Exploring Facial Biometrics in Multi-Factor Authentication Systems for Secure Banking Applications

Pragya Vaishnav[1] , Monika Jyotiyana[1*]
[1]Department of Computer Applications
[1]Manipal University Jaipur, Jaipur Rajasthan

ABSTRACT

Recently digital security is more important than ever, as the banking sector is under tremendous pressure to safeguard private financial data and stop frauds. Existing techniques, such as passwords, are vulnerable to hacking, theft, and forgetting. Biometrics, a technology that verifies identity by using distinctive facial features. To improve security and prevent unwanted access, the proposed method was created for banking applications, to integrate facial biometrics into multifactor authentication. To register facial features on the server, all experiments were performed on 210 subjects. For the 206 subjects the equivalent error rate (EER) in the statistical analysis is 4.195, the false rejection rate (FRR) is 6.73% and the false acceptance rate (FAR) is 1.66%.)

Keywords: FAR, FRR, EER, Multi-factor authentication, OTP

1. Introduction

Multi-factor authentication also known as two-factor authentication (2FA), is a technique to access a system or application, there users must provide multiple authentication factors. Even if something is compromised, it becomes more difficult for unauthorized users to gain access. Multi-Factor Authentication (MFA) is essential for banking applications because it adds an extra layer of verification to passwords, significantly improving security. Even if your password is recovered, this extra layer, often in the form of a one-time password (OTP), pattern matching, biometric authentication, or human recognition, makes it much more difficult for unauthorized users to access your account. Biometric authentication verifies and identifies the user's distinctive and pre-recorded biological characteristics through fingerprints, voice patterns, retinal scans, and facial structures. Biometric authentication is an excellent technology for ensuring secure navigation in banking applications and reducing the risk of banking fraud in digital banking services [1]. Facial recognition technology analyzes and compares digital images of faces to identify individuals. It uses algorithms to detect and map facial features and then compares these features against a database of known faces to establish a match. This technology is used in various applications, including security, law enforcement, and mobile device authentication [2].

How face biometric system works; it presented below:

- Face Detection: Designed algorithm identify the presence and location of faces in an image or video.
- Feature Extraction: Once a face is detected, algorithms extract key features, such as the distance between eyes, nose, and mouth, as well as the shape and texture of the face.
- Matching: The extracted features are then compared against a database of known faces.
- Identification/Verification: If a match is found, the system can identify or verify the individual's identity.

In this digital and internet era, it has become common and popular to use a mobile phone for financial transactions [3]. With the spread of mobile banking services and the increasing number of users, user security and authentication have become increasingly important [4]. To improve and enable this, smart facial authentication has emerged as a new and powerful technology [5]. In order to create an effective system, especially for online banking, the security level of biometric devices must be increased [6]. To enable online banking, mobile banking, and mobile payments while ensuring security, mobile authentication can be a good option [7],[8]. Authentication itself is vulnerable to attacks; security can be easily compromised if stolen or disclosed to a third party [9]. Most passwords appear weak, making it easy for hackers to bypass security measures. Customers can feel secure knowing their data is protected and can conduct business safely thanks to secure banking [10]. The author has created a mobile app supporting multi-factor authentication to enhance the security of online banking systems. In this system, a user is identified both by their login credentials and by their distinctive facial features.

2. Literature Review

By successfully bridging the gap between optical and thermal modes, Cheema et al. [11] proposed a cross-modal discrimination network (CMDN) to overcome the problems of high-frequency recognition (HFR). HFR traditionally relies on methods such as regular subspace projection, feature extraction, and image preprocessing, all of which pose performance and optimization challenges. Overcoming the limitations of facial disguises in recognition systems was the main goal of Ahmad et al. [12]. The lack of comprehensive training data means that traditional face recognition algorithms often struggle to detect disguises such as makeup, beards, and glasses. To address this problem, researchers created artificial datasets of masked faces using cyclic coherence loss networks and generative adversarial networks (GANs). To improve the performance of hidden heterogeneous face detection (HFR), Cheema and Moon [13] developed the Deep Neighborhood Difference Relational (DNDR) network combined with Joint Discrimination Loss (JDL). Previous methods, which often encountered challenges such as the need for large amounts of training data, adaptation problems, and the difficulty of obtaining differentiating features in synthesized images, focused either on image synthesis or on extracting domain-invariant features. The DNDR network uses deep feature relations to solve these problems instead of reducing domain gaps or performing intensive preprocessing. An innovative method for thermovisual face verification was developed by Kowalski et al. proposed. [14], useful in difficult situations with little light or movement. Previous studies mainly used data from the visible spectrum for face recognition. These performed well, but poorly in low light. By using thermal photography, which is less affected by illumination, the thermovisual method closes this gap. To address the different properties of the thermal and visual spectrum, Kowalski et al. [14] developed the triplet technique, which combines multiple convolutional neural networks (CNN). By combining information from the visual and thermal spectra, this technique significantly increases the accuracy and reliability of the detection while strengthening the robustness of the process. Abdullah et al. [15] presented a GAN-based technique focusing on using CycleGAN to create thermal images from visible-light images. This method is important because thermal image data for training facial recognition algorithms is scarce, unlike the abundance of visible-light images. The study demonstrates the ability of CycleGAN to extract stylistic features from thermal images and then translate them into visible-light images to create realistic thermal representations. To increase the system's resilience against identity fraud attacks, Ahmad et al. [16] investigated the creation of camouflaged artificial faces using GANs. By incorporating a variety of camouflaged faces into the training dataset, this unique technique effectively improves facial recognition systems and significantly increases recognition accuracy in various camouflaging scenarios. Alkadi et al. [17] developed a multimodal facial recognition system that combines visual, infrared, and thermal images for biometric identification at ATMs. By integrating multiple imaging techniques, our system improves accuracy and security while combating presentation attacks and face obscuration. The study investigated various machine learning algorithms before selecting ResNet-50 due to its efficiency and effectiveness. Padmashree and Kotegar [18] presented a novel approach that focuses on areas of facial skin that are less likely to be obscured by disguises. Their approach uses a CNN for feature extraction and a region-based, marker-guided watershed algorithm for skin segmentation. This is followed by deep learning-based classification. Fuzzy extractors have become indispensable for integrating cryptographic security into biometric identification. They enable the generation of reliable cryptographic keys from fluctuating and inherently noisy biometric data [19],[20]. Fuzzy extractors account for the variability of biometric data and secure generation and renewal of cryptographic keys. This enables secure transmission and storage of biometric templates [21],[22]. Standard encryption methods are vulnerable to quantum attacks due to the threat of quantum computing [23],[24]. Erasure- and code-based encryption are examples of post-quantum encryption that have been explored as a potential method for ensuring quantum-resistant security in biometric systems [25]. The McEliece cryptosystem, based on cryptographic code-based technology, is known for its robust defense against quantum attacks. For this reason, it is a viable option for securing biometric systems in the coming era of quantum computing [26],[27]. The connection between biometrics and cryptography also raises many ethical and privacy-related issues. When storing, transmitting, and processing biometric data, careful consideration of confidentiality, consent, and data protection is essential, particularly with regard to international data protection laws and ethical considerations [28],[29]. Therefore, the design and implementation of biometric systems must address the challenge of ensuring robust security while also addressing privacy and ethical concerns. New algorithms [30] and paradigms are being explored in biometric authentication and cryptographic security research and development. The ability to develop robust, secure, and ethical biometric systems makes this ongoing research not only necessary but also inspiring. You play a crucial role in this process and as an expert in this field. New extractors are becoming increasingly popular, especially those based on post-quantum encryption techniques.

3. Proposed System

In this Section we have discussed the detailed methodology and proposed algorithm in detail are discussed in next Subsections.

3.1 Research Methodology

In this manuscript we proposed a technique to improve the efficiency of banking applications. Furthermore, a deep learning-based facial recognition technique is used in the search model. The author uses photographs taken with mobile cameras as input data for the application. Before starting the facial recognition process, the input data is preprocessed to ensure normalization and consistency. Face detection, feature extraction, and face matching are the three basic steps in a typical facial recognition process. If the facial features in the captured image match those

of a person registered in the database, the identification process is considered complete. Facial data is extracted by the system and stored in the server database. The research study uses mobile camera to improve real-time identification, login, and registration for banking applications. The Kotlin programming language is used in Android Studio to create applications that are flexible enough to handle large amounts of data. Figure 1 represented the flow of the proposed system.

3.2 Proposed Model

When users register for the developed application, they take a photo with their phone. Each user's facial information must be entered correctly into the system. To enable further use of the facial recognition process, this image is stored in the Face Cloud database for automated learning on the training

The AI engine takes a face image. In order to evaluate and understand the person's facial structure, the face image is entered into the computer within the scope of face recognition. The distance between the eyes, orbital depth, the vertical distance between the glabella and the tongue, the shape of the cheekbone arches, the alignment of the lip and ear bones are important factors. The approach we propose determines the distinctive facial features that can be used to distinguish individuals in the main database. After the photo is converted into data by the system, the face recognition process is started. This process converts a photograph of a person's face into a set of digital information based on their individual facial features and characteristics. Algorithms process the facial features and generate unique facial data for each person. The next step is to conduct a comparative study with the existing facial database. Resnet and ArcFace models are used to create the facial recognition algorithm. Finally, a database is created to facilitate the storage of facial data. Once the captured face has been successfully compared with an image stored in the server database, the identification process is complete. If this requirement is not met, the user will not be able to use the banking application.

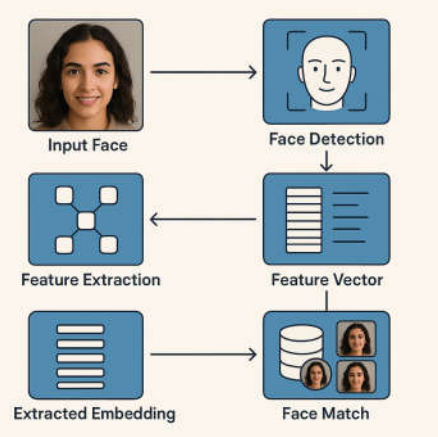

Fig. 1: Flow diagram of proposed system

3.3. Designed AI Engine

The AI engine selects the highest-quality image after dividing the video stream into multiple frames. The facial image is fed into the program to examine and decode the structure of the person's face as part of the facial recognition process. The technique of detecting or validating one or more faces in an image is sometimes called facial recognition. The three main processes of facial recognition are generally face matching, feature extraction, and face detection in an image.

3.3.1 Face Detection Process. The process of identifying a human face without comparing facial features is called face detection. In this study, a multi-task cascaded convolutional network (MTCNN) is used to detect and align faces. Developed in 2006, MTCNN is a powerful neural network for detecting faces and determining their location. . Pseudocode 1 shows the feature detection procedure

Pseudocode 1 : Face Detection
1. Input for face recognition: A dataset of facial images must be identified. Output: A face was found in the blue rectangle.
1. Split the live video stream into multiple frames.
2. Preprocess the image pyramid. Resize the image (224, 224).
Convert colors from cv2.COLOR_BGR2RGB. Calculate the image integral.
normalize the image.
3. To enable accurate delineation of facial areas in an image, apply the face recognition model.
Find a face. Discover faces (img_rgb)
x, y, w, and h = Detect["Yaw Angle, Roll Angle"] represents the drawn detection frame.
img[int(y):int(y + h), int(x):int(x + w)] = detected face
4. Return the recognized face.

3.3.2 Face Extraction Process: The first essential step in effectively representing facial information in face recognition applications is feature extraction. Each of the finite number of elements that make up a digital image has a unique value at a given position. The final product is a feature vector indicating the position of the face. Pseudocode 2 shows the feature extraction procedure.

Pseudocode 2: Feature Extraction
Input: A collection of labeled images of people. Result: Each person's label was used in the email script to create a mailing list.
1. Define the image data
img_pixels = np.expand_dims(img_pixels, axis = 0) img_pixels = image.img_to_array(img)
2. The nature of the process
For the image_images dataset:
image = preprocess(size = "224,224", bbox, landmark)
bounds, bbox = SSD(image) add list image
The image index is rendered as a collection of aligned face images in a 224 × 224 format.
3. Extract photo features and store them in a database.
For labeled records: Face recognition: Image: Index of images in each folder; image = preprocess(size="224,224") for image in images; Pred = SSD(image), bbox
Feature = list_feature.append(Feature) modelResNet.get_feature(bbox)
folder.append(list_label)
4. Return the white label and index function

3.3.3 Face Recognition Process: The principle of face recognition is that the closer two images (of the same person) are to each other, the more similar they are. Conversely, the farther the distance between the two images, the more similar they are. The distance between the input image (u(x1, y1)) and the data image (v(x2, y2)) is the standard Euclidean distance. Pseudocode 3 shows the feature recognition procedure.

Pseudocode: Face Recognition
Input: A collection of people's photos with identified and extracted features.
Output: List the record details.
1. ResNet34 model instruction "
Keras layer input image (shape = (116, 116, 4)) x = keras.layers.tensorflow
To configure a Keras layered model, add an image. Normalized output model images.
2. Block1(x, Filter, conv_shortcut = true, Name = None, Pass = 1, Kernel size = 3);
bn_axis = III.
short = add_tensorflow_keras_layers(layer arguments)(x) if conv_shortcut
Else short = x
3. Step 1: 'stack1(x, filters, blocks, strid1' = 2, name = None): x = block1(x, filters, strid = str1, name = name + '_block1'
x = block1(x, filters, conv_shortcut = false, name = name + '_block' + str(i)) for i in the range (2, blocks + 1) returns x
The fourth step is stack_fn(x): x = STACK(x, 64, 3, name = "conv2"). (x, 128, 4, name = "conv3") = stack (x, 256, 6, name = "conv4").
dat Stack1(x, 512, 4, name = "conv5").
5. Calculate theta and marginal logit
6. Decide
If the squared distance or cosine similarity is less than the interval; Face matching in return

4. Result Analysis Method and Metrix

In this Section we will discuss the result and analysis in detail, rest of the details are discussed in upcoming subsections.

4.1 Data Collection:

The author of this study collected 210 facial images from the subjects and placed them on a database server. The collected data included 206 functional subgroups (eyes, eyebrows, nose, lips, chin). For each participant, face-to-face image data was collected at two stages: registration time and login time. The authors of FRR and ERR provided a demonstration using wide-ranging applications.

4.2 Facial Biometric Analysis

There are methods to confirm the legitimacy of the facial biometric authentication procedure. The techniques called FAR, FRR, and EER use the percentage of applications logged in by legitimate users and those that would

not validate the authentication process. The formulas for FAR, FRR, and EER analyses are specific. The login value of each user is used to determine the system performance, which provides the FAR and FRR values. FAR and FRR were applied during the application login phase.

4.2.1 False Acceptance Rate (FAR)

The failure rate of accepting a fraudulent user as an authorized user is defined by FAR. FAR informs the user about the security of their authentication. If hackers can easily log in to the authentication system, the FAR percentage is higher. By calculating the success value of each user to evaluate the performance of the system, the proposed system achieves the FAR value. The FAR analysis, which determines the number of fraudulent users recognized as legitimate users, is presented in Table 1 to verify the legitimacy of the system. This FAR technique was used throughout the connection process. The formula for determining FAR is:

$$\textbf{FAR} = \left(\frac{\text{Number of wrong acceptances}}{\text{Total number of intruder attempt made}}\right) * 100$$

Table 1: FAR Analysis

No of User	FAR
206	1.66%

4.2.2 False Rejection Rate (FRR)

The percentage of errors that occur when an authorized user is rejected as fraudulent is indicated by FRR. FRR determines whether an application is authentic and usable. The authentication mechanism may not detect a valid user if the FRR percentage is higher. By using each user's pass-through value to obtain the system's performance, the proposed solution achieves the FRR value. Check out the FRR analysis, which shows how many authenticated users were rejected as fraudulent after 206 people attempted to log in and use the application. The formula to determine FRR is:

$$\textbf{FRR} = \left(\frac{\text{Number of wrong rejections}}{\text{Total number of genuine attempts made}}\right) * 100$$

Table 2: FRR analysis

No of User	FRR
206	6.73%

4.2.3 Equal Error Rate (EER) Analysis

The EER compares and evaluates the overall accuracy of different biometric authentication techniques and displays several performance metrics. The EER is determined by finding the intersection of two graphs, the first being the FRR and the second the FAR. The formula to determine the ERR is:

$$\text{ERR} = \left(\frac{\text{FRR} + \text{FAR}}{2}\right)$$

FAR and FRR are used to examine the dataset and determine the EER value; The success value is variable, meaning it is determined independently for each subject. Only the time domain data is analyzed. The EER data in Table 4 illustrates the EER value.

Table 3: EER Analysis

User	FAR	FRR	EER	Accuracy
206	1.66%	6.73%	4.195%	96%

4.2.4 Accuracy

The accuracy of the system has been determined using the effectiveness percentage when it comes to identification methods, where a threshold may not always be a parameter that is available. This percentage is obtained by dividing the number of correctly identified users by the total number of users. For instance, the accuracy A of the system would be shown as follows if u is the number of successfully identified users out of a total of U users:

$$A = u/U \cdot 100.$$
$$96.11 = 198/206 \cdot 100$$

4.3 Result Analysis

We have performed several experiments and do the result analysis and comparative studies in details. All are discussed in the upcoming subsections.

4.3.1 Results of FRR, FAR and EER

The author, after reviewing the data obtained for this study, established a False Rejection Rate of return (FRR) of 6.73% and a False Acceptance Rate of return (FAR) of 1.66%. FRR and FRR percentage indicate the performance of the system. If the FRR percentage is high, it can be considered. On the other hand, if the security return percentage is high, this cannot be the case, as the system demonstrates that hackers could access and steal confidential banking data and can-do illegal money transactions from the application. The system's Equal Error Rate (EER) of 4.195% proves its accuracy. The proposed system has been proven to be safe and effective for many users. This proposed system is completely beneficial for all kinds of banking applications and can stop unauthorized access from the intruders as accuracy is 96%, which is better than previous studies.

Comparative Study of FAR, FRR and EER

In Table 4, FAR, FRR, and ERR of previous studies are compared. Where more than 50 users, the FAR value was close to or greater than 10%, while the ERR value was above 10%. Given that there are only 50 users, the FAR value in the Karatzouni S. Clarke 2007[36] study is larger than the FRR. The FAR, FRR, and EER values in the study by Lin J-H, Chang T-Y, and Tsai C-J (2012) [34] are nearly identical. When the FAR number is greater than the FRR, the system becomes risky (Darren Cilia Frankie Inguanez 2018 [32]).

Study	User	FAR%	FRR %	EER %
Kyle R. Corpus, Ralph Joseph DL.Gonzales,2016[31]	6	7.0	40	-
Darren Cilia Frankie Inguanez2018 [32]	24	4	3	3.93
Tanapat Anusas-amornkul2000 [33]	20	-	-	5.1
Lin J-H, Chang T-Y, Tsai C-J,.2012 [34]	100	14.54	14.6	14.6
Cheng PC, Tasia CJ, Chang TY, Lin JH.2014 [35]	100	9.78	19	10
Karatzouni S, Clarke N.2007 [36]	50	15.8	9.1	12.2
V Pragya, K Manju, R Linesh [10]	208	1.66	6.730	4.1

Table 4 Comparison of FAR, FRR and ERR

In this research, author measured FAR value 1.66% of 60 subjects, FRR 6.730% of 208 subjects and EER value 4.1 of the KDSmart system. FAR is less than FRR which is a great number as compared to other studies, it makes system reliable and authentic. It determined that KDSmart system is secure and working good in large amount of people.

5. Conclusion

The author of this research study created a banking application based on multi-factor authentication. This application uses a user ID and password to verify the user's identity. Once the ID and password are matched, the user's facial features are used to confirm their identity. The process of accurately identifying a face in an image or video by comparing it to an existing facial database is called facial recognition. First, it detects and separates human faces from other objects in the image. Then, it identifies these faces. The authors analyzed the application using FAR, FRR, and EER and achieved an accuracy of 96%, significantly exceeding previous studies. This demonstrates that the developed application can leverage facial recognition technology to improve the security of banking applications on mobile devices. To further improve security, the authors plan to use pattern recognition in the future.

References

[1] Smith-Creasey, M., Albalooshi, F. A., & Rajarajan, M. (2018). Continuous face authentication scheme for mobile devices with tracking and liveness detection. *Microprocessors and Microsystems*, *63*, 147-157.
[2] Jafri, R., & Arabnia, H. R. (2009). A survey of face recognition techniques. *journal of information processing systems*, *5*(2), 41-68.
[3] Mohan, J., & Rajesh, R. (2021). Enhancing home security through visual cryptography. *Microprocessors* and Microsystems, 80, 103355.

[4] Adesuyi, F. A., Oluwafemi, O., Alabi, I. O., Victor, A. N., & Rick, A. V. (2013). Secure authentication for mobile banking using facial recognition.
[5] Stragapede, G., Vera-Rodriguez, R., Tolosana, R., Morales, A., Acien, A., & Le Lan, G. (2022). Mobile behavioral biometrics for passive authentication. Pattern Recognition Letters, 157, 35-41.
[6] Saxena, N., & Varshney, D. (2021). Smart home security solutions using facial authentication and speaker recognition through artificial neural networks. *International Journal of Cognitive Computing in Engineering*, *2*, 154-164.
[7] Xue, B., Yang, Q., Jin, Y., Zhu, Q., Lan, J., Lin, Y., ... & Zhou, X. (2023). Genotoxicity assessment of haloacetaldehyde disinfection byproducts via a simplified yeast-based toxicogenomics assay. *Environmental Science & Technology*, *57*(44), 16823-16833.
[8] Pérez, J.C., Alfarra, M., Thabet, A., Arbeláez, P., Ghanem. B. Towards assessing and characterizing the semantic robustness of face recognition. arXiv preprint arXiv:2202.04978 (2022)
[9] Vaishnav, P., Raja, L., Singh, P., & Vairavasamy, R. Multilayered authentication for ATM transaction using keystroke dynamics and touch dynamics.
[10] Vaishnav, P., Kaushik, M., & Raja, L. (2022). Design An Algorithm For Continuous Authentication On Smartphone Through Keystroke Dynamics And Touch Dynamics. *Indian Journal of Computer Science and Engineering*, *13*(2), 444-455.
[11] Cheema, U., Ahmad, M., Han, D., & Moon, S. (2021). Heterogeneous visible-thermal and visible-infrared face recognition using unit-class loss and cross-modality discriminator. *arXiv preprint arXiv:2111.14339*.
[12] Ahmad, M., Cheema, U., Abdullah, M., Moon, S., & Han, D. (2021). Generating synthetic disguised faces with cycle-consistency loss and an automated filtering algorithm. *Mathematics*, *10*(1), 4.
[13] Cheema, U., & Moon, S. (2023). Disguised heterogeneous face recognition using deep neighborhood difference relational network. *Neurocomputing*, *519*, 44-56.
[14] Kowalski, M., Grudzień, A., & Mierzejewski, K. (2022). Thermal–visible face recognition based on cnn features and triple triplet configuration for on-the-move identity verification. *Sensors*, *22*(13), 5012.
[15] Abdullah, M., Lee, A., & Han, D. (2022, October). GAN based Visible to Thermal Image Translation. In *2022 IEEE International Conference on Consumer Electronics-Asia (ICCE-Asia)* (pp. 1-3). IEEE.
[16] Ahmad, M., Abdullah, M., & Han, D. (2022, July). One-Shot Synthetic Disguised Face Generation to improve Robustness against Disguise Attacks. In *2022 37th International Technical Conference on Circuits/Systems, Computers and Communications (ITC-CSCC)* (pp. 1038-1041). IEEE.
[17] Alkadi, A. M., AlMahdawi, R. A., Anwahi, S. M., & Soudan, B. (2023, February). Biometric authentication based on multi-modal facial recognition using machine learning. In *2023 Advances in Science and Engineering Technology International Conferences (ASET)* (pp. 1-6). IEEE.
[18] Padmashree, G., & Kotegar, K. A. (2024). Skin Segmentation-Based Disguised Face Recognition Using Deep Learning. *IEEE Access*.
[19] Y. Dodis, L. Reyzin, and A. Smith, ''Fuzzy extractors,'' in *Security With Noisy Data: On Private Biometrics, Secure Key Storage and Anti- Counterfeiting*. Berlin, Germany: Springer, 2007, pp. 79–99.
[20] Dodis, Y., Reyzin, L., & Smith, A. (2004). Fuzzy extractors: How to generate strong keys from biometrics and other noisy data. In *Advances in Cryptology-EUROCRYPT 2004: International Conference on the Theory and Applications of Cryptographic Techniques, Interlaken, Switzerland, May 2-6, 2004. Proceedings 23* (pp. 523-540). Springer Berlin Heidelberg.
[21] Li, N., Guo, F., Mu, Y., Susilo, W., & Nepal, S. (2017, June). Fuzzy extractors for biometric identification. In *2017 IEEE 37th International conference on distributed computing systems (ICDCS)* (pp. 667-677). IEEE.
[22] Kirss, J. M. (2022). 'Biometrics in splitkey using fuzzy extraction. *Cybernetica AS, Tallinn, Estonia, Tech. Rep. D-2-456/2022*.
[23] Horowitz, M., & Grumbling, E. (Eds.). (2019). Quantum computing: progress and prospects. Washington, DC, USA: National Academy of Sciences, 2018.
[24] Preskill, J. (2018). Quantum computing in the NISQ era and beyond. *Quantum*, *2*, 79.
[25] Bernstein, D. J., & Lange, T. (2017). Post-quantum cryptography. *Nature*, *549*(7671), 188-194.
[26] Overbeck, R., & Sendrier, N. (2009). Code-based cryptography. In *Post-quantum cryptography* (pp. 95-145). Berlin, Heidelberg: Springer Berlin Heidelberg.
[27] McEliece, R. J. (1978). A public-key cryptosystem based on algebraic. *Coding Thv*, *4244*(1978), 114-116.
[28] Chingovska, I., Erdogmus, N., Anjos, A., & Marcel, S. (2016). Face recognition systems under spoofing attacks. *Face Recognition Across the Imaging Spectrum*, 165-194.
[29] Hamme, T. V., Garofalo, G., Joos, S., Preuveneers, D., & Joosen, W. (2022). AI for biometric authentication systems. In *Security and Artificial Intelligence: A Crossdisciplinary Approach* (pp. 156-180). Cham: Springer International Publishing.
[30] Kuznetsov, A., Kiyan, A., Uvarova, A., Serhiienko, R., & Smirnov, V. (2018, October). New code based fuzzy extractor for biometric cryptography. In *2018 International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T)* (pp. 119-124). IEEE.
[31] Kyle R. Corpus, Ralph Joseph DL. Gonzales,Larry A. Vea, Alvin Scott Morada, "Mobile User Identification through Authentication using Keystroke Dynamics and Accelerometer Biometrics" IEEE/ACM International Conference on Mobile Software Engineering and Systems, (2016).

[32] Darren Cilia Frankie Inguanez, “Multi-Model authentication using keystroke dynamics for Smartphones”, Information and Communication Technology Institute, University College, Malta College of Arts, Science and Technology Corradino Hill, Paola PLA 9032, Malta, (2014).
[33] Tanapat Anusas-amornkul, ”Strengthening Password Authentication using Keystroke Dynamics and Smartphone Sensors” Department of Computer and Information Science, King Mongkut’s University of Technology North Bangkok, THAILAND. (662) 555- ext 4618, (2000).
[34] Chang T-Y, Tsai C-J, Lin J-H, “A graphical-based password keystroke dynamic authentication system for touch screen handheld mobile devices”. Journal of Systems Software. 85(5):1157–65, (2014).
[35] Chandrasekar Venko Vivekanandha Educational Institutions, Krishna Sankar P 3Edge Solutions, “Biometric Authentication Based on Keystroke Dynamics for Realistic User” Chennai See discussions, stats, (2014).
[36] Karatzouni S, Clarke N., “Keystroke analysis for thumb-based keyboards on mobile devices”. IFIP International Federation for Information Processing, New approaches for Security, Privacy and Trust in Complex Environments; Boston. p. 253–63, (2007).