Face Recognition Login Authentication for Digital Payment Solution at COVID-19 Pandemic

by Nurlaila Nurlaila

Submission date: 06-Jan-2022 11:38AM (UTC+0700)
Submission ID: 1737999113
File name: entication_for_Digital_Payment_Solution_at_COVID-19_Pandemic.pdf (288.13K)
Word count: 3420
Character count: 18408

Face Recognition Login Authentication for Digital Payment Solution at COVID-19 Pandemic

Muhammad Irwan Padli Nasution
Department of Information System
Universitas Islam Negeri Sumatera Utara Medan
Indonesia
irwannst@uinsu.ac.id

Nurbaiti Nurbaiti
Department of Management
Universitas Islam Negeri Sumatera Utara Medan
Indonesia
nurbaiti@uinsu.ac.id

Nurlaila Nurlaila
Department of Sharia Accounting
Universitas Islam Negeri Sumatera Utara Medan
Indonesia
nurlaila@uinsu.ac.id

Tri Inda Fadhila Rahma
Department of Sharia Banking
Universitas Islam Negeri Sumatera Utara Medan
Indonesia
triindafadhila@uinsu.ac.id

Kamilah Kamilah
Department of Accounting
Universitas Islam Negeri Sumatera Utara Medan
Indonesia
kamila@uinsu.ac.id

***Abstract*—On March 11, 2020 the World Health Organization has announced the status of global pandemic of corona virus disease 2019 or also called corona virus disease 2019 (COVID-19). The World Health Organization defines this disease as a pandemic because all citizens of the world are potentially exposed to COVID-19 infection. With the establishment of the global pandemic status, WHO also confirmed that COVID-19 was an international emergency. The trend of digitalization is becoming a new business trend to develop and survive in the midst of a crisis due to this pandemic. The online buying and selling market, digital payments and electronic health services, from online training classes to consulting with doctors via the internet, continue to increase. Some companies in the offline market also continue to operate by implementing health protocols. The form of digital payments continues increasing, this is because according to WHO the surface of objects can be a medium in the spread of the covid-19 virus. However, some digital payment media still require a card and enter a Personal Identification Number (PIN) in the Electronic Data Capture machine. For a solution so that the buyer does not need to bring a card and touch the Electronic Data Capture machine, face recognition authentication can be developed instead of PIN.**

Keywords— covid-19, digital payment, pin, face, security

I. INTRODUCTION

Coronavirus disease (COVID-19) is initially identified as a pneumonia virus in Wuhan, and it is named as SARS-CoV-2 by the World health organization (WHO) on 12th Jan 2020. The Corona virus pandemic has destroyed the world economy [1]. Almost all small and medium business turnover is affected by the Corona virus. Entrepreneurs and business people must be able to find new opportunities to survive in the midst of a crisis. For novice entrepreneurs who need to be ensured in business, cash availability. This money is used for capital and then changes the way of selling and marketing to get new customers. The new strategy is the basis for differentiating business entrepreneurs from other competitors. The capital that has been collected at this time is prioritized for rounds at the business growth stage. Not to shop that is not important, but more important to reduce spending in the midst of this pandemic crisis. The online buying and selling market, digital payments and electronic health services, from online training classes to consulting with doctors via the internet are likely to increase. Services on the offline market still occur despite a very significant decline. Some mini markets, supermarkets and malls continue to operate with special provisions. The payment instrument used in the offline market is cash, but many also accept non-cash using a credit card or debit card. Each card used, either a credit or debit card, is equipped with a PIN as a means of authorizing transactions. Personal Identification Number (PIN) is a numeric code that is commonly used in many electronic financial transactions, as of now it has been used as many as 6 digits. In accordance with Bank Indonesia Circular Letter no 16/25 / DKSP regarding 6-digit PINs, for increased security in the operation of payment instruments using cards, starting on July 1, 2020 all credit card transactions for purchases at merchants in Indonesia must use a PIN as a means of authorizing transactions [2]. The use of a PIN is safer than a signature, remembering that a PIN is a secret number only known to its owner. Card users cannot share their PIN with others. In addition, transactions using a PIN are encrypted and transactions are carried out in real time. If making a payment transaction with a credit card or other debit card, you will be asked to type the PIN on the EDC (Electronic Data Capture) machine. The EDC machine not only functions as a cash swipe tool, but you can also use the EDC machine for shopping payment transactions, payment of toll fees, payment of airline tickets and electricity. It can be concluded that if you use a card as a transaction in the offline market, you are asked to enter your PIN at every payment transaction [3].

Technological developments have made so many choices for conducting financial transactions. E-money is a non-cash payment instrument that uses electronic media, namely computer networks and the internet. The money value of the customer is stored in the electronic smartcard media. Thus, security and convenience aspects are very important factors in transacting using e-money. On electronic money has a stored-value or prepaid value in which a certain amount of money is stored in an electronic media owned by a person. The value of money stored in the form of stored balance on the chip e-money card will be reduced when the consumer uses it for payment. The balance can top up through a wide selection of scattered channels. For verification of identity data in a computer system is done using key, card, password, PIN and so on. However, this authentication has a shortcoming such as

easily forgotten (password, PIN), hacked, or can be changed by irresponsible people.

Viruses can enter the body through a number of methods, both directly and indirectly. Direct transmission can occur through close contact with people infected with the virus, direct contact with the blood or bodily fluids of people infected with the virus, or animal bites. While indirect transmission can occur through intermediary media, such as the surface of objects. The most important thing to know about coronavirus on the surface of objects is that it is easy to clean using normal household disinfectants that can kill the virus. Research has shown that the COVID-19 virus can last up to 72 hours on plastic and stainless steel, less than 4 hours on copper, and less than 24 hours on cardboard [1].

To avoid COVID-19 transmission to each card user consumer as a means of payment in the offline market, a new form of payment transaction tool can be developed. The development of face recognition as a PIN change is a solution that can be developed and is very supportive because there is no shaping of objects. Face recognition offers features that are far superior that is much faster, accurate, inexpensive and practical. The cost for face recognition is also cheaper because the device used is a camera.

II. FACE RECOGNITION SOLUTION

There are many privacy and security issues that are associated with the biometric technology. Development of face recognition as a PIN change is a solution that can be developed and is very supportive because there is no shaping of objects. The following are the security risk factors in the use of electronic money: (1). Theft. The simplest form of e-money crime is to steal another person's e-money card and then use the remaining funds. Theft can also be done by unscrupulous organizers of e-money, for example by charging funds illegally. Theft can also be done, for example by stealing a cryptographic key without the company's knowledge; (2). Duplication of devices. The risk of this crime is an attempt to duplicate the original card, so it can be used to make payment transactions like the original card. This type of crime is quite complicated and carried out by unscrupulous individuals with high levels of technical expertise. Because the offender must have different types of chips and operating system exactly the same as the original card; (3). Alteration or duplication of data / software This risk is a Crime Risk through attempts to change or modify data or applications contained on the original card, in such a way that the offender receives a financial gain. For example, adding e-money or changing the internal system of the application, so the calculation procedure is not working properly. Can also through 'physical attacks' against the chip itself; (4). Alteration of the message. This risk through the effort of change / intervention when the electronic data / message is sent, at the time of transaction. This potential risk is more likely to occur when e-money is used for internet payments; (5). Transaction denial (repudiation). Another misuse of e-money is the denial of transactions. The potential risk is an e-money-based software and uses message delivery when transactions over the internet network; (6). Malfunction. It risks can be corrupt or missing data, malfunctioning of the application or failure in message delivery. The risk of malfunction can be caused by physical or electronic disturbance of the instrument or due to interruptions in the transmission of messages between the transacting parties.

Thus, it is possible to develop techniques for the identification or verification of reliable and accurate use of biometric technology that utilizes special characteristics of the individual, such as face, iris, fingerprint, signature, etc. Biometrics is the branch of science that deals with the identification and verification of an individual based on the physiological and behavioral traits. The main uses of biometrics include the identification of individuals to be able to access certain facilities as well as various applications to overcome and prevent crime. Physiological biometric data deals with the physical aspects of a person's body, such as face print, fingerprints, hand lines, retinal scans, and DNA, is shown in Fig. 1 [1], [7].

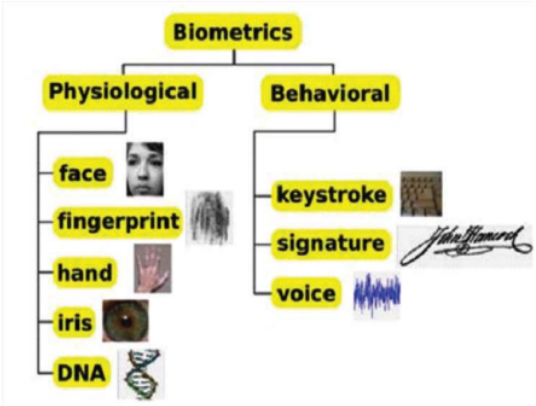

Fig. 1. Biometric Characteristic

If verification conditions, then biometric technology performs a singular comparison the data presented with the previously stored template. Every face has numerous, distinguishable landmarks, the different peaks and valleys that make up facial features [3], [4].

TABLE I. COMPARISON OF BIOMETRIC TAKING TECHNIQUE

Characteristic	Finger prints	Hand Geometry	Retina	Iris	Face	Signature	Voice
Ease of Use	High	High	Low	Medium	Medium	High	High
Error Incidence	Dryness ,dirt, age	Hand injury, age	Glasses	Lighting	Lighting, age, glasses, hair	Changing Signatures	Noise, colds
Accuracy	High	High	Very High	Very High	High	High	High
User Acceptance	Medium	Medium	Medium	Medium	Medium	High	High
Long-Term Stability	High	Medium	High	High	Medium	Medium	Medium

From various research results, is shown in Table I, that biometric data of face become an appropriate choice as authentication for the following reason: 1) Affordable, the cheapest cost, more economical because of its easy and inexpensive data recording device for face verification

requires a camera only, 2) Remote verification is possible, it only requires you to show your face in front of the camera and the scanner will do its work to unlock your device, 3) Ease of use, on most devices with a facial recognition feature, the face verification can take place seamlessly. It is fast, effortless and efficient. It has been a breakthrough in biometric authentication, 4) Uniquely, there is no possibility even though twins. Security, facial ID verification has a high acceptability rate than fingerprints. They are also universal in nature as every person has facial features but not everyone has fingerprints. Facial Recognition is fast and secure. It allows many businesses to verify their customers within seconds and can eliminate the threat of identity fraud. If using a face recognition, it is no longer necessary to remember the PIN and or multiple password because the security device is the body itself so it will be difficult to duplicate or stolen by people. Thus will facilitate the mobility of every person to make payment transactions anywhere without having to be bothered because they have to carry cards [4] - [7].

III. RESULT AND DISCUSSION

Biometric is the new technology which mostly used for person identification. Biometric systems can seem complicated, but they all use the same three steps is shown in Fig. 2 [3], [6], [7].

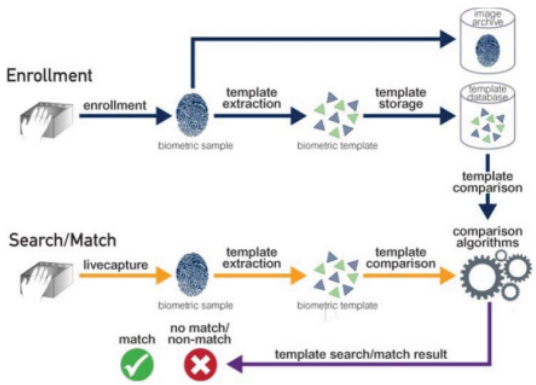

Fig. 2. Biometric System Processes

Step-1. Enrollment: The first time you use a biometric system, it records basic information about you, like your name or an identification number. It then captures an image or recording of your specific trait. Face identification is the method of identification based on the different patterns of human face, which is actually unique among each person. It is the most popular way of acquiring details of any person and is the easiest and convenient way of identifying a person. An advantage of face identification method is that the face pattern remains same for a person throughout his/her life, making it an infallible method of human identification [11], [12]. This process is done by using equipment that has sensors to retrieve data digitally such as a face reader, digital cameras and smartphones. Performance of biometric systems is dependent on the quality of the acquired input samples. If quality can be improved, either by sensor design, by user interface design, or by standards compliance, better performance can be realized. For those aspects of quality that cannot be designed-in, an ability to analyze the quality of a live sample is needed. So, selecting the right face reader is a very important step. The standard recommends that a template protection system should incorporate these privacy aspects [6].

Step-2. Storage: Contrary to what you may see in movies, most systems don't store the complete image or recording. They instead analyze your trait and translate it into a code or graph. Some systems also record this data onto a smart card that you carry with you. A face pattern is stored into the database because it is a solid and invariable template object [8], [10].

Step-3. Comparison: The next time you use the system it compares the trait you present to the information on file. Then, it either accepts or rejects that you are who you claim to be. This process is to identify and authentication or match the owner's original security device with the template stored in the database. The data with the owner and the database is authentic if both are the same.

The mechanism of payment transactions with e-money as can be explained in Fig. 3 [7], [9], [10], [12].

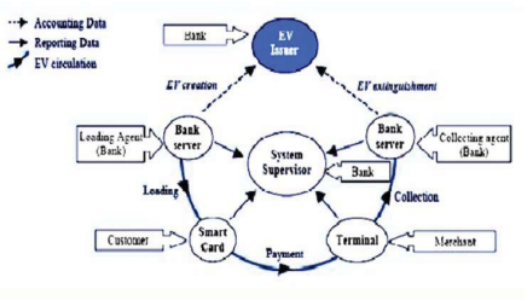

Fig. 3. E-money Transaction Using Cards

Subsystems that exist in payment transactions with e-money usually contain four functions, namely loading agent, user (customers), merchants and collecting agent. Loading and collecting agent is usually a bank. Loading agent converts from monetary value to another form into electronic monetary value on this electronic money system [13].

Collecting agents work the other way around, converting from money to electronic money systems to monetary value in other forms (e.g. banknotes). If using an e-money card, then the payment transaction is done by taking the value of money recorded digitally on the e-money card. However, if a faceprint is used instead of an e-money card, it is necessary for the party to store the biometric by digitally recording the value of money in the faceprint template, so that the payment mechanism of e-money with faceprint can be explained in Fig. 4 [14]. Authentication of payment transactions simply, only shows your face to a payment machine's camera.

Wallet is a customer account that stores the value of money in accordance with their own biometric face, so everyone will have different wallet. The process of payment transactions to the merchant occurs of course, when face authentication gives successful results that the faceprint read on the sensor in accordance with the owner. For top-up the money can be done by transfer to the wallet faceprint account of the consumer [15].

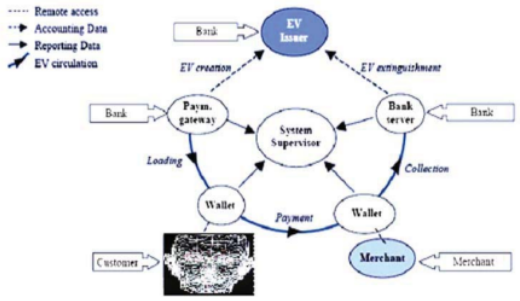

Fig. 4. E-money Transaction Using Face Recognition

IV. CONCLUSION

Biometric authentication systems using individual physiological and behavioral characteristics are very effective and efficient for use as automating access control and identity verification. The unique characteristics of the human body would be very difficult to fake. Therefore, security systems that use biometric technology will be difficult to break. In this way we can bond digital data to our identity with permanency, consistency, and unambiguity, and retrieve that data using computers in a rapid and automated fashion. Face recognition is the latest technology that allows us to identify or verify a person's face through a 3-dimensional digital image. If using biometric techniques, it is no longer necessary to remember the Personal Identification Number (PIN) and / or password because the security device is the body itself so it will facilitate the mobility of every person to make payment transactions anywhere without having to be bothered to bring e-money card and to avoid COVID-19 transmission to each card user consumer as a means of payment in the offline market because using face id requires no physical contact. In the future development, it will be necessary to add a security system to importance of biometric templates so that to avoid fraud and stolen.

REFERENCES

[1] Manigandan S., Wu M.-T., Ponnusamy V.K., Raghavendra V.B., Pugazhendhi A., Brindhadevi K, "A systematic review on recent trends in transmission, diagnosis, prevention and imaging features of COVID-19", (2020), Process Biochemistry, 98 , pp. 233-240.

[2] Bank Indonesia, "Banking System Payment," (2020), http://www.bi.go.id/id/peraturan/sistem-pembayaran last accessed 01-July-2020

[3] MIP, Nasution, Suendri, Samsudin, Zufria, I., Triase, Fakhriza, M., Ikhwan, A. "Biometrics for e-money transaction," (2018) AIP Conference Proceedings, 2030, art. no. 020301. https://aip.scitation.org/doi/abs/10.1063/1.5066942 ISBN: 978 073541752-6 https://doi.org/10.1063/1.5066942

[4] Tracy V.Wilson, "How Biometrics Works", (2017), retrieved from https://science.howstuffworks.com/biometrics.htm

[5] S. K. Choudhary and A. K. Naik, "Multimodal Biometric Authentication with Secured Templates — A Review," (2019), 3rd International Conference on Trends in Electronics and Informatics (ICOEI), Tirunelveli, India, 2019, pp. 1062-1069, doi: 10.1109/ICOEI.2019.8862563.

[6] S. Rane, "Standardization of Biometric Template Protection,"(2014), in IEEE MultiMedia, vol. 21, no. 4, pp. 94-99, Oct.-Dec.2014, doi: 10.1109/MMUL.2014.65.

[7] K. Nandakumar and A. K. Jain, (2015), "Biometric Template Protection: Bridging the performance gap between theory and practice," in IEEE Signal Processing Magazine, vol. 32, no. 5, pp. 88-115, Sept. 2015, doi: 10.1109/MSP.2015.2427849.

[8] Shaveta Dargan, Munish Kumar, "A comprehensive survey on the biometric recognition systems based on physiological and behavioral modalities", (2020), Expert Systems With Applications,143 (2020) 113114 Elsevier Ltd. All rights reserved. https://doi.org/10.1016/j.eswa.2019.113114

[9] Muhammad Irwan Padli Nasution., Andriana, S. D., Syafitri, P. D., Rahayu, E., & Lubis, M. R. (2016). Mobile device interfaces illiterate. In Proceedings of the 2015 International Conference on Technology, Informatics, Management, Engineering and Environment, TIME-E 2015. https://doi.org/10.1109/TIME-E.2015.7389758

[10] B. Yang and E. Martiri, "Using Honey Templates to Augment Hash Based Biometric Template Protection," (2015), IEEE 39th Annual Computer Software and Applications Conference, Taichung, 2015, pp. 312-316, doi: 10.1109/COMPSAC.2015.247.

[11] R. Tolosana, R. Vera-Rodriguez, J. Ortega-Garcia and J. Fierrez, "Increasing the robustness of biometric templates for dynamic signature biometric systems," (2015), International Carnahan Conference on Security Technology (ICCST), Taipei, 2015, pp. 229-234, doi: 10.1109/CCST.2015.7389687.

[12] A. Taralekar, G. Chouhan, R. Tangade and N. Shardoor, "One touch multi-banking transaction ATM system using biometric and GSM authentication," (2017), International Conference on Big Data, IoT and Data Science (BID), Pune, 2017, pp. 60-64, doi: 10.1109/BID.2017.8336574.

[13] A. Jain and S. Soni, "Visual cryptography and image processing based approach for secure transactions in banking sector," (2017), 2nd International Conference on Telecommunication and Networks (TEL-NET), Noida, 2017, pp. 1-5, doi: 10.1109/TEL-NET.2017.8343545.

[14] J. Galbally, S. Marcel and J. Fierrez, "Image Quality Assessment for Fake Biometric Detection: Application to Iris, Fingerprint, and Face Recognition," (2014), in IEEE Transactions on Image Processing, vol. 23, no. 2, pp. 710-724, Feb. 2014, doi: 10.1109/TIP.2013.2292332.

[15] R. Abdellaoui, M. Pasquet and O. Berthelier, "Integration of new electronic payment systems into B2C internet commerce," (2011), International Conference on Collaboration Technologies and Systems (CTS), Philadelphia, PA, 2011, pp. 484-491, doi: 10.1109/CTS.2011.5928727.

Face Recognition Login Authentication for Digital Payment Solution at COVID-19 Pandemic

ORIGINALITY REPORT

17%	14%	10%	13%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to SRM University Student Paper	1%
2	Submitted to University of Derby Student Paper	1%
3	Submitted to iGroup Student Paper	1%
4	www.bbc.co.uk Internet Source	1%
5	M. Muzaffar Hameed, Rodina Ahmad, Miss Laiha Mat Kiah, Ghulam Murtaza. "Machine learning-based offline signature verification systems: A systematic review", Signal Processing: Image Communication, 2021 Publication	1%
6	Submitted to Universitas Brawijaya Student Paper	1%
7	www.sciencepubco.com Internet Source	1%

8	Submitted to St John Paul II College Student Paper	1 %
9	repository.library.du.ac.bd:8080 Internet Source	1 %
10	www.xajzkjdx.cn Internet Source	1 %
11	ijircce.com Internet Source	1 %
12	web.archive.org Internet Source	1 %
13	Submitted to University of Greenwich Student Paper	1 %
14	Submitted to BITS, Pilani-Dubai Student Paper	1 %
15	Brandon Sieu, Marina Gavrilova. "Person Identification From Audio Aesthetic", IEEE Access, 2021 Publication	1 %
16	Submitted to Otago Polytechnic Student Paper	1 %
17	amtel.co.nz Internet Source	1 %
18	Tim Van hamme, Enrique Argones Rua, Davy Preuveneers, Wouter Joosen. "On the Security	1 %

of Biometrics and Fuzzy Commitment Cryptosystems: A Study on Gait Authentication", IEEE Transactions on Information Forensics and Security, 2021
Publication

19	Submitted to Higher Education Commission Pakistan Student Paper	<1 %
20	bhavanajagat.com Internet Source	<1 %
21	Marlene Elizabeth López-Jiménez, Víctor Rubén Virgilio-González, Raúl Aguilar-Figueroa, Carlos Daniel Virgilio-González. "Chapter 19 Touchless Fingerphoto Extraction Based on Deep Learning and Image Processing Algorithms; A Preview", Springer Science and Business Media LLC, 2021 Publication	<1 %
22	jurnal.iain-bone.ac.id Internet Source	<1 %
23	www.growkudos.com Internet Source	<1 %
24	www.hillagric.ac.in Internet Source	<1 %
25	j.mecs-press.net Internet Source	<1 %

26	www.scribd.com Internet Source	<1 %
27	assets.researchsquare.com Internet Source	<1 %
28	www.iaeme.com Internet Source	<1 %
29	Saadia Omer, Muhammad Bilal Sarwar, Muhammad Roman, Muhammad Usman et al. "Epidemiology, Clinico-Pathological Characteristics, and Comorbidities of SARS-CoV-2 infected Pakistani Patients", Cold Spring Harbor Laboratory, 2021 Publication	<1 %
30	repository.ihu.edu.gr Internet Source	<1 %
31	www.tandfonline.com Internet Source	<1 %
32	Marco Veranda, Susanna Cappello, Daniele Bonfiglio, Dominique Franck Escande, Artur Kryzhanovskyy. "Magnetic reconnection in three-dimensional quasi-helical pinches", Rendiconti Lincei. Scienze Fisiche e Naturali, 2020 Publication	<1 %

Exclude quotes	Off	Exclude matches	Off
Exclude bibliography	Off		