Advances in Social Science, Education and Humanities Research, volume 451
Proceedings of the 2020 5th International Conference on Humanities Science and Society Development (ICHSSD 2020)

Research on the Application of Face Recognition System

Chen Mingtsung [1, *], Lu Cai [2]

[1]*Department of Public Administration, Nan fang College of Sun Yat-sen University, Guangzhou, Guangdong, 510000, China*
[2]*Department of Public Administration, Nan fang College of Sun Yat-sen University, Guangzhou, Guangdong, 510000, China*
[*]*Corresponding author's e-mail: 306470714@qq.com*

ABSTRACT
For the unrestricted investment of face recognition technology, whether it is to protect the safety of people's life and property or to infringe on people's basic rights. Face recognition is the most typical one of pattern recognition. It extracts the feature information of face in different ways, compares or tests the collected information with the original information, to realise the record verification of identity or the tracking and positioning of personnel. Nowadays, face recognition technology has been widely used in everyone's daily life. On the one hand, it brings great convenience to life, on the other hand, whether personal information security and privacy can be guaranteed. Everything has two sides, and face recognition technology is no exception. How to balance the advantages and disadvantages of privacy and security still needs to be further explored?
Keywords: *face recognition; network security law; personal information; privacy; artificial intelligence*

1. PREFACE

In recent years, the rapid development of artificial intelligence, derived from various applications are numerous. Among them, face recognition, with the convenience of face brushing, has gradually become a fashion for new face brushing applications, such as face brushing check-in, face brushing shopping, etc. it can be said that face recognition technology is rapidly promoting application to various industries in the society. Face recognition also has a wide range of applications in life, such as using face tracking to locate missing or fugitive people, using face verification recognition to verify the identity of people and so on. In theory, people should be protected, but in such measures, people are the objects of prevention and control. Living in this society, people will feel distrusted. Subway will use face recognition technology to carry out classified security check for passengers because it can improve the traffic efficiency of passengers. As soon as the iPhone x, which attracts people's attention all over the world, has attracted people's attention with its unique face unlocking and wireless charging and other new technologies. It also makes the application of face recognition more deeply into our life and raises a discussion upsurge of face recognition technology and its application. Face recognition is a technology based on human facial features to detect whether there is a face in an image or video stream. If there is a face, it can further detect its location, size and the location of various facial organs, and can automatically track and identify. At present, with the rapid development of face recognition technology in the past few years, it has almost reached the level of keeping pace with fingerprint recognition and other recognition technologies. It has gradually replaced fingerprint recognition in some mobile phones, attendance and other fields, becoming a new way of identity recognition.

2. OVERVIEW OF FACE RECOGNITION TECHNOLOGY

2.1. Features

2.1.1. non-mandatory

The first feature of face recognition technology is that it is non-mandatory. Palm vein Palm vein recognition, iris recognition, retina recognition and other recognition technologies require the tested person to consciously cooperate with the instrument and equipment to collect relevant feature information. After these special collection methods are detected by the tested person, the person with ulterior motives will use the corresponding methods to camouflage and cheat. However, face recognition is different. Face recognition system can automatically collect and analyse face images in the unconscious state of the recognition object. The non-mandatory feature is very important for a recognition method, which will make the recognition method not offensive, and it is not easy to be prevented and cracked because it is not easy to attract people's attention. To some extent, this makes face recognition easier to achieve than other mandatory recognition such as fingerprint recognition.

2.1.2. concurrency

Another feature of face features recognition technology is concurrency. Through the camera and other image or video acquisition equipment, it can quickly and simultaneously acquire and identify multiple faces contained in one frame of an image or video, which has incomparable advantages for fingerprint, palm print and other identification technologies. For example, in many crowded places such as railway stations, stadiums, airport entrances and exits, through the monitoring system to identify and process the face images of multiple people in the acquisition screen, without affecting the efficiency and speed of personnel access, it has strong practicability to identify and confirm the identity of the tested person in time.

2.1.3. non-contact

Face recognition technology also has the characteristics of non-contact. At present, the widely used fingerprint identification is to use an electronic pressure sensor to collect fingerprint for identification and comparison. For hospitals and other health environment sensitive places, the contact identification system is not conducive to prevent the spread of disease. Although palm print, retina and other recognition methods do not need to contact the subject substantially, the acquisition distance is relatively close, and the subject also needs to cooperate with the acquisition. Face recognition system does not need any contact with the recognition object from collecting face information to completing identity recognition, and it can normally work even when it is far away.

2.2. Application

2.2.1. face tracking

Face tracking is mainly used to find relatives of missing persons or track suspects at large. With the development of 3D face recognition system and algorithm, the negative face recognition has been greatly improved. The photos of the lost children or suspects are input into the system. Then, in a large number of surveillance video data, the dynamic image information is extracted, the most matching face information is locked and tracked.

2.2.2. face retrieval

This technology is widely used in company and school's punch in and sign in. The application needs to input the face information of the staff in the system first. At the time of check-in, it only needs to be close to the image collection equipment, and then the face information of the check-in personnel will be collected and compared with the data in the information database. If the matching is successful, the clock in will be successful. This technology is simple and fast, needs the cooperation of people is low, and the recognition of static image is good, so it is widely used in this field.

2.2.3. face verification

This technology is mainly used in customs stations and other places to verify personnel information. When the detected person is close to the acquisition equipment, the face recognition system collects the face information in real-time. It compares it with the ID card and other original information in the database, which can detect the authenticity of the identity information of the verified person.

2.3. Disputes

The rapid development of face recognition technology has caused the public to think deeply about personal information security. With the rapid development and popularisation of its commercial colour, we need to reexamine the choice between personal privacy and personal privacy. But it can not be ignored that, in law, face recognition technology and privacy issues have a certain degree of antagonism. Article 41 of the network security law of the people's Republic of China, which came into effect in 2017, stipulates that "when network operators collect and use personal information, they shall follow the principles of legality, legitimacy and necessity, publicly collect and use the rules, clearly indicate the purpose, method and scope of collecting and using the information and obtain the consent of the collectors. Network operators shall not collect personal information irrelevant to the services they provide, collect and use personal information in violation of the provisions of laws and administrative regulations and the agreements of both parties, and shall process the personal information they keep by the provisions of laws and administrative regulations and the agreements with users. Compared with fingerprint recognition, the whole operation process of face recognition has certain concealment, which can be realised without the cooperation of the identified person without the prior consent of the parties. The students in the class may have been caught all the class state and facial expression by the face recognition system without knowing it and used to analyse the class concentration, listen carefully and so on. These unauthorised personal information analysis data are likely to infringe on the personal privacy of students and even affect personal safety. Between the subject of recognition and the public, information mastery is asymmetric. It makes use of its greater advantages in information collection and application and arbitrarily uses face recognition technology to capture the facial features of citizens in public places to achieve its purpose. It is difficult to

protect the behaviour, which does not constitute an infringement of citizens' privacy and public social rights.

3. DEBATE ON FACE RECOGNITION TECHNOLOGY

The widespread application of face recognition system has gradually aroused doubts about its security and privacy protection from all walks of life. In September 2017, an article in the British business journal the economist said: "human faces are open, but computers with the ability to record, store and analyse face images in a low cost, fast and large amount will eventually lead to people's concealment of individuals The concepts of privacy, fairness and trust have changed. " It can be seen that with the accelerating process of big data openness, the big data system and public surveillance system of face recognition will face the risk of being abused or monopolised by individuals or organisations, resulting in the public's concern about personal privacy and security under the supervision of public surveillance system, which leads to the debate between the pros and cons.

3.1. In favor

To improve community security and increase "additional security" in a wide range of media debates, the main point of view of supporters is: this system can provide the social public with extremely strong security and minimum privacy loss, and any privacy loss can be offset by huge security interests. As an accurate and effective monitoring system, its wide application will be reduced Crime, the important means to improve the safety of the community and the quality of people's life. At the same time, this system can bring the social public an irreplaceable "additional sense of security". The ubiquitous public surveillance system provides the public with far more comprehensive security than manual monitoring means. Also, some supporters pointed out another social value of the system, namely, the location of missing persons, suspects at large and floating population. On the issue of privacy, the supporters of the system hold different attitudes. Some of them deny the existence of privacy or weaken the threat of technology to privacy fundamentally, while others admit that it is a potential problem. However, those who realise that the public surveillance system will have a significant negative impact on personal privacy come to the conclusion of the system based on its benefit trade-off analysis The security benefit is greater than the loss of privacy and freedom, so we still choose to support this system.

3.2. Objection

First of all, face recognition involves the collection of biological data important to individuals. Before collection, relevant organisations or institutions must prove the legitimacy of this approach. According to existing laws and regulations, ordinary personal information, including address, telephone number, email, account and trace, must be collected with the prior consent of the person to be collected because of its recognisable. At the same time, if the collecting party improperly uses, sells or divulges the corresponding information, it may also cause legal liability, including criminal liability. The personal direction of biological data is more clear and for individuals, it is more important than the general personal information. Why the consent of the collected person is not required when collecting biological data. Also, there is no restriction on the subject, purpose, method, scope and procedure of collection, and there is no corresponding legal liability for the illegal collection or use. If the government is the main body of the collection, it needs to be explicitly authorised by law; if the law is not authorised, it cannot be done, and the government has no right to collect biometric data of ordinary citizens in the name of security. If it is done by enterprises or other institutions, the collection of biological data of individuals requires at least the express consent of the person being collected; collection without consent is an illegal act of obtaining personal information of citizens.

Secondly, taking face recognition in the subway as an example, because it involves the important personal rights and interests of the public, it needs to be implemented without hearing, and it lacks the least rationality. A few years ago, Beijing subway fare adjustment, had widely sought the public opinion, and through strict hearing procedures. If the adjustment of ticket price requires extensive consultation and hearing procedure, how can we directly decide to implement the face recognition technology, which involves more important personal rights and interests without consultation or hearing? Is personal biological data not as important as several yuan RMB? Without any proof, people are ready to rush into large-scale face recognition, and there is reason to doubt whether it involves illegal interest transactions, or whether it is the result of lobbying by relevant interest groups.

Thirdly, it claims that the application of face recognition technology is to achieve classification security, but the problems involved in the standard itself have not been solved. What power does a traffic management department have to classify passengers? What law is it based on? More than that, what kind of standards are relevant departments going to adopt to classify passengers, what contents are included in the standards, who are the people and how to determine the standards, and whether the standards should be made public? Shouldn't these problems be solved before the implementation of face recognition? The classification standards of garbage should be made clear, not to mention the classification of people. If relevant departments intend to adopt internal standards, how can we know whether the standards are legal and reasonable? How to know whether there is discrimination prohibited by law? How to know if there is any problem of setting standard content at will? If the interested parties do not agree with the classification standards or think that improper classification infringes

their legitimate rights and interests, how should they appeal and how can they ensure that their rights are effectively remedied? Before these problems are solved, how can we make such a rash decision to use face recognition for classification and security inspection on a large scale in places like subway? If we arbitrarily adopt internal standards to classify passengers and take different security measures accordingly, we have reason to suspect that such practices violate the principle of equality in the Constitution and the fundamental right of citizens to inviolability of their freedom. Article 37 of the Constitution stipulates that it is prohibited to illegally detain, illegally deprive or restrict citizens' freedom by other means, and illegally search citizens' bodies.

Finally, there is not enough evidence to show that face recognition can improve the traffic efficiency in the subway; even if there is evidence to prove, the efficiency itself is not enough to become the full basis for implementation. Officials at the rail transit command said that the implementation of human identification technology in the subway is to improve the traffic efficiency during the period of large passenger flow. The problem is that claims do not represent objective facts. Before doing solid empirical research, how can we believe that the application of this technology in the subway will help improve traffic efficiency? Based on my experience at the airport and in the hotel, it's hard for me to believe this conclusion. Even with some support from experts, we have reason to doubt the accuracy of their judgment. Because this involves the prediction and evaluation of the unknown situation, the expert's judgment is likely to fall into error. For example, in many years before the opening of the second child policy, many population experts have made it clear that the full opening of the second child policy will lead to a sharp increase in China's population. Since the opening of the second child, what is the actual fertility rate, it is obvious to all. To take a step back, even if face recognition can improve efficiency, the efficiency itself is not enough to become the full basis for implementation. Don't fool the public in the name of efficiency. In terms of efficiency, not carrying out the so-called security check on the subway can best improve efficiency during the period of large passenger flow. The current personnel inspection, especially the personnel inspection among them, is nothing in the peak period or the general period. In addition to the waste of taxpayer's tax, we really can't see the practical role and significance of such a personal inspection.

Based on the above-mentioned corresponding reasons, especially considering the potential risks and negative effects, I am not only opposed to the use of face recognition technology in the subway, but also opposed to forcing people to accept face recognition inspection in airports and hotels and other occasions. Commercial organisations lure people into using face recognition voluntarily with small profits or convenient and safe factors. Because most of the information is not fully informed, it is difficult to establish effective user consent, so its use is also difficult to be legal. In modern criminal procedure law, the principle of presumption of innocence is generally applied. According to this principle, anyone is presumed innocent in law until he is found guilty by the court. However, the current security measures are all based on the presumption of guilt. Everyone is presumed to be at risk to public safety and needs to undergo increasingly stringent security checks without exception.

4. RISK ON FACE RECOGNITION SYSTEM

A public place is the most popular and controversial place of the face recognition system. How to balance the advantages and disadvantages of privacy and security still needs to be further discussed? At present, the face recognition system in public places mainly faces the following three problems:

4.1. Technical error

The immaturity of face recognition technology will lead to a certain probability of wrong matching, which may cause innocent citizens to be harassed by the police or building residents can not normally pass through the access control. This problem is not caused by the repetition of human faces. The error of personal information collected in the database, the improper operation of system users, and the estimation and matching based on a certain probability may result in the error of system matching. When discussing with more profound privacy issues, the technical error of technology itself is not enough to be a theoretical point against the use of this system. However, it does show that the system used for identity recognition has a high requirement for fault tolerance, and the potential negative benefits caused by the inaccuracy of the system itself are difficult to evaluate.

4.2. Functional latent change

Functional latent change is a kind of phenomenon that a specific technology designed to achieve a limited purpose may obtain additional and unexpected purposes or functions. The expansion of the application field of technology or the abuse of technology may lead to the occurrence of latent functional change. Face recognition technology has high flexibility, so its application field is very easy to expand from the original recognition and location tracking function to other aspects and the function potential change of face recognition technology is also very easy to achieve. The expansion of identity information database, the expansion of function application purpose and the replacement of users of face recognition system will lead to the phenomenon of a potential change of its function Life. The original design purpose of face recognition technology is to apply it to criminal information management of public security department for criminals and accurate tracking of fugitive

suspects. However, with the improvement of big data technology and data publicity, the originally relatively independent centralised face recognition system has gradually evolved into an interconnected distributed system, which can integrate Under the control of the system, at least relying on the centralised hardware facilities, users can cooperate to perform a dynamic task so that users can achieve some other purposes that were not expected at the beginning of the technical design through the system and the application of the technology for other purposes will also cause unexpected related problems.

4.3. Privacy disclosure

It is very difficult to avoid infringing the privacy of the object of surveillance by monitoring the public in public places without consultation and information collection. In addition to information privacy and space privacy, we should pay special attention to the individual's self-conscious privacy, that is, the individual's right not to be interfered by the outside world and to decide his privacy life independently. Whether personal information is open or not and how to use it should all depend on the independent free will of the obligee. However, the current face recognition technology infringes on the above privacy without any technical barriers, especially It is self-conscious privacy. The face recognition system can collect, analyse and disclose stable information such as personal name, age, occupation, property status, and real-time information such as movement track and consumption record without the permission of personal self-determination. With the improvement of monitor accuracy and micro-expression psychoanalysis technology, in the future, the computer is even expected to read the sensitive information such as personality, emotion, conversation content, even potential diseases and sexual orientation of the monitored object through face recognition technology.

It can be said that under the comprehensive monitoring of face recognition system in public places, everyone has been alienated as a pure "information label", and face has been incorporated into a larger identity recognition or authentication system, in which face plays a specific role, with the same meaning as traditional identifiers such as character password and bar code. In this sense, the human face is regarded as an information structure and the whole human body is equivalent to a small mobile database under a large database. However, the potential change of the function of recognition technology will cause the information of these "small databases" to be picked up by technology users at any time and without cost. Face recognition technology creates the information equivalent of the face. Although this information equivalent belongs to the recognition object itself, the right to use it is in the hands of technology users, and it will hardly create any positive benefits for its owners. Therefore, the monitoring system in public places is faced with a dual privacy problem. On the one hand, the monitor collects the privacy information of the monitored object ; on the other hand, the database information leakage caused by the potential function change. However, although the face recognition system in public places can not prove that its security benefits exceed the individual privacy loss, with the continuous expansion of the application field of this system, the face recognition system in public places will become a rigid demand, its technology research and development and application field expansion will not stop. The contradiction between the privacy and security of face recognition technology will continue The discussion went on in-depth.

5. REFLECTION ON FACE RECOGNITION TECHNOLOGY

Nowadays, face recognition technology has been widely used in our daily life. On the one hand, we feel that it brings great convenience to our life; on the other hand, we cannot help worrying about whether our information security and privacy can be guaranteed. Everything has two sides, and face recognition technology is no exception. On the one hand, the emergence of face recognition technology marks the progress of human society and plays a role in promoting the development of various fields of society. Face recognition technology is convenient in information collection; different from traditional information collection methods, a computer can quickly and accurately give a recognition result by accurate calculation with a simple sweep of the face, which can save more time and cost. By using face recognition technology to manage and collect information, government agencies can improve management efficiency, reduce management and operation costs, make up for the lack of traditional information collection methods, and better realise the efficient management of citizen information. Through face recognition technology, businesses can also better extract the basic information of customers, quickly locate and classify the target groups of customers, and make different plans for the information data of different customer groups, which can improve customer satisfaction at the same time, effectively increase enterprise income, and achieve high-profit return under convenient information collection.

In technical practice, face structure has the characteristics of similarity and variability, which is not good for the use of face to distinguish human individuals. If law enforcement agencies use face recognition technology to find criminals in public, they may catch the wrong person due to similar facial features; when we use our face to unlock mobile phones or electronic payments, they may fail to recognise because of lighting conditions, face masks, age changes and other factors. However, with the gradual integration of two-dimensional and three-dimensional recognition technology and the continuous improvement of algorithm performance, face recognition technology has gradually overcome various adverse factors, has reached a considerable accuracy, and the recognition rate is rising rapidly. At the same time, due to the inherent convenience

of face recognition technology in hardware configuration, compared with fingerprint recognition and iris recognition, the convenience of face recognition is more prominent. If a group of individuals can't complete fingerprint recognition due to the lack of fingerprint features and the difficulty of imaging, there is no such problem in face recognition, and it doesn't need to raise hands, adjust the strength, just "sweep through", and all the information can be reflected. The cost of iris recognition equipment is high, and it can not be widely promoted, which is one of the main reasons why we seldom use iris recognition in our daily life. The low threshold of face recognition in technical equipment makes it very convenient to be used and promoted.

When we are immersed in the joy that face recognition technology brings great convenience to our daily life, we should think more about how to maintain personal information security and how to protect personal privacy. With the development of face recognition technology, the privacy of the public should not be the victim. In the United States, for example, in May 2019, the San Francisco Board of supervisors decided to ban San Francisco police from using face recognition software to find criminals with an absolute majority of votes. The city, which has many high-tech companies, became the first city in the United States to introduce a ban on face recognition. Taking Sweden as an example, the board of directors of a high school in the country considers that this processing method of personal information of students is not in line with the provisions of the general data protection regulations (GDPR) of the European Union because of the use of face recognition system to record students' attendance. The Swedish data regulatory authority issued a fine of SEK 200000 (about the privacy protection of RMB 147000) to this high school Single.

Therefore, developed countries in Europe and the United States have begun to restrict face recognition technology. In the face of human rights protection and scientific and technological development, they do not hesitate to choose the former. Therefore, to achieve a harmonious coexistence of face recognition technology and citizen privacy, the most fundamental problem is the control of information intake and application process. We need to regulate the behaviour from the legislative level. At the same time, we need to use technical means to protect the personal information security and privacy rights and interests of citizens from the root. Enterprises and businesses play a leading role in the process of data information intake and application. The source and processing of data information are controlled by enterprises and businesses. The whole process is in a dark box. No matter in the face of government regulatory departments or ordinary users, there is a lack of transparency. The legislative way to judge whether the regulation is caused by malignant results will be in an obvious passive state. At the same time, the way of "using technology to control technology" is considered. For example, the face recognition system can automatically blur features after recognition, desensitise the output results in advance, and achieve a certain protective effect.

With the rapid development of high technology, it is more necessary to regulate illegal behaviours and protect citizens' privacy from the legal level. The legal design has a certain lag, but in the face of new technology, we should speed up the legislative work and put forward some specific solutions to the existing problems. We should broaden the legislative thinking, given the new problems that may appear in the future high-tech development, we should also take into account the new legislative plan, and pay attention to the predictability of legal design.

6. CONCLUSION

The accuracy and reliability of face recognition technology can not meet the requirements in some fields for the time being. At this stage, the significance is to liberate those who have been in the repetitive working environment for a long time, to achieve the purpose of reducing cost and enhancing efficiency, Still, it does not mean to replace a certain profession or technology. With the development of pattern recognition, computer vision, image processing and machine learning, the accuracy and speed of face recognition will be improved. Just like computers can surpass human beings in many fields through deep learning, machine vision cooperates with databases and processors in the background through advanced devices in the front end, and computer face recognition will surpass human recognition speed and accuracy in an all-round way. In addition to identity recognition, it will also realise new functions such as judging age, beauty and health. Shortly, face recognition technology will gradually come into daily life and be widely used.

In the name of safety, for public places such as subway, where people flow in and out on a large scale daily, the first physical examination is carried out. Then the same examination of people is carried out. Now face recognition is to be carried out. Shortly, gene or fingerprint recognition may be further carried out. If it develops according to the current trend, there is such a possibility. In the near future, public transportation such as subway will become a kind of privilege that only some members of society can enjoy. If this society has not yet fallen into the state of persecution delusion, it should stop at security issues. What hysterical pursuit of security brings to society is not security at all, but comprehensive repression and panic. For the subway to use face recognition for classified security check, the real worry and fear are that their information is abused by the public authority. Because when they abuse, people have no idea what kind of price they and their families will pay. Property, reputation, occupation, freedom, health or life are all possible. Therefore, it is necessary for the Standing Committee of the National People's Congress to conduct basic legitimacy review. At the same time, it is necessary to consider starting the corresponding legislative procedures to regulate the random use of face recognition technology.

ACKNOWLEDGMENT

This research was supported by colleagues and students in the Department of Public Administration, Nan fang College of Sun Yat-sen University. Thanks, for their hard-working.

REFERENCES

[1] Nie Ruihua, Li Kingman, Shi Ting, Research on Information Security in Face Recognition System, Digital Technology & Application. 37 (11) (2019), p. 167.

[2] Wang Junxiu, What is Privacy——Privacy Reconstruction in Digital Society, Exploration and Free Views. (02) (2020), pp. 86–90.

[3] Mao Yanan, The first case of face recognition: what is it, Fangyuan Magazine. (24) (2019), pp. 14–17.

[4] Guan Chenglin, The Application of Face Recognition in the Field of Social Public Security, Management & Technology of SME. (12) (2019), pp. 189–191.

[5] Wang Chunhui, Abuse of "face recognition technology" violates legal requirements, China Telecommunications Trade. (12) (2019), pp. 68–70.

[6] Sheng Ya, Yin Xuanxi, Face recognition faces privacy issues, where do we go from here, China Telecommunications Trade. (09) (2019), pp. 31–33.

[7] Wang Yan, Zhang Lei, Security, privacy, and civil liberties: reflections on the technical security of face recognition systems in public places, Journal of the Party School of Shengli Oilfield. 32(01) (2019), pp. 74–76.

[8] Wang Qiaochen, Wu Zhengang, A Survey on Security and Privacy Problems in Application Systems of Face Recognition, The Journal of New Industrialization. 9(05) (2019), pp. 47–50.

[9] Duan Jianing, Development and function of face recognition technology, Public Communication of Science & Technology. 10(18) (2018), pp. 100–101.

[10] WEN Y, ZHANG K, LI Z, et al. A Comprehensive Study on Center Loss for Deep Face Recognition, International Journal of Computer Vision. 127(6-7) (2019), pp. 668-683.

[11] RAMACHANDRA R, BUSCH C. Presentation Attack Detection Methods for Face Recognition Systems: A Comprehensive Survey, ACM Computing Surveys (CSUR). 50(1) (2017), pp. 1-37.

[12] ZHAO X, LIN Y, HEIKKILA J. Dynamic Texture Recognition Using Volume Local Binary Count Patterns With an Application to 2D Face Spoofing Detection, IEEE Transactions on Multimedia. 20(3) (2018), pp. 552-566.

[13] AKHTAR Z, RATTAN A. A Face in any Form: New Challenges and Opportunities for Face Recognition Technology, Computer. 50(4) (2017), pp. 80-90.

[14] RAGHAVENDRA R, RAJA K B, BUSCH C. Exploring the Usefulness of Light Field Cameras for Biometrics: An Empirical Study on Face and Iris Recognition, IEEE Transactions Information Forensics and Security. 11(5) (2016), pp. 922-936.

[15] RAGHAVENDRA R, RAJA K B, BUSCH C. Presentation Attack Detection for Face Recognition Using Light Field Camera, IEEE Transactions on Image Processing. 24 (3) (2015), pp. 1060-1075.

[16] SUN X, HUANG L, LIU C. Multispectral face spoofing detection using VIS-NIR imaging correlation, International Journal of Wavelets, Multiresolution and Information Processing. 16(2) (2018), pp. 1-15.

[17] PENG F, QIN L, LONG M. Face presentation attack detection using guided scale texture, Multimedia Tools and Applications. 77(7) (2018), pp. 8883-8909.