ROMANIAN JOURNAL OF INFORMATION SCIENCE AND TECHNOLOGY
Volume **26**, Number 2, 2023, 151–162

Biometric Authentication Model Based on Transformation of Face Image into a PIN Number Usable During the Covid-19 Pandemic

Nenad BADOVINAC* and Dejan SIMIC

Faculty of Organizational Sciences, University of Belgrade, Jove Ilica 154, 11000 Belgrade, Serbia
E-mails:nenad.badovinac@gmail.com*, dejan.simic@fon.bg.ac.rs
* Corresponding author

Abstract. The digitization trend is developing throughout the crisis caused by the COVID-19 pandemic. The volume of digital payments is increasing. The most common way of checking the authentication in electronic payment systems is the PIN number that users type into the PINPAD device. Digital payment devices still require the entry of smart cards and the manual entry of a PIN into an ATM or POS device. In order to reduce the possibility of infection due to contamination from multiple touches of the PINPAD device by different people, cardholders use the PINPAD device with gloves. Instead of entering the PIN number on the PINPAD device, biometric authentication is available for the authentication process. On the other hand, the use of gloves and a medical face mask, during the Covid-19 pandemic, limits the biometric scanning of fingerprints and facial images. In this paper, a biometric authentication model is proposed that uses biometric features of the eyes, as these biometric data are available to scanners even in the case when the cardholder uses a protective medical mask on his/her face. The proposed model transforms data on the basis of correlations of characteristic points around the eyes and eye color into a stable PIN. Quantitative presentation of the experimental results confirms that for six different facial expressions of each of the 50 tested persons, the deviation of the authentication PIN from the reference PIN does not exceed 1%. Using the proposed innovative model, the existing infrastructure of payment systems should not be changed.

Key-words: biometric authentication; Covid-19; electronic payments; facial biometric; PIN number.

1. Introduction

The authentication model in which the cardholder enters the PIN on the PINPAD device is a widely accepted method of authentication. One of the problems with this method of authen-

tication during the Covid-19 pandemic is the potential source of infection when a cardholder needs to enter the PIN on the PINPAD device or when it needs to be biometrically authenticated by scanning a finger on a biometric scanner. Unhygienic fingers can potentially leave behind surviving bacteria including COVID-19, which is mainly spread by contaminated hands [1]. Research has shown that the COVID-19 virus can last up to 72 hours on plastic and stainless steel [2]. Instead of typing the PIN, where the customer needs to bring a card and touch the machine for electronic data recording, authentication by facial recognition can be developed. In order to avoid the transmission of COVID-19 to card users as a means of payment, it is necessary to develop a new electronic payment model. This paper is a continuation of the author's research published in "A Multimodal Biometric Authentication (MBA) in Card Payment System", 2019 International Conference on Artificial Intelligence: Applications and Innovations (IC-AIAI) [3]. In this paper, a model of transformation of biometric data of a fingerprint and a face image into a multi-digit PIN is presented. A non-invasive biometric method was used, which does not require physical contact with the biometric sensor, and which will be useful in case the cardholder has a covered face with a medical mask as protection against Covid-19 virus infection.

The contribution of the research is a software system for PIN authentication that is intended for use during a virus pandemic, but also in other cases when there is a reduced possibility of using traditional PIN authentication methods. The capability of the presented authentication model is in the fact of a simple upgrade of the existing PIN authentication model with a view of users' health care, because they will have a simpler interface of the existing ATM and POS infrastructure with cameras even when wearing a face mask.

By applying the presented model of PIN authentication in e-payment systems, the user will not have to enter the authentication PIN, as it will be created from the biometric data of the face image and in the case when wearing a medical mask on his/her face. During the virus pandemic, it is possible for financial institutions to set the PIN authentication model to either the classic method in which the PIN is entered on a PINPAD device, or to the introduced biometric method in which the PIN is calculated from the biometric data of the facial image.

Biometric payments are an option that reduces the risk of infection when performing payment transactions [5]. The European Union's Second Payment Services Directive (PSD2) excludes the possibility of applying e-payment authentication models based only on payment card data [4]. New research on e-payment models that will meet the Regulatory Technical Standards on strong customer authentication and secure communication under PSD2 is needed. One of the most innovative technologies, with the greatest growth potential, is based on the use of biometric techniques, with predictions that by 2025 they will be used to authenticate more than $3 trillion in payment transactions, compared to only $404 billion in 2020, and that's an increase of 650% [6]. Payment systems based on facial image recognition have not yet been sufficiently studied and there is no standardization for biometric authentication, but this technology provides the highest security in user authentication [7]. Unlike other biometric attributes, such as fingerprints, their use does not require physical contact with the device.

During the Covid-19 pandemic [8] new payment systems have been established to reduce contact between buyers and sellers. The authors in [9] investigated and concluded that there are concerns about the collection of biometric data. The presented method uses a limited set of biometric data, and this has a positive effect on protecting the cardholder's privacy.

During the research, the main challenges were the research of existing literature, regulations and standards on biometric cardholder authentication methodologies in electronic payment systems and investigating available biometric SDK software environments solutions. A Python

code was developed for a commercial SDK software solution [10] that calculates the IPD distances and the average RGB value of the eye pigment from the face image, as well as the final PIN. The challenge was to research a database of facial images that could be used for research. A professional image database [11] was used, which was created at Binghamton University in New York and is often used by researchers.

This paper is conceived as follows: Section 2 presents an overview of previous research. Section 3 presents a conceptual model of the authentication method, and Section 4 describes the algorithm. Section 5 presents the results of experimental research. There is a Future Work given in Section 6, and conclusions are highlighted in Section 7.

2. Review of the State of the Art

Available scientific papers in the field of transformation of biometric data into PIN were researched. The authors of [12] note that biometric technologies are gaining great popularity due to the ease of acquisition of biometric samples. However, in their model, the biometric samples are stored and recorded, while on the other hand, the advantage of our model is that the biometric data is not stored on the medium. In the model [13], the authors present an e-payment model in which, in the authentication process, the biometric sample of the face image is compared with the template found in the database, and then the biometric sample of the fingerprint is compared with the template in the database. Once both authentication schemes are confirmed, access to the bank account will be granted. The authors of [14] present an e-payment model in which biometric data is encrypted because they believe that it is necessary to encrypt them in order to preserve a person's identity. In the presented model, the identity of a person cannot be revealed because a limited set of biometric data is used. In the paper [15], the authors state that the exponential growth of storing biometric data leads to the creation of a large amount of data. The authors propose a model for mobile biometric authentication based on data storage in the Cloud. The authors of [16] use Reed-Solomon codes to generate keys and correct wrong codes. The authors of [17] during the Covid-19 see the limitations of the biometric authentication model and say that fingerprints or systems based on facial recognition may not be applicable in a pandemic situation like this one, when gloves or face masks are mandatory for protection from unwanted exposure. They use behavioral biometric methods. Models for the transformation of fingerprint biometric data into a Password are presented in [18, 19]. A comparison of these methods is synthesized in Table 1, which is available in a PDF file at the link [20].

Generating a stable password from biometric data has been a challenge for many authors [21–24] as it is difficult to overcome the instability of biometric characteristic points. The authors of [25] present a comparison of methods for creating digital keys from biometric data.

We studied the scientific literature and concluded that the PIN / Password can be easily compromised, and smart cards can be lost, but that biometric features are suitable for user authentication. The risk of infecting users with Covid-19 and other viruses and diseases when using an ATM, a POS device with a built-in PINPAD, and a biometric fingerprint scanner is raised. Using these devices, users are at risk of transmitting infectious diseases [26]. Viruses can enter the human body directly and indirectly. Direct transmission can occur through close contact with people infected with the virus, while indirect transmission can occur through intermediate media, such as the surface of POS and ATM devices [27].

Such as fingerprint authentication, some face image authentication models will not be applicable during the Covid-19 pandemic, as the mandatory wearing of protective gloves and a face

mask covering part of the face prevents biometric authentication. Studying the available scientific literature, the authors of this paper recognized the need to create a new non-invasive method of biometric authentication that will be effective during the Covid-19 pandemic.

The scientific contribution presented in this paper refers to a new method of non-invasive biometric authentication using an eye color classifier and correlation of characteristic biometric points around the eyes that will be available to the camera even when the cardholder wears a medical mask (Fig. 1). The authors of the work [28] classified the color of the iris of the eye and constructed a method for automatically extracting the color of the eyes from photographs of the face image and classified it into seven color groups. By applying NIR (near infrared) imaging, the authors in [29] made it easier to extract the texture of even darker eye colors (e.g., brown eyes). It has been shown that in the NIR spectrum, it is possible to distinguish between light eye colors (blue, green) and dark ones (brown). The authors confirmed that readings from NIR iris images contain sufficient information for eye color classification.

3. Transformation of Biometric Data into PIN

To effectively prevent the spread of the COVID-19 virus, almost all people wear face masks. During this period, conventional biometric authentication technologies become ineffective. Fig. 1 shows the face of the cardholder covered with a protective medical mask that will not prevent authentication because the authentication model, presented in this paper, will transform the inner biometric points around the eyes by transforming the biometric data of eye color and correlation of characteristic biometric interpupillary distance (IPD), create a PIN for the authentication process. Using the presented model, the electronic payment authentication process would be as follows: the cardholder inserts the smart card into the smart card reader, ATM and POS device with a built-in camera, or uses a smartphone application that contains the data from the smart card. The face of the cardholder covered with a medical mask (Fig. 1) against Covid19 infection should be in front of the camera. By transforming biometric data from the area of interest from the face image, which is not covered by a protective mask, a PIN is created which will be compared with the authentication PIN that the bank enters as a reference PIN in the smartcard.

Fig. 1. Block diagram and the pseudocode of the proposed approach.

The presented authentication model creates a stable PIN by transforming biometric data of eye color and Euclidean distances of characteristic biometric interpupillary distance (IPD), which are robust to the change of emotion and facial expression. Since the vector of biometric features of the face image is relatively large, the algorithm uses a smaller vector with features whose basic elements are: Eye color feature and IPD (distance between the center of the left and right pupil of the eye). The presented model transforms the biometric data of the face image that are available to the camera when the cardholder wears a medical mask on his/her face (Fig. 1). The following are biometric features available to the camera when the cardholder has a face mask:

1. Eye color is an important facial feature that can be used for authentication [28]. We suggest using a system for eye iris segmentation [30] as well as eye color detection based on the algorithm presented in [29].

2. The pupil is one of the smallest units of the eye. The pupil is located in the center of the Iris of the eye. Researchers in [31] develop the Pixellary Pupil Distance framework in which they use the RGB color spectrum to calculate the distance between the center of the left and right eyes. In our distance calculation algorithm, we use the Euclidean equation, which cannot define a unique distance but allows the 2FA standard to create an authentication PIN. The analysis of iris image data can be improved by applying a neural network [32] or by applying a model based on multi-scale deep learning presented by the author in [33].

3. Radius of the iris – Once the eye is localized, the processing is required to segment the iris region and pupil. After that, it is possible to calculate the radius of the iris [10]. This value will be used to normalize the IPD distance.

The idea of the presented authentication model is that the difference obtained in the phase of comparing the vector of biometric features of the face image, and the reference vector, be as small as possible. The proposed model uses an algorithm to transform the face image vector into a PIN that is compared to the PIN obtained by transforming the reference vector. In case the PINs are the same, the cardholder authentication will be confirmed. The research presented in Section 5 has shown that the algorithm does not always transform cardholder biometric data into the same PIN, but the PINs are different for the same person's facial images. Given this instability of biometric characteristics, the allowed deviation of the PIN obtained in the authentication process and the reference PIN written on the smart card has been defined. The PIN created in this way will be robust to change of the expression, i.e. facial emotions. The algorithm of the presented authentication model is divided into two parts. In the first part, a biometric feature of eye color is used, and in the second part, IPD distance. There are many types of ATM devices used to issue cash. Most of them have a screen, a card slot, a cash slot, a PINPAD and a camera. A classic ATM transaction involves the user inserting a smart card into the slot, entering their authentication number (PIN), and after verifying the authentication, withdrawing cash. This simple procedure can be upgraded with a software update with a proposed authentication model that would use a camera to make a photo of a cardholder's face, instead of manually entering a PIN. The software would create an authentication PIN from the biometric data of the face image, that would be compared to the PIN written in the chip on the smart card or on the remote server. In the case that the authentication system is set up to allow the PINs obtained in the authentication process to deviate from the reference PIN, the device would confirm the authenticity of the user and allow electronic payment. In the case that the deviation exceeds the allowable threshold, user

authentication and payment transactions would be denied. There are many types of POS devices and ATM machines that have built-in cameras. The payment procedure using a POS device with the camera shown in Fig. 2, i.e. a POS device that has a built-in camera for photographing faces [34] available in a PDF file on weblink [20], with the biometric authentication model presented here, instead of entering a PIN, would require the camera to photograph the cardholder's face after he leans forward and removes the smart card.

The software would create a PIN from the face image, which would be compared to the reference PIN written in the chip on smart cards or on a remote server. In case the compared PIN has a deviation of less than 1%, the device would authenticate the cardholder and execute the electronic payment transaction, otherwise, the authentication would be denied.

4. Algorithm Implementation

The biometric authentication model process can take place in a smartphone, in an ATM machine or POS device with a camera. In the enrollment process, the biometric data of six facial images of different facial expressions of the cardholder are transformed into a PIN, and the mean value of the six PINs thus obtained will be the reference PIN. The reference PIN should be entered in the memory of the smart card or in the remote server. In the authentication process, the PIN is compared to the reference PIN. The basic idea was to always transform biometric data into the same PIN, but experimental research, presented in Section 5, showed that this was not the case.

Therefore, it is envisaged that the software in the authentication device, in the process of comparing the authentication PIN and the reference PIN, authenticates the cardholder with the allowed deviation of the authentication PIN. The results of experimental research presented in Section 5 show that, under this condition, the presented innovative model enables biometric authentication. The authentication device software will be upgraded for the process of creating a PIN from biometric data of a face image that has in Algorithm 1:

- FUNCTION (Create a PIN number for the uploaded photo)
- FOR FaceImage do Detection (Iris Landmark (5 points)) [10]
- FOR (Iris Landmark) do:
  - Calculate (Iris Radius)
  - Calculate (IPD EuclidDistance)
  - Calculate (Iris RGB color do = Color Parameter)
  - Calculate (PIN = (4000 x Iris Radius / IPDEuclidDistance)+Color Parameter)
- Return PIN
- END function

The proposed model of cardholder biometric authentication that can be applied in e-payment systems is represented by a block diagram in Fig. 3, which is available in a PDF file on weblink [20]. The first step is the activation of one of the two authentication modes - entering a classic or

biometric PIN. In the first solution, the system will ask the cardholder to manually enter the PIN on the PINPAD device, while in the second solution, the system will ask the cardholder to place his face in front of the camera. The system will create the PIN and in the final step will compare it with the reference PIN written on the chip.

The idea presented in this paper is to enable the most accurate possible method for biometric authentication using a PIN created from biometric facial image data. Therefore, it is important to distinguish as accurately as possible biometric characteristics such as the characteristic points surrounding the eye's iris, and its color. The programming code was developed within the Python programming language and using the Ailia SDK development environment [10], which ultimately creates a PIN from the biometric characteristics of the face image. The program code has two basic functions: 1) IPD calculation and PIN calculation; 2) Determining eye color. The number of PIN digits in the model is a parameter. The value of the parameter can be 4 or more.

4.1. Algorithm creates a 4-digit number from the Interpupillary distance

After loading the photograph of the face image, the extraction of characteristic biometric points around the eyes is performed. Then, the face image is normalized with a radius of the Iris value, and the IPD distance is calculated rounded to a 4-digit number. For the purposes of this research, Python program code was developed using the Ailia SDK working environment and Mediapipe Iris model [10] to identify characteristic points of the face, iris, pupil and eye contour. The Mediapipe Iris model is used to detect the 5 key points of the outer circle of the eye's iris and the center of the eye's pupil. The input value of this function of the program code is the coordinates of the points bounding the surface of the iris of the eye obtained from the Mediapipe Iris model.

The calculation of the IPD and radius of the iris is based on the geometric characteristics of the face, while the color of the iris is based on the most common RGB pixel value.

5. Experiments

For the needs of experimental research, a program code transforms the biometric data of a face image into a 4-digit PIN. The program code was developed according to the model shown in Algorithm 1 and was applied to the Facial Expression Database. The experiments used a large database of face images of different people and different facial expressions BU-4DFE (3D Dynamic Facial Expression Database) from Dr Lijun Yin at the Department of Computer Science, State University of New York at Binghamton [11]. Those databases are used in numerous research projects. All eyes in the study were classified as brown eyes. In the first study, the deviation threshold of the presented authentication model was calculated, which will enable every person for whom a test was performed to authenticate. In another study, the probability of false acceptance was calculated, in case the person with the most common PIN loses the authentication smart card.

5.1. Case Study 1

In this research, images of different facial expressions of 50 people were transformed into a PIN. Facial expressions are divided into: Angry, Disgust, Fear, Happy, Sad and Surprise, an example is illustrated in Fig. 4, which is available in a PDF file on weblink [20].

Table 3 available in a PDF file on weblink [20] shows the created PINs and the values of the standard deviation of the PINs from the reference PIN. In the authentication process, the reference PIN (r) is calculated as the arithmetic mean of the PIN (1–6) obtained from 6 facial images of the same person. In the last column in this table is the standard deviation for 50 people. This value is from 5 to 19 PINs.

Five levels with different standard deviations of the presented authentication model were defined. Table 4 available in a PDF file on weblink [20] shows the results for the case the authentication model is set with a tolerance threshold of 1.00% of the allowed deviation of PIN(r) from the PIN obtained in the authentication process, all persons with six different facial expressions were successfully authenticated.

5.2. Case Study 2

This research was done with 94 face images, one image of a neutral facial expression for each of the 94 persons. The calculated minimum PIN is 3341 and the maximum PIN is 3473, which is a range of 132 PINs. In Case Study 1, the maximum deviation of the reference PIN from the PINs created from different facial expressions was calculated and it is 19. Groups of 19 PINs were created, starting from the minimum to the maximum PIN. Table 5 available in a PDF file on weblink [20] shows the groups of PINs and frequencies of persons belonging to a particular group.

The results of the research show that out of the total number of tested people, 28.72% have a PIN in the range of the most common PIN. Quantitative presentation of experimental results on the presented authentication model works with the probability that the highest possible rate of falsely authenticated people is 28.72% because so many people can have the most common PIN. On the other hand, this model will, in at least 72.28% of cases, recognize and reject the attempt of false authentication.

In the results of the research of the presented authentication model based on a smart card, there is a possibility that more people have the same PIN, but this is not a problem, because it is suggested to use a smart card as a second layer of cardholder authentication. The use of the second authentication layer will reduce the rate of false acceptance and thus reduce the percentage of cases of misuse of the presented authentication model, which will be possible in cases where cardholders wear protective masks on their face.

6. Future Work

The disadvantage of the presented model is that daylight is required to detect the correct eye color. Room light darkens the color of the eyes, and a deviation of eye color coding occurs. In future work, we can change the algorithm and create numerical values in the form of asymmetric keys only from the value of the interpupillary distance. Methods for creating asymmetric keys from biometric data are analyzed in the paper [25].

We suggest researching the application of the model in the system of border crossings in which, along with the passport check, a numerical sequence (password) would be checked, which would be created from the biometric data of the face image, and thus improve the performance of the system.

A direction of further research besides the application of asymmetric keys is the application of artificial intelligence tools as presented in [12]. Artificial intelligence would help detect

anomalies in the locations with which the cardholder logs into an ATM or POS device, such as cases when the distance between the location of the previous login and the location where the login attempt was made is not close, and the time interval is not sufficient for the user to be at another location.

We will develop our model for use in digitally signing Blockchain transactions. By synthesizing Blockchain technology, which eliminates the obligation of the presence of a third-party validator of transactions from the electronic payment model, and biometric technology, which allows signing a blockchain transaction without a token, the existing system can be improved for working with payment cards [25]. This will allow us to apply biometric authentication for digitally signing transactions with digital currencies of central banks - CBDC.

In 2023, more than 20 countries will take significant steps toward piloting CBDCs. Australia, Thailand, Brazil, India, South Korea and Russia intend to continue or begin pilot testing in 2023. As of the end of 2022, all G7 countries have entered the CBDC development phase. The European Central Bank has launched a project to research the development of CBDCs [35].

7. Conclusions

This paper presents an innovative model of biometric authentication of the electronic payment system that is applicable in the era of the Covid-19 virus pandemic. Recommendations for maintaining health during the pandemic suggest the wearing of a protective face mask and protective gloves for the hands. The presented model of biometric authentication enables the conversion of biometric features from faces that are not covered by a protective medical mask into a PIN.

The model is based on a non-invasive method of acquisition of a biometric facial image sample. Biometric data is not stored on media and cannot be compromised. The biometric authentication model enables the protection of a person's identity and privacy, as it uses a limited set of facial image biometric data from which it is not possible to reveal the person's identity. Cardholder authentication is possible even when the face is masked and the facial expression changes.

The results of the research show that the method of transforming the biometric features of the IPD distance into a PIN, with a deviation from the reference PIN of 1%, enables the authentication of the cardholder wearing a medical mask. They also show that out of the total number of people tested, 28.72% of them have a PIN in the range of the most common PIN. On the other hand, this model will reject a fraudulent authentication attempt at least 72.28% of the time. This result is further increased because the model meets the 2FA (two-factor authentication) international standard through the obligation that the cardholder uses a payment card and biometric data for authentication. The research results confirm that bank clients, even with the minimum range of biometric data related to the interpupillary distance between the center of the left and right eyes, can use the advantages of biometric authentication.

The presented method has implications for financial institutions and end users of banking services. Financial institutions can implement a biometric authentication model during a pandemic without changing the existing authentication infrastructure. A software update in POS and ATM devices with built-in cameras is sufficient. By using the presented model, end users get a simple authentication process by placing their faces in front of the camera.

References

[1] G. KAMP, D. TIDT, S. PFAENDER and E. STEINMANN, *Persistence of coronaviruses on inanimate surfaces and their inactivation with biocidal agents*, Journal of Hospital Infection **104**(3), pp. 246–251, 2020.

[2] S. MANIGANDAN, M.-T. Wu, V. K. PONNUSAMY, V. B. RAGHAVENDRA, A. PUGAZHENDHI and K. BRINDHADEVI, *A systematic review on recent trends in transmission diagnosis prevention and imaging features of COVID-19*, Process Biochemistry **98**, pp. 233–240, 2020.

[3] N. BADOVINAC and D. SIMIC, *A Multimodal Biometric Authentication (MBA) in Card Payment Systems*, Proceedings of 2019 International Conference on Artificial Intelligence: Applications and Innovations, Belgrade, Serbia, pp. 23–26, 2019.

[4] Regulatory Technical Standards on strong customer authentication and secure communication under PSD2. Accessed: Mar. 10, 2023. [Online]. Available: https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/regulatory-technical-standards-on-strong-customer-authentication-and-secure-communication-under-psd2.

[5] F. LIEBANA-CABANILLAS, F. MUNOZ-LEIVA, S. MOLINILLO and E. HIGUERAS-CASTILLO, *Do biometric payment systems work during the COVID-19 pandemic?* Insights from the Spanish users' viewpoint, Financial Innovation **8**(1) paper 22, 2022.

[6] Biometrics to secure over $3 trillion in mobile payments by 2025. Accessed: Mar. 10, 2023. [Online] Available: https://www.juniperresearch.com/press/biometrics-to-secure-over-3-trillion-in-mobile.

[7] A. MODIBBO and Y. ALIYU, *Cashless society, financial inclusion and information security in Nigeria: the case for adoption of multifactor biometric authentication*, International Journal of Innovative Research in Science Engineering and Technology **4**(11), pp. 872–880, 2019.

[8] G. MERTENS, L. GERRITSEN, S. DUIJNDAM, S. SALEMINK and E. ENGELHARD, *Fear of the coronavirus (COVID-19)*: predictors in an online study conducted in March 2020. Journal of Anxiety Disorders **74**, paper 102258, 2020.

[9] V. BHARATHAN, *Digital dollar project in light of recent congressional hearings*, Forbes, Jun. 29, 2020. Accessed: Mar. 10, 2023. [Online]. Available: https://www.forbes.com/sites/vipinbharathan/2020/06/29/digital-dollar-project-in-light-of-recent-congressional-hearings.

[10] Commercial Biometric SDK software, Accessed: Mar. 10, 2023. [Online]. Available: https://ailia.jp/en/.

[11] L.-J. YIN, X.-C. CHEN, Y. SUN, T. WORM and M. REALE, *A high-resolution 3D dynamic facial expression database*, Proceedings of 8th International Conference on Automatic Face and Gesture Recognition, Amsterdam, Netherlands, pp. 1–6, 2008.

[12] N. CAVUS, Y. B. MOHAMMED, M. BULAMA and M. L. ISAH, *Examining user verification schemes, safety and secrecy issues affecting M-banking: Systematic literature review*, SAGE Open **13**(1), 2023.

[13] J. JAYANTHAN, N. K. PRIYA, S. P. KUMAR and K. SANGEETHA, *Facial recognition controlled smart banking*, IJRESM **4**(3), pp. 185–187, 2021.

[14] A. ZULFIQAR, M. SHAMIM HOSSAIN, M. GHULAM, I. ULLAH, H. ABACHI and A. ALAMRI, *Edge-centric multimodal authentication system using encrypted biometric templates*, Future Generation Computer Systems **85**, pp 76–87, 2018.

[15] K. A. SHAKIL, F. H. ZAREEN, M. ASLAM and S. JABIN, *BAMCloud: A cloud based mobile biometric authentication framework*, Multimedia Tools and Applications **220**, pp. 1–30, 2022.

[16] P. GAURANG and S. DEBASIS, *A novel approach to fingerprint biometric-based cryptographic key generation and its applications to storage security*, Computers & Electrical Engineering **69**, PP 461–478, 2018.

[17] A. THAPLIYAL, O. VERMA and A. KUMAR, *Multimodal behavioral biometric authentication in smartphones for Covid-19 pandemic*, International Journal of Electrical and Computer Engineering Systems **13**(9), 2022.

[18] B.-R. CHA, K.-J. KIM and H.-S. NA, *Random password generation of OTP system using changed location and angle of fingerprint features*, Proceedings of 8th IEEE International Conference on Computer and Information Technology, Sydney, NSW, Australia, pp. 1–6, 2008.

[19] K. P. KRISHNA and P. S. AITHAL, *A study on fingerprint hash code generation based on MD5 algorithm and Freeman chain code*, International Journal of Computational Research and Development **3**(1), pp. 13–22, 2018.

[20] Appendix for a scientific paper, Available: https://nenadbadovinac.com/appendix-rojist-2023.

[21] X. SHAN, L. YOU and G. HU, *Two efficient constructions for biometric-based signature in identity based setting using bilinear pairings*, IEEE Access **9**, pp. 25973–25983, 2021.

[22] A. O. HASSAN, A. A. ABDULHUSSEIN, M. S. DARWISH, Z. A. OTHMAN, S. TIUN and A. Y. LOTFY, *Towards a secure signature scheme based on multimodal biometric technology: Application for IoT blockchain network*, Symmetry **12**, paper 1699, 2020.

[23] K. TAKAHASHI, T. MATSUDA, T. MURAKAMI, G. HANAOKA and M. NISHIGAKI, *Signature schemes with a fuzzy private key*, International Journal of Information Security **18**, pp.581–617, 2019.

[24] Y. ZHANG, Y. HU, Y. GAN, Y. YIN and H. JIA, *Efficient fuzzy identity-based signature from lattices for identities in a small (or large) universe*, Journal of Information Security and Applications **47**, pp. 86–93, 2019.

[25] N. BADOVINAC and D. SIMIC, *Biometric creation of digital signatures and their application in blockchain*, in SymOrg 2022: Sustainable Business Management and Digital Transformation: Challenges and Opportunities in the Post-COVID Era, M. Mihic, S. Jednak and S. Savic, Eds., Springer, Cham, Lecture Notes in Networks and Systems **562**, pp. 3–13, 2023.

[26] G. L. KAYSER, R. NAMRATHA, J. RUPA and A. RAJB, *Water, sanitation, and hygiene: measuring gender equality and empowerment*, Bulletin of the World Health Organization **97**, pp. 438–440, 2019.

[27] M. I. P. NASUTION, N. NURBAITI, N. NURLAILA, T. I. F. RAHMA and K. KAMILAH, *Face recognition login authentication for digital payment solution at COVID-19 pandemic*, Proceedings of 3rd International Conference on Computer and Informatics Engineering, Yogyakarta, Indonesia, pp. 48–51, 2020.

[28] H.-J. JANG, J.-K. YOON, Y.-J. KIM and Y.-K. PARK. *Classification of iris colors and patterns in Koreans*, Healthcare Informatics Research **24**(3), pp. 227–235, 2018.

[29] D. BOBELDYK and A. ROSS, *Predicting eye color from near infrared iris images*, Proceedings of 2018 International Conference on Biometrics, Gold Coast, QLD, Australia, pp. 104–110, 2018.

[30] F. JAN, S. ALRASHED and N. MIN-ALLAH, *Iris segmentation for non-ideal iris biometric systems*, Multimedia Tools and Applications **220**, pp. 1–29, 2022.

[31] A. SAIF, M. S. HOSSAIN, K. T. HASAN and M. RAHMAN, *Measurement of unique pupillary distance using modified circle algorithm*, International Journal of Computer Applications **180**(9), pp. 1–5, 2018.

[32] R.-E. PRECUP, G. DUCA, S. TRAVIN and I. ZINICOVSCAIA, *Processing, neural network-based modelling of biomonitoring studies data and validation on Republic of Moldova data*, Proceedings of the Romanian Academy, Series A: Mathematics, Physics, Technical Sciences, Information Science **23**(4), pp. 403–410, 2022.

[33] T. BARBU, *Content-based image retrieval framework using multi-scale deeplearning-based feature extraction and graph-based clustering*, Proceedings of the Romanian Academy, Series A: Mathematics, Physics, Technical Sciences, Information Science **23**(3), pp. 289–298, 2022.

[34] Android POS machine with fingerprint, card readers, 2SIM and camera. Accessed: Mar. 10, 2023. [Online]. Available: https://www.globalsources.com/POS-kit/POS-1174917610p.htm.

[35] Y. MERSCH, An ECB digital currency – a flight of fancy, Speech at Consensus Virtual Conference, 2020. Accessed: Mar. 10, 2023. [Online]. Available: https://www.ecb.europa.eu/press/key/date/2020/html/ecb.sp200511 01209cb324.en.html.