualities are processed using the picture in painting based on pre-trained GAN.

J. C. Piland et al. in [6] describes about how low focus is correlated with a high Shannon entropy of model saliency (CAM entropy), as the model assigns equal probability to every pixel, even the ones that are irrelevant. As a result, low-information and indiscriminate models have high entropy. Models trained using the traditional cross-entropy loss function exhibit this. System can anticipate that as CYBORG adds human saliency to the model, entropy will drop as information increases. System notes this, which naturally raises the question, "Is low entropy just an effect, or can it be a cause of increased information and performance?" In order to address such topic, novel loss functions that directly alter CAM entropy are introduced in this study. While FMMMSE aggressively minimizes CAM entropy, DROID attempts to find an acceptable medium ground by minimizing log entropy. HSEB matches the typical human-salience entropy.

In [7], this explains the order to detect single image morphing attacks, this research uses spatial and channel attention modules to emphasize discriminative regions. System specifically provided quantitative evidence of the three visual attention modules' effectiveness for the downstream job of morph identification in a binary classification environment. As a form of representation learning, the integrated attention modules are meant to be used for both feature selection and refining. To increase the accuracy of morph recognition on many datasets, a trainable soft attention mechanism, convolutional block attention module, and multi-headed attention-augmented feature maps were specifically used. Furthermore, in order to benefit from the fine-grained spatial-frequency information given by wavelet decomposition, the system has moved the input data domain from the RGB space into the wavelet domain.

L. J. Gonzalez-Soler et al [8] discusses the viability of employing various face regions for PAD was investigated in this paper. Specifically, 14 regions—both single and composite—were assessed using the parameters outlined in the ISO/IEC 30107-3 international standard [11] for biometric PADs. The results of the experimental evaluation carried out on publicly accessible databases, including CRMA, OULU-NPU, REPLAY-MOBILE, REPLAY-ATTACK, and CASIA, showed that the composite regions had the best detection performances. The entire face produced a median D-EER of 3.92%, which was followed by the jaw (median D-EER = 5.53%), middle face (median D-EER = 6.28%), and right and left faces (median D-EER = 4.61%). Naturally, there is a relationship between depicting the eyebrows and both the left and right sides of the face. Furthermore, facial regions with common accessories that can be employed in unattended applications were identified by the proposed Facial Region Utility metric. Actually, by combining the facial regions with a high Facial Region Utility—that is, the jaw, middle face, left face, and right face—it is possible to enhance the specific outcome that is reported when the entire face is used in those applications.

In [9] It has been suggested to use a new AM micro-LED display architecture with external compensation to enable fingerprint recognition without the need for extra light sources or sensors. The universal fingerprint recognition technology is based on the shared structure of all LED pixel circuits. Moreover, the AM micro-LED display adopting System's suggested architecture can enhance the security of mobile devices by recognizing numerous fingerprints.

Y. Zhu et al. in [10] proposes a model of Latent fingerprint enhancement is formulated as a constrained fingerprint generation issue, and this research suggested a Finger GAN for latent fingerprint enhancement. It can ensure that its generated enhanced latent fingerprint is indistinguishable from the matching ground truth instance in terms of the orientation field regularized by the FOMFE model and the fingerprint skeleton map weighted by minutia positions. System provides a comprehensive framework that may perform latent fingerprint enhancement in the context of directly optimizing minutia information, since minutia is the fundamental feature for recognition and can be acquired directly from the fingerprint skeleton map.

This will greatly enhance the performance of latent fingerprint identification. Results from experiments on two public latent fingerprint datasets show that System's approach performs noticeably better than the state of the art.

[11] Includes an initial quality and recognition performance analysis along with a multi-sensor, longitudinal FP dataset. The dataset is made up of about 108,000 samples that were collected over the course of two years from 50 volunteers at the System's time-separated sessions using 10 commercially available capturing devices—four of which are capacitive, five of which are optical—and one thermal. The dataset can be obtained at http://wavelab.at/sources/PLUS-MSL-FP and is open for research use. The proposed longitudinal FP dataset spans a 2-year time interval, which allows for the detection of template aging effects, such as behavioral changes in subjects, while the influence of physiological subject aging is unlikely to be noticeable. This is in contrast to other existing longitudinal FP datasets, which range in length from minutes to up to 30 years.

In [12] A novel design was put forth for a micro-LED display that can identify fingerprints without the need for extra sensors. The system confirmed that the active-matrix pixel circuits may employ regular LEDs as photo detectors. This is the first study of its kind in the world: fingerprint recognition in a micro-LED display without any additional light supply or sensing equipment. Multiple fingers can be recognized once the micro-LED display supports multiple touches. For mobile devices, this allows for far higher biometric security.

X. Yin el al. [13] System presented a lightweight, length-flexible fingerprint template design in this article for privacy-preserving authentication systems in resource-constrained Internet of Things applications. There are two parts to the suggested template design: 1) Lightweight cancellable feature creation based on the encoding-nested-difference OR method, and 2) length-flexible partial-cancellable feature generation based on the reinedxing approach. IoT applications can benefit greatly from the system's template design, which offers high performance, lightweight, cancelability, and customizable feature lengths. The suggested cancellable fingerprint template achieves equivalent authentication performance compared to the state-of-the-art methods, according to comprehensive experimental results evaluated on eight benchmark data sets, FVC2002 DB1–DB4 and FVC2004 DB1–DB4. However, the system's design significantly reduces computational and storage costs. More significantly, an actual IoT prototype system was used to demonstrate that the suggested lightweight cancellable template is adaptable and appropriate for a range of resource-constrained IoT devices. To the best of System's knowledge, this is the first lightweight, highly-performing, and length-flexible cancellable fingerprint template design for Internet of Things applications with limited resources.

In [14] it is described that Despite only having been trained on FVC2000, the system's approaches attain the state of the art on FVC2002 DB1 A, FVC2004 DB1 A, and FVC2004 DB3 A. Furthermore, System outperforms other systems on the remaining dataset. Given that the learned model is likely to be restricted to the training data domain, this is a difficult machine learning task. The system's approach to low-temperature fingerprints works incredibly well.

R. C. Contreras et al, in [15] To enhance the security provided by BASs, two developments on the subject of fingerprint spoofing detection were put forth in this work. The first advance is the suggestion to employ mapping sets to expand the matrices-based texture descriptor vector format. The second innovation comes in the form of a multi-phase framework that enables the construction of texture pattern descriptors and filtering sets to boost the capacity for representing images and, as a result, raise classifier accuracy. The work's contributions were provided in a generalized manner, thus in order to carry out the proper assessments of its implementation, it was required to specify real-world examples, or versions, of the content. Ten distinct iterations of the proposed framework were established utilizing the three pattern descriptors, s BRISK, s SIFT, and s Dense SIFT, that were defined using the suggested mapping representation technique.

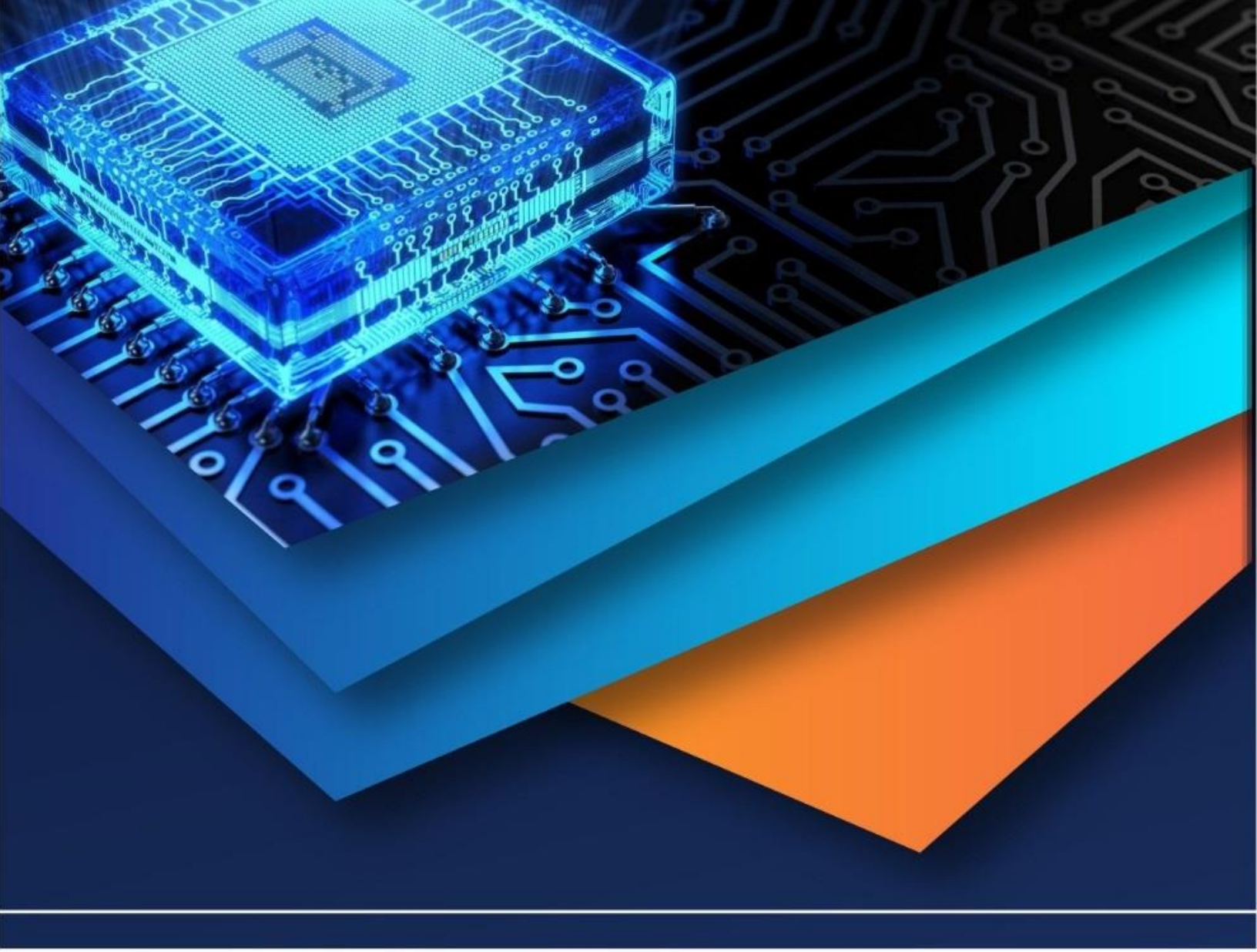
III. CONCLUSION AND FUTURESCOPE

India's technological achievements have made improved simplicity of use and dependability feasible. The banking sector has also thrived and achieved significant advancements that benefit customers. ATMs, or automated teller machines, have transformed the way that transactions can be completed and reduced the possibility of human error. ATMs are constantly open for cash deposits and withdrawals. The bank-issued cards can be used for this, which also greatly simplifies integration. ATM security and dependability have decreased, though, as a result of an increase in fraudulent transactions and card thefts. Therefore, to improve the confidentiality and reliability of the Automated Teller Machines, a method that identifies the user at the time of the transfer—rather than the card, as is being done in the current system—must be implemented. To achieve identity verification through a virtual ATM technology, a biometric security system must be developed. This technique builds a very efficient virtual ATM by combining live streaming, channel-boosted convolutional neural networks, one-time password generation, and fingerprint and face recognition. The approach will be thoroughly explained in the next research projects.

In the future this concept can be implementable in the real time ATM kiosks to perform the different actions of the automated teller machine.

REFERENCES

[1] H. Qi, C. Wu, Y. Shi, X. Qi, K. Duan and X. Wang, "A Real-Time Face Detection Method Based on Blink Detection," in IEEE Access, vol. 11, pp. 28180-28189, 2023, doi: 10.1109/ACCESS.2023.3257986.
[2] M. Ibsen et al., "Attacking Face Recognition With T-Shirts: Database, Vulnerability Assessment, and Detection," in IEEE Access, vol. 11, pp. 57867-57879, 2023, doi: 10.1109/ACCESS.2023.3282780.
[3] M. O. Alassafi et al., "A Novel Deep Learning Architecture With Image Diffusion for Robust Face Presentation Attack Detection," in IEEE Access, vol. 11, pp. 59204-59216, 2023, doi: 10.1109/ACCESS.2023.3285826.
[4] N. M. Alnaim, Z. M. Almutairi, M. S. Alsuwat, H. H. Alalawi, A. Alshobaili and F. S. Alenezi, "DFFMD: A Deepfake Face Mask Dataset for Infectious Disease Era With Deepfake Detection Algorithms," in IEEE Access, vol. 11, pp. 16711-16722, 2023, doi: 10.1109/ACCESS.2023.3246661.
[5] J. M. Singh and R. Ramachandra, "Deep Composite Face Image Attacks: Generation, Vulnerability and Detection," in IEEE Access, vol. 11, pp. 76468-76485, 2023, doi: 10.1109/ACCESS.2023.3261247.
[6] J. C. Piland, A. Czajka and C. Sweet, "Model Focus Improves Performance of Deep Learning-Based Synthetic Face Detectors," in IEEE Access, vol. 11, pp. 63430-63441, 2023, doi: 10.1109/ACCESS.2023.3282927.
[7] P. Aghdaie, S. Soleymani, N. M. Nasrabadi and J. Dawson, "Attention Augmented Face Morph Detection," in IEEE Access, vol. 11, pp. 24281-24298, 2023, doi: 10.1109/ACCESS.2023.3254539.
[8] L. J. Gonzalez-Soler, M. Gomez-Barrero and C. Busch, "Toward Generalizable Facial Presentation Attack Detection Based on the Analysis of Facial Regions," in IEEE Access, vol. 11, pp. 68512-68524, 2023, doi: 10.1109/ACCESS.2023.3292407.
[9] D. -H. Jeon, W. -B. Jeong and S. -W. Lee, "Novel Active-Matrix Micro-LED Display With External Compensation Featuring Fingerprint Recognition," in IEEE Electron Device Letters, vol. 43, no. 9, pp. 1483-1486, Sept. 2022, doi: 10.1109/LED.2022.3189211.
[10] Y. Zhu, X. Yin and J. Hu, "FingerGAN: A Constrained Fingerprint Generation Scheme for Latent Fingerprint Enhancement," in IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 45, no. 7, pp. 8358-8371, 1 July 2023, doi: 10.1109/TPAMI.2023.3236876.
[11] S. Kirchgasser, C. Kauba and A. Uhl, "The PLUS Multi-Sensor and Longitudinal Fingerprint Dataset: An Initial Quality and Performance Evaluation," in IEEE Transactions on Biometrics, Behavior, and Identity Science, vol. 4, no. 1, pp. 43-56, Jan. 2022, doi: 10.1109/TBIOM.2021.3104108
[12] D. -H. Jeon, W. -B. Jeong, H. -J. Chung and S. -W. Lee, "Novel Micro-LED Display Featuring Fingerprint Recognition Without Additional Sensors," in IEEE Access, vol. 10, pp. 74187-74197, 2022, doi: 10.1109/ACCESS.2022.3190608.
[13] X. Yin, S. Wang, Y. Zhu and J. Hu, "A Novel Length-Flexible Lightweight Cancelable Fingerprint Template for Privacy-Preserving Authentication Systems in Resource-Constrained IoT Applications," in IEEE Internet of Things Journal, vol. 10, no. 1, pp. 877-892, 1 Jan.1, 2023, doi: 10.1109/JIOT.2022.3204246.
[14] C. -H. Cheng et al., "Multiple Training Stage Image Enhancement Enrolled With CCRGAN Pseudo Templates for Large Area Dry Fingerprint Recognition," in IEEE Access, vol. 11, pp. 86790-86800, 2023, doi: 10.1109/ACCESS.2023.3303532.
[15] R. C. Contreras et al., "A New Multi-Filter Framework for Texture Image Representation Improvement Using Set of Pattern Descriptors to Fingerprint Liveness Detection," in IEEE Access, vol. 10, pp. 117681-117706, 2022, doi: 10.1109/ACCESS.2022.3218335.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY