Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 245 (2024) 166–175

Procedia
Computer Science

www.elsevier.com/locate/procedia

9th International Conference on Computer Science and Computational Intelligence 2024 (ICCSCI 2024)

Face Recognition as Base Protocol in Online Transactions

Mohammad Fauzi Aziz[a], Gavin Sadiya Taraka[a], Sidharta Sidharta[a]*

[a] *ComputerScience Department, School of Computer Science, Bina Nusantara University, Jakarta 11480 Indonesia*

Abstract

From each to each year, from decades and decades, the fraud and scam are growing more and more powerful, although we cannot avoid it 100% since the fraud and scams using any method to make a crack of hole or other chances to steal that make a company and other e-commerce suffer losses in small or large numbers. This leads to new rules that can make e-commerce stand a chance and avoid the losses of either the e-commerce itself or the client that is trying to make online transactions. This paper has a goal to answer 5 research questions about face recognition as base protocol in online transaction. Method that we use is systematic literature review that has 7 steps from deciding research question until data synthesis. For the result from 5 research questions are answered very well, which is RQ1. How effective face recognition can decrease fraud identity on online transactions. RQ2. What kind of struggle and problem makes this technology unable to integrate with online payment. RQ3. What kind of perception and the acceptance of the user about the face recognition method for authentication in online transactions? RQ4. How far the technology is for face recognition can integrate with the system online payment transaction that increases the efficiency transaction with or without compromising security. RQ5. What kind of law of implication and etiquette from the user face recognition in online transactions and how can the system be made to follow the regulation that already exists. From that our conclusion is clear which is face recognition is safe and secure but since the technology is very well and good, then need proper technology to support it further.

Keywords: e-commerce; fraud; debit card; credit card; face recognition.

* Corresponding author. Tel.: +62-81332492299.
E-mail address: sidharta@binus.ac.id

10.1016/j.procs.2024.10.240

1. Introduction

Face recognition technology is rapidly becoming a fundamental aspect of securing digital transactions. It offers an advanced solution that surpasses the limitations of passwords and physical tokens. The face recognition method uses features on the human face that are different from one human to another, this makes the face recognition method more secure than another traditional authentication. But the face recognition method has various challenges, one of which is vulnerability to spoofing attacks that allow hackers to use photos or videos for the authentication process [1]. Another challenge is that different lighting conditions, facial changes due to age, and expressions have the potential to fail identification. To address these challenges, ensuring the performance of facial recognition for financial transactions is critical [1].

Allocating and storing data for face recognition requires very strict security so that it cannot be accessed by anyone who does not have access rights or other than users who are authorized for this responsibility. The protocols for the data collected are very strict and very important to prevent any activity that harms users who have entrusted their data to be stored as well as any misuse of personal data outside the applicable provisions. All forms of laws that can support security will be deployed and categorized as priorities that help security to be more secure and reliable. All related things must be able to help and balance each other to take advantage of opportunities and related technology to protect the data of an individual [2].

Although challenges are present in this regard, facial recognition technology in financial and security transactions has significant and reliable advantages. Technology can help improve or change the way that security against any form of fraud or deception can be improved and provide assurance to users. The related integration between technology developers, cybersecurity and other charts is helpful in realizing the main goals and benefits of full incorporation. The relationship between these things can increase the diversity of innovations in face recognition which makes it more secure. they can provide standards and rules to protect the privacy of users as a whole [3].

There is a possibility that the future of transaction security will change and rely on face recognition if it can be managed better and make it more effective than traditional methods. For all its technical limitations and data privacy concerns, face recognition is expected to provide a multidisciplinary approach that integrates insights from technology, law, and ethics. And of all forms, introducing continuous improvement and prioritizing ethics while incorporating face recognition into the system can achieve harmony with security and other matters [4]

2. Literature Review

2.1. Face Recognition System

Face Recognition System have many ways to understand about how Face Recognition can be work all along with any other source of technology or any method that can integrate with it. For our research we can give an example about how things work if we make a simple workflow about our face recognition.

On Fig.1 we can give an example of how face recognition works. From the camera view we can use it as a detector for person face and from that we can channel it or distribute it to the program or technology we use, then we can make it to have an answer or conclusion to choose whether it allow or not to get the access to the next option or any kind that we integrated with.

From some figure above we can understand of some steps have more than one decision and how complex it can be if we want to collaborate it onto something that might be on higher priority or higher risk that contain mass of activity or transaction at once, which is it will be more dangerous to be underestimated about how this process will work on other than that we simulated.

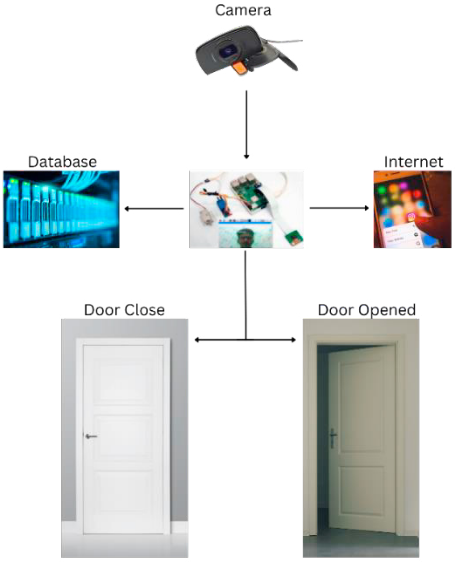

Fig. 1. Workflow of a facial recognition system related to authentication in online transactions.[1][2]

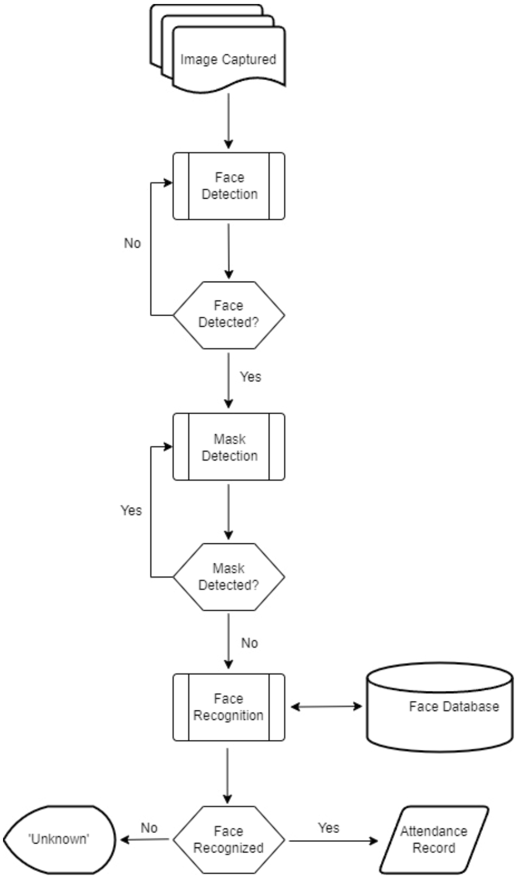

Fig. 2. Facial detection system workflow [3]

3. Method

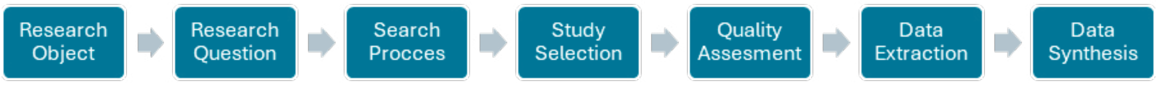

Fig. 3. Systematic literature review process

3.1. Research Object

The understanding about SLR (Systematic Literature Review) is a research method design to collect and assess studies related to a specific topic area, through a structured process of gathering and evaluation [5]. For the Research object we are trying to achieve is to decrease fraud and stealing identity in online transactions. Any reason why we choose this as one of our objectives are:

a. Preventing identity theft that happened a lot in our daily activities and make it more secure so there is no concern while making transaction.
b. To make it credible any transaction that is made can be trusted because the customer itself who made it on agreement by using face recognition to proceeding agreement in transaction.
c. Utilize this technology for supporting any other kind of method that has similar security, so it makes it more difficult to steal from any other user outside its own account.

3.2. Research Questions

On our method section, we are using the Comparison table that we made as base of our research and, we are using our RQ (Research Question) as a reason base of this research, in other reason we use this from common and recently event that happened in every country that has any criminal level even its high or low. Any question that we made after collect each source and review it, we found that 5 of our questions that has been made from any paper that we collect as a reference namely as follows:

a. RQ1. How effective face recognition can decrease fraud identity on online transactions other than traditional methods?
b. RQ2. What kind of struggle and problem makes this technology unable to integrate with online payment, and how is the best solution to handle the problem and find the solution?
c. RQ3. What kind of perception and the acceptance of the user about the face recognition method for authentication in online transactions?
d. RQ4. How far the technology for face recognition can integrate with the system online payment transaction that increases the efficiency of transaction with or without compromising security?
e. RQ5. What kind of law of implication and etiquette from the user face recognition in online transactions and how can the system be made to follow the regulation that already exists?

From the comparison table we found that many methods, advantages, and disadvantages on each paper contain face recognition and other useful information that is related to our research.

3.3. Search Process

To obtain the right data that we need, we access the database on Scopus to gather data that we need including other related papers that we could use to make it a more credible and stronger statement. Since the data that we need is the newest possible, we make it only a 5-year maximum date, so it's only contained from 2019 - 2023. We took the paper that was credible by only using journals and conferences, and free access to make it easier to filtrate and no expense from our team that can make us feel free to access the paper anytime. The data that we gather is from the title and the abstract that we have collected. From data we have collected, we use keywords such as “Face recognition”,” Face recognition protocol”,” Face recognition base protocol”, and” Transaction security”. Any reason why we use this keyword is to find and make it more filtrate between only related to make it match to our title. it more lot easier than only using one title or keyword on our paper and data search process rather than using more than one title.

3.4. Study Selection

In study selection we eliminate and use only related and same as our title. In other circumstances, the paper or data will be eliminated if it is not related or duplicated. Otherwise, any excluded paper that we have found will be considered if it matches with our systematic literature review, and all those requirements will be placed in exclusion criteria.

a. Inclusion criteria:
   - Article is Written on English language.
   - Article is ready to use in Scopus database.
   - Article is Open access.
   - Article is Have same Title as our research.
   - Article was published 2019-2023.

b. Exclusion criteria:
   - Article Only related but does not have the same title.
   - Article that using SLR (Systematic Literature Review)

3.5. Quality Assessment

Quality assessment in the context of a systematic literature review is a critical process to evaluate the validity, reliability, and relevance of the studies being reviewed in relation to the research topic. This is crucial to ensure that we only study relevant papers with the newest paper and maximum year that we use to make it easier and credible with the newest data and all data will be evaluate with question that support the paper with specific criteria:[5]

QA1. Did the paper only use 2019-2023?

QA2. Did the paper mention what technology is used, and any AI related deep learning and architecture?

QA3. Did the paper have the same database and be credible enough from the publisher for the database?

From all those papers we already check, we will give an answer as consideration to all relevancy data that we already gather and checked as Y (yes) and N(no).

QA1. Y (yes, all the paper we check and choose is filtered from 2019-2023)

QA2. Y (yes, the technology is provided by the paper is clear and related)

QA3. Y (yes, this paper we took from Scopus through Mendeley access)

3.6. Data Extraction

In the Data Extraction session, we already summarized to make it easier for us to access and filtrate. From such many data we collect, we can simplify data that is easy to collect or extract such as: Author name, Date published, Title, problem, method, solution, and data set. Any other data that is needed for high accuracy and detail, such as weakness of some AI, and Architecture, we will use it for further research in Data synthesis.

3.7. Data Synthesis

In Data Synthesis session, any kind of data that extracted will be taken and used to achieve in research, so it will be cleared and can be considered as proof that data is supporting this research. For the data that we gather, we can collect it from any research that has already been invented and can be collected from heterogenous research source [6]. For the Data synthesis we took valuable data that useful and collect it as summary on Tabel (excel) form. From that data we already collect, we will review it again and it will be making it easier while we check it one by one.

Because from that we know what paper we will use and relevant to our paper and not relevant. For the result that we will gain and collect in result and discussion, we will gather it from Research object, Research Question, Search process, Study selection, and Data extraction, which is going to be helping us on answering the research question that we are looking for.

4. Result and Discussion

4.1. Search Process Results

We only use the database on Scopus, which is the only database that we focus on, since IEEE needs to buy, and our focus is on open access only and free. Any support tools that we use is only the search navigation and any related tools in Scopus database, which is only searching the open-access article that stored on Scopus database itself. The article that we find is based on 2019 to 2023, any details for the paper we place it on inclusion and exclusion criteria, and the table that we use in Scopus search bar is described on Table 1.

Table 1. Keyword and paper information

Database	Keyword	Paper	Description
Scopus	Title:" Face recognition" OR Title:" Face recognition protocol" OR Title:" Face recognition base protocol" OR Title:" Transaction security"	50	Focused on journal and conference that published 2019-2023. which have open access type

4.2. Study Selection Results

In the study selection results we will find it on inclusion and exclusion criteria, which is from the inclusion and exclusion criteria. From that, we will only use the data on the limitation that describe in inclusion and exclusion criteria, further we review on the section 1 and section 2 we can make it simple on this table below.

Table 2. Table of criteria

No.	Inclusion Criteria	# of articles included
1	Written in English	50
2	Scopus database	50
3	Open access	50
4	Relate to research topic	0
5	Paper from 2019 - 2023	50
No.	Exclusion Criteria	# of articles included
1	Related paper	16
2	Article SLR	5

From the table of criteria, we only focus on what we need by limiting what we will search. More than that, we will eliminate it and search for other papers that related or have the same criteria from our paper.

4.3. Quality Assessment Result

On this section, we will crosscheck all the paper that we found and review and read it 1 by 1. Our paper will meet the Quality assessment question that we made and prepare, so it will make it easier to read and find the data that we need from each paper that we collected. Any Quality assessment questions that we made are QA1, QA2, and QA3. Which of those 3 types of that question will be represent of our filter to make the paper more focus on what we will use on. And from all the papers we collect, all the paper are correct, related, and filtered as we need and follow our need and limitation rule. For the total paper that match on our criteria is 50 papers from 50 paper that we collect, and all those papers was passed our review and no difficulties when we review any related paper.

4.4. Data Extraction Result

For the data extraction result, we only extract from the criteria on section 2.D, and section 3.B. which is all the criteria that has been found, and all data that relevant source that we gather from both section that we already got, we will use it and compare any similar data that we need for the systematic literature review (SLR) research that we trying to make, which those data will we use only for research purpose and only to make newest knowledge that have the conclusion between old and the newest data.

Table 3. Data extraction

No	Reference	Method	Information
1	[7]	Face Recognition with CCTV	Integrate Face Recognition with Fingerprint for better security
2	[8]	The main module to obtain output using a real-time input stream from the camera	This module uses cv2 and NumPy to manipulate image pixel arrays. This module compares trained images with real-time images using the LBPH algorithm to make predictions. If the face is recognized, an OTP is sent for additional verification before completing the transaction.
3	[9]	Face Recognition with CCTV	Utilize CCTV for monitoring and confirm user for using ATM
4	[10]	Face Recognition with Machine Learning	Using algorithm VGG16 or other for enchanting the accuracy on Face Recognition
5	[11]	Face Recognition and OTP	Utilize OTP for an additional layer of security in authenticating online transactions

4.5. Data Synthesis Result

The data synthesis result is where we will be answering all our research questions on this paper, which is any related data that exist on this paper, is from the reference paper that we got.

RQ1. How effective face recognition can decrease fraud identity on online transactions other than traditional methods?

Face recognition technology can enhance the security of online transactions beyond traditional methods! It offers a robust alternative to conventional PIN and password authentication systems. These systems are susceptible to phishing attacks and security breaches. Face recognition technology compares a user's face with a pre-stored database to verify their identity! This ensures that only authorized users can conduct transactions, significantly reducing the risk of fraud associated with stolen or guessed PINs. The use of biometric data provides a more secure and user-friendly alternative to traditional passwords, as it is inherently more difficult to replicate or steal [9].

The integration of advanced facial recognition algorithms in banking and e-commerce platforms makes the authentication process easier and more secure against identity fraud in online transactions. The articles 'Securing ATM Transactions using Face Recognition' and 'Online Transaction Security Using Face Recognition' cover this topic. A Review: I wanted to share with you how this amazing technology can help mitigate the prevalent issue of unauthorized access through stolen credentials. It offers a seamless yet secure method for verifying user identity. Hey there! The advancement in facial recognition technology presents a formidable barrier against unauthorized access, ensuring a higher level of transactional security [8].

RQ2. What kind of struggle and problem makes this technology unable to integrate with online payment, and how is the best solution to handle the problem and find the solution?

The rise in security threats to Automated Teller Machines (ATMs), such as skimming, PIN logging, and integrity violations, highlights the shortcomings of traditional PIN-based security systems. This critical need for more robust protective measures must be addressed with urgency. It discusses the integration of biometric authentication, specifically fingerprint and facial recognition, to increase security and reduce fraud. The article entitled 'Cardless ATM Transactions using Biometrics and Facial Recognition – An Overview' emphasizes the need for improved security policies and technological advances to address the risk of data misuse and privacy concerns [7]. The paper highlights the technological and regulatory challenges associated with implementing such systems. The article 'Online Transaction Security Using Face Recognition: A Review' confidently discusses the vulnerabilities of online transactions to fraud, such as account takeover and merchant collusion. It proposes facial recognition technology as a solution to enhance transaction security and mitigate attack risks. The article emphasizes the importance of supporting face recognition with other security measures, such as OTP verification, to combat unauthorized access and identity theft effectively [8]. Moreover, 'IDENTI~1.PDF' implicitly addresses the same themes of augmenting security in financial transactions via cutting-edge biometric techniques like facial recognition. The document underscores the intricacies of integration, privacy concerns, and the necessity of supplementary security measures to guarantee all-encompassing protection in financial transactions. The trend towards incorporating advanced technologies into financial security systems to address emerging security challenges is clearly demonstrated by these discussions.

RQ3. What kind of perception and the acceptance of the user about the face recognition method for authentication in online transactions?

Facial recognition technology has provided advantages in authenticating online transactions, especially in terms of security and convenience. Users consider this method safer because it reduces the risk of automated attacks and unauthorized access [11]. Additionally, facial recognition also offers convenience, as users do not need to remember complex passwords or use physical tokens [11]. Nonetheless, privacy concerns are in the spotlight as users worry about the storage and use of their biometric data [12]. System accuracy and reliability are also a consideration, as errors in recognizing faces or false negative results can reduce user confidence [12].

To overcome this problem, several studies recommend a multifactor authentication approach. This approach combines facial recognition with other authentication methods, such as fingerprints or OTP, to add a layer of security and increase user trust [11]. In addition, the use of algorithms such as Faster R-CNN and LIME can improve facial recognition accuracy and provide better reliability [12]. Models that have a high level of accuracy and perform well in a variety of environments can increase user acceptance of this technology [12]. Consistency in results and the ability to adapt to changing conditions are also important factors in building user trust [12].

To increase user acceptance, transparency in the process and strong security measures are essential [11]. Facial recognition technology can be an effective tool in online transactions, but it must be balanced with appropriate privacy protection [12]. Additionally, system reliability and accuracy are critical to ensuring user acceptance [11]. With a multifactor approach that combines various security techniques, facial recognition technology has the potential to become a safe and convenient authentication method in online transactions [12].

RQ4. How far the technology is for face recognition can integrate with the system online payment transaction that increases the efficiency transaction with or without compromising security?

Face Technology can be integrated with online payment systems to increase efficiency without compromising security [13]. provides a fast and secure way to complete transactions without using a card or additional account information, various with biometric approaches such as face and fingerprint. This reduces the risk of card theft and PIN-related fraud. In addition, a fingerprint detection system with a mask detection algorithm [14] ensures fingerprints remain accurate even when the user is wearing a mask, thereby increasing security during payment transactions. Improving image quality also helps improve facial expression performance, which is important for more efficient and polite transactions [15].

Other systems that use facial recognition with an attention mechanism can improve accuracy even when parts of the face are covered by a mask [16]. This technology can be adapted into online payment systems, especially in the context of a pandemic. Integration with the Internet of Things (IoT) and office automation using facial recognition [14] shows the potential use of facial recognition in various scenarios, including payment transactions. Additionally, an explainable AI-based facial recognition system [14] provides additional transparency and security in the context of payments. With the combination of these technologies, online payment transaction systems can become more efficient, safe, and reliable, also reducing the risk of fraud and increasing transaction security.

RQ5. What kind of law of implication and etiquette from the user face recognition in online transactions and how can the system be made to follow the regulation that already exists?

Security, this technology is considered safer than technology that uses password methods for security because of its ability to reduce the risk of automatic attacks and invalid access [8]. This occurs accompanied by additional security such as OTP (One Time Password), providing a better level of security in banking transactions [8]. This technology is also convenient for users, there is no need to remember complex passwords or use physical tokens, so it is faster and more efficient [10].

Therefore, the use of facial recognition technology is not without problems. However, privacy is becoming a major topic in security, as users express concerns about the storage and use of their biometric data [7]. In addition, the level of accuracy of this system can influence the level of user trust and acceptance. If the system often experiences problems in recognizing faces or provides negative results, this can reduce user trust in the system [9]. In addition, the cost of implementing this technology can be a determining factor in adoption in areas with limited technological infrastructure [8].

To increase user acceptance, several studies recommend a multifactor authentication approach. Combining facial recognition with other authentication methods, such as fingerprint, OTP, or reverse OTP, can increase user trust by providing an additional layer of security [7]. In addition, the integration of advanced algorithms such as VGG16 and Local Binary Pattern Histogram (LBPH) can improve accuracy thereby increasing user confidence [10][7]. Ultimately, a transparent approach and strong security measures are key to gaining user trust and acceptance in the application of facial recognition technology for online transactions.

Table 4. Security method

No	Tittle	Method	Details Information
1	Online Banking Security with Real Time Face Recognition Approach	Facial Recognition and OTP	Usage of OTP for an additional layer on security in authenticating online transactions
2	Face Recognition Based Banking System Using Machine Learning	Facial Recognition with Machine Learning	Using algorithms such as VGG16 to increase accuracy in facial recognition
3	Card-Less ATM Transaction Using Biometric and Face Recognition – A Review	Facial and Fingerprint Recognition	Combines facial recognition with fingerprints for better security
4	Securing ATM Transactions by using Face Recognition	Facial Recognition with CCTV	Utilizing CCTV to monitor and confirm the user's face at the ATM

5. Result and Discussion

Online payments using face recognition can be done effectively. Systems like BioPay enable safe, more trusted, and fast payments without the need for physical cards or additional identity data by utilizing biometrics, such as fingerprints and facial recognition. This can reduce the rate of card theft and fraud using PINs. Even if the user wears a mask, the accuracy and security of the transaction is maintained by technology that combines facial recognition with mask detection. In addition, a more competent and user-friendly transaction process is possible with the use of this technology.

Face recognition technology has some problems because, it is gullible and does not work well when lighting conditions are different, ages are different, or expressions are different. To keep the system maintained and safe, new technology is needed, to keep people safe from fake access and identity theft, facial recognition technology also needs to be equipped with other security measures such as OTP verification. Facial recognition technology can help

References

[1] Woodward, J. D., Orlans, N. M., & Higgins, P. T. (2003). Biometrics. McGraw-Hill/Osborne.

[2] Jain, A. K., Ross, A., & Prabhakar, S. (2004). An introduction to biometric recognition. IEEE Transactions on Circuits and Systems for Video Technology, 14(1), 4-20.

[3] Li, S. Z., & Jain, A. K. (Eds.). (2011). Handbook of face recognition. Springer.

[4] Zhao, W., Chellappa, R., Phillips, P. J., & Rosenfeld, A. (2003). Face recognition: A literature survey. ACM Computing Surveys (CSUR), 35(4), 399-458.

[5] Triandini, E., Jayanatha, S., Indrawan, A., Putra, G. W., & Iswara, B. (2019). Metode Systematic Literature Review untuk Identifikasi Platform dan Metode Pengembangan Sistem Informasi di Indonesia. *Indonesian Journal of Information Systems*, *1*(2), 63.

[6] Brown, D., Van Den Bergh, I., De Bruin, S., Machida, L., & Van Etten, J. (2020). Data synthesis for crop variety evaluation. A review. Agronomy for Sustainable Development (Online), 40(4). https://doi.org/10.1007/s13593-020-00630-7

[7] Manish C. M., Chirag, N., Praveen H. R., Darshan M. J., & Kasim Vali, D. (2020). Card-Less ATM Transaction using Biometric and Face Recognition– A Review. International Journal for Research in Applied Science & Engineering Technology (IJRASET), 8(VII), 1493-1498. https://doi.org/10.22214/ijraset.2020.30444

[8] Karale, A., Tiwari, A., Wadkar, A., Patil, A., & Waghulde, D. (2022). Online Transaction Security Using Face Recognition: A Review. International Journal for Research in Applied Science & Engineering Technology (IJRASET), 10(6). https://doi.org/10.22214/ijraset.2022.44214

[9] Murugesan, M., Santhosh, M., Sasi Kumar, T., Sasiwarman, M., & Valanarasu, I. (2020). Securing ATM Transactions using Face Recognition. International Journal of Advanced Trends in Computer Science and Engineering, 9(2), 1295–1299. https://doi.org/10.30534/ijatcse/2020/59922020

[10] Mohanraj, K. C., Ramya, S., & Sandhiya, R. (2022). Face recognition-based banking system using machine learning. International Journal of Health Sciences, 6(S8), 468–477. https://doi.org/10.53730/ijhs.v6nS8.9724

[11] Rajeshkumar, G., Braveen, M., Venkatesh, R., Josephin Shermila, P., Ganesh Prabu, B., Veerasamy, B., Bharathi, B., & Jeyam, A. (2023). Smart office automation via faster R-CNN based face recognition and internet of things. Measurement: Sensors, 27, 100719. https://doi.org/10.1016/j.measen.2023.100719

[12] Rajpal, A., Sehra, K., Bagri, R., & Sikka, P. (2023). XAI-FR: Explainable AI-Based Face Recognition Using Deep Neural Networks. Wireless Personal Communications, 129, 663–680. https://doi.org/10.1007/s11277-022-10127-z

[13] Singh, G., Kaushik, D., Handa, H., Kaur, G., Chawla, S. K., & Elngar, A. A. (2021). BioPay: A Secure Payment Gateway through Biometrics. Journal of Cybersecurity and Information Management, 7(2), 65-76.

[14] Md Suhaimin, M. S., Ahmad Hijazi, M. H., Kheau, C. S., & Kim On, C. (2021). Real-time mask detection and face recognition using eigenfaces and local binary pattern histogram for attendance system. Bulletin of Electrical Engineering and Informatics, 10(2), 1105–1113. https://doi.org/10.11591/eei.v10i2.2859

[15] Zeng, J., Qiu, X., & Shi, S. (2021). Image processing effects on the deep face recognition system. Mathematical Biosciences and Engineering, 18(2), 1187–1200. https://doi.org/10.3934/mbe.2021064

[16] Wang, Y., Li, Y., & Zou, H. (2023). Masked Face Recognition System Based on Attention Mechanism. Information, 14(2), 87. https://doi.org/10.3390/info14020087