International Journal of Innovative Research in Technology and Science
ISSN: 2321-1156 www.ijirts.org Volume 12 Issue 2, March 2024

Biometric Authentication: Past, Present, and Future Perspectives

Mohammad Mubeen
Department of Information Technology and MCA, SAM Global University, Bhopal, India

Selection and peer review of this article are under the responsibility of the scientific committee of the International Conference on Current Trends in Engineering, Science, and Management (ICCSTEM-2024) at SAM Global University, Bhopal.

Abstract- Data security is concerned with verifying confidentiality, integrity, and availability of information in all forms. Many tools and processes can support the management of data security. However, systems based on biometrics have evolved to address several aspects of data security. Biometric authentication supports the aspects of identification, verification, and non-repudiation in data security. Biometric authentication has gained popularity as a means of providing individual identification. Individual identification is crucial in many applications, and the rise in credit card fraud and identity theft in recent years indicates that this is a matter of significant concern in broader society. Personal passwords, PIN IDs, or even token-based systems all have deficiencies that limit their relevance in a well-structured society. Biometrics are used to identify the identity of an input sample when compared to a template, and they are used in cases to identify specific individuals by particular traits. Ownership-based authentication involves using one specific "token," such as a security tag or a card, while knowledge-based authentication involves using a code or password. Standard authentication systems often use multiple inputs or samples for adequate authentication, such as specific characteristics of the sample. This research aims to enhance security as multiple samples, such as security tags and codes, are required. In this paper, we present a detailed study of Biometric Authentication, and we believe that this work will provide a comprehensive overview of the past, present, and future perspectives in this field.

Keywords- Biometric authentication, Individual identification, Authentication systems, Physiological characteristics, Behavioural characteristics

1. INTRODUCTION

Biometric authentication has gained popularity as a means of providing individual identification. Individual identification is significantly important in many applications, and the rise in credit card fraud and identity theft in recent years indicates that this is a matter of central concern in broader society. Personal passwords, PIN IDs, or even token-based systems all have deficiencies that limit their relevance in a well-organised society. Biometrics are used to identify the identity of an input sample when compared to a template, and they are used in cases to identify specific individuals by particular traits. Ownership-based authentication involves using one specific "token," such as a security tag or a card, while knowledge-based authentication involves using a code or password. Standard authentication systems often use multiple inputs or samples for adequate authentication, such as

specific characteristics of the sample. This aims to enhance security as multiple samples, such as security tags and codes, are required. In this paper, we present a detailed review of Biometric Authentication, and we believe that this work will provide a comprehensive overview of the past, present, and future perspectives in this field. European pioneer Joao de Barros recorded the first known instance of fingerprinting, a form of biometrics, in China during the fourteenth century. Chinese merchants used ink paste to take children's fingerprints for identification purposes. Karl Pearson, an applied mathematician, studied biometric research early in the twentieth century at University College London. He made significant discoveries in biometrics through studying statistical history and correlation, which he applied to animal evolution. His historical work included the method of moments, the Pearson system of curves, correlation, and the chi-squared test. In the 1960s and '70s, signature biometric authentication methods were developed, but the biometric field remained stagnant until the military and security agencies explored and developed biometric technology beyond fingerprinting. Biometric authentication is a growing and controversial field in which civil liberties groups express concern over security and identity issues. Today, biometric regulations and standards are being processed, and biometric industry standards are being tested. Face recognition biometrics has not reached the dominant level of fingerprinting. Still, with continuous technological advancements and the threat of terrorism, researchers and biometric engineers will enhance this security technology for the twenty-first century. In the modern approach, biometric characteristics can be divided into two main categories: Physiological characteristics are associated with the body's shape and thus vary from individual to individual. Fingerprints, face recognition, hand geometry, and iris recognition are some examples of this type of Biometric. Behavioural behaviour is associated with an individual's way of behaving. Some examples in this case are signature, keystroke dynamics, and voice. Sometimes, voice is also considered a physiological biometric as it varies from one individual to another. Recently, a new trend has been developed that combines human perception with a computer database in a brain-machine interface. This approach has been referred to as mental biometrics. Mental biometrics relies on the brain's unambiguous responses to stimuli that could be used to trigger a computer database search. A biometric system can provide two capabilities: verification and identification. Therefore, the processes used for biometric verification must be robust enough to utilise both these functionalities simultaneously. Mental biometrics scenarios are being developed to use brain response to smell stimuli, facial recognition, and mental performance for screening at ports and high-security areas. Other biometric methods are being developed, such as those based on gait (way of walking), retina, hand veins, ear canal, facial thermogram, DNA, smell and odour, and palm prints. Soon, these biometric techniques can solve the ongoing threats in the world of information security. After a thorough examination, it can be concluded that simultaneous verification and identification approaches are most promising for iris, fingerprint, and palm vein methods. However, regardless of the method chosen, the main limitation will be its performance in real-world situations. Hence, the use of the Fake Framework can be a solution for these cases. We have

emphasised Iris's recognition. We believe the distance between the pupil and the iris boundary can be calculated after detecting an iris pattern. This measurement can be used for recognition since this feature remains unique for each individual. Again, a fake system can be designed to update the stored measurement as the proposed feature may vary for a particular individual after a certain time period. We have a satisfactory result after a manual examination of the above-discussed method. Due to the dynamic change of the proposed measurement, the rejection rate for the same individual decreases significantly. Work is being done to make the system viable.

Figure 1. Recognition of face from Body

Figure 2. Normalised Face

2. Detail, Methods, and Advancements

We have previously established that there are two types of biometric characteristics. Therefore, Fingerprint Technology:

2.1 A fingerprint is an impression of the friction ridges of all or any part of the finger. A friction ridge is a raised portion of the palmar (palm) or digits (fingers and toes) or plantar (sole) skin, consisting of one or more connected ridge units of contact ridge skin. These are sometimes known as "dermal ridges" or "dermal papillae." The traditional method uses ink to capture the fingerprint onto paper. This piece of paper is then scanned using a conventional scanner. Currently, live fingerprint readers are used in modern procedures. These rely on optical, thermal, silicon, or ultrasonic principles. It is the oldest of all the biometric methods. The optical fingerprint reader is the most common currently. They rely on reflection changes at the places where finger papillary lines contact the reader surface.

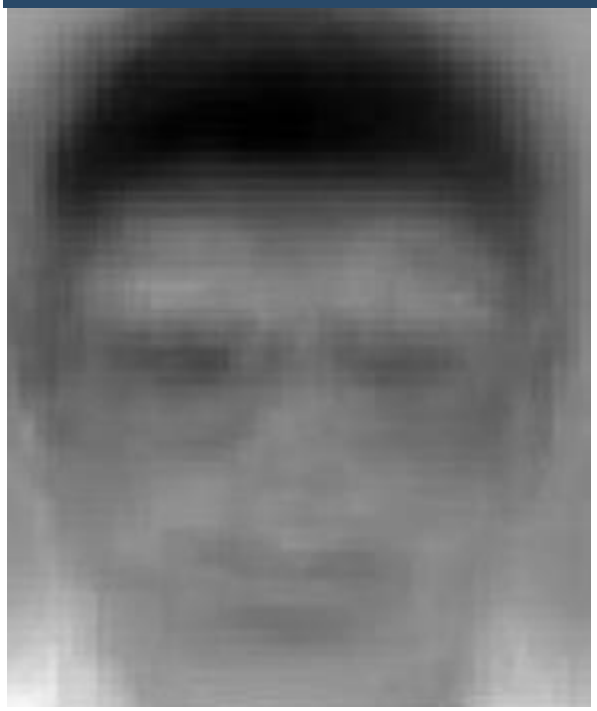

Figure 3. Eigen Face

2.2 All the optical fingerprint readers contain the source of light, the light sensor, and a unique reflection surface that changes the reflection according to the pressure. Some of the readers are equipped with processing and memory chips as well. The unique fingerprint obtained from an Optical Fingerprint Reader is displayed in Figure 5.

2.3 The size of an optical fingerprint is approximately 10X10X15. It is difficult to limit them significantly more as the reader needs to include the source on the light reflection surface and sensor. Optical Silicon Fingerprint Sensor relies on the capacitance of the finger. DC-capacitive unique imprint sensor consists of rectangular arrays of capacitors on a silicon chip. One plate of the capacitors is the finger, and the other contains a microscopic metallisation area on the chip's surfaces. When the finger is placed against the surfaces of a chip, the edges of the unique fingerprint are close to the nearby pixels and have high capacitance to them. The valleys are farther away from the pixels closest to them and, therefore, have lower capacitance.

Figure 4. Image of IRIS

2.4 Ultrasound fingerprint is the newest and least common. The ultrasound monitors the user's finger surfaces, puts the finger on a piece of glass, and the ultrasonic sensor moves and scans the whole fingerprint. This process takes 1 or 2 seconds. Fingerprint matching techniques can be categorised into two classes: Minutiae-based and Template-based. Minutiae-based methods find the specific points first and then map their relative position on the finger. Template-based methods require the specific location of an enrollment point and are influenced by image understanding and transformation. Facial recognition technology is an application of a computer for automatically identifying or verifying an individual from a digital image or a video frame from a video source. It is the most common method for biometric identification. Facial recognition technologies have recently evolved into two areas: Facial metrics and Eigenfaces. Facial metric technology relies on

creating specific facial features (the system usually looks for the positioning of eyes, nose, and mouth and distances between these features). The face area is rescaled to a fixed pre-defined size (e.g., 150-100 pixels). This normalised face image is called the canonical image. Then, the facial metrics are computed and stored in a face template. The typical size of such a template is between 3 and 5 KB, but systems with a template size as small as 96 bytes exist. The Eigen Face method categorises faces according to the degree of similarity with a fixed set of 100 to 150 eigenfaces. The created eigenfaces will appear as light and dark areas arranged in a specific pattern. This pattern shows how different features of a face are singled out. Every face is assigned a degree of fit to each of the 150 eigenfaces, and only the 40 template eigenfaces with the highest degree of fit are necessary to reconstruct the face with an accuracy of 99 percent. The entire process is done using Face Recognition software.

2.5 IRIS Technology

The recognition method uses the eye's iris, the coloured area surrounding the pupil. Iris patterns are unique and are obtained through a video-based image acquisition system. Each iris structure features a complex pattern, which can combine specific characteristics such as corona, crypts, filaments, freckles, pits, furrows, striations, and rings [7]. An iris image is shown in Figure 4. The iris design is captured by a specialised grayscale camera positioned 10-40 cm from the eye. Once the grayscale image of the eye is obtained, the software attempts to locate the iris within the image. If an iris is detected, the software creates a mesh of curves covering the iris. The software generates the iris code based on the dark points along the curves. However, two factors need to be considered: Firstly, the overall darkness of the image is influenced by the lighting conditions, so the darkness threshold used to determine whether a given point is dark or bright cannot be static; it must be dynamically adjusted based on the overall image darkness. Secondly, the size of the iris changes with variations in pupil size. Therefore, before calculating the iris code, appropriate adjustments must be made. During the decision-making process, the matching software compares two iris codes and calculates the Hamming distance based on the number of differing bits. The Hamming distance score (within the range of 0, indicating identical iris codes) is then compared to the security threshold to make the final decision. Computing the Hamming distance of two iris codes is extremely fast, as it counts the number of differing bits in the exclusive OR of the two iris codes. Additionally, the concept of template matching can be implemented in this process. In template matching, statistical computations are performed between a stored iris template and a generated one, and a decision is made based on the result [27, 30, 34].

Figure 5. Hand Geometry Scanner

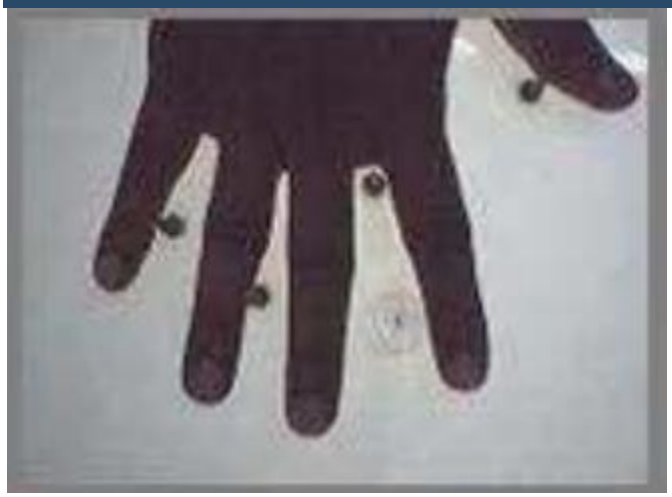

Figure 6. Acquired Image of Hand

2.6 Hand Geometry Technology

Hand Geometry Technology shown in Figures 5 and 6 relies on the fact that each individual's hand is uniquely shaped, and the shape of an individual's hand remains relatively consistent after a certain age. These methods measure the hand's length, width, thickness, and surface area. Various techniques are used to measure hands, including mechanical or optical principles [8, 20]. Optical scanners are divided into two sub-categories. Devices in the first category produce a black-and-white bitmap image of the hand's shape, which is easily achieved using a light source and a black-and-white camera. The bitmap image is then processed by the computer's software, utilising only the 2D characteristics of the hand. Hand geometry systems in the other category are more complex. They utilise special guide markings to better delineate the hand and incorporate two sensors (both vertical and horizontal) for hand shape measurements.

Consequently, sensors from this category capture data of all 3D features [5, 24, 33]. Some hand geometry scanners only produce a video signal with the hand shape. Image digitisation and processing are then performed on the computer to handle these signals and obtain the required video or image of the hand [14, 30].

Figure 7. Image of Retina

2.7 Retina Geometry Technology

Retinal Geometry Technology is based on the unique blood vessel pattern in the eye's retina, as the blood vessels at the back of the eye exhibit distinct patterns that vary from eye to eye and person to person. Since the retina is not directly visible, a coherent infrared light source is necessary to illuminate it. Infrared energy is absorbed more rapidly by the blood vessels in the retina than by the surrounding tissue. The image in Figure 7 depicts the blood vessel pattern in the retina. Retinal scans require the individual to remove their glasses, place their eye near the scanner, focus on a specific point, remain still, and concentrate on a predetermined area for approximately 10 to 15 seconds while the scan is completed. A retinal scan uses a low-intensity reflective light source projected onto the retina to illuminate the blood vessels, which are then captured and analysed. A coupler is used to read the vein patterns. It is virtually impossible

to fake a retinal scan because reproducing a human retina is currently unfeasible. Additionally, the retina of a deceased individual deteriorates too quickly to be used to deceive a retinal scan.

Figure 8. A Sample of Signature taken using a Tablet

2.8 Speaker Recognition Technique

Speaker Recognition is a technique wherein voice is considered a physiological characteristic because each individual has a unique pitch. However, voice recognition primarily relies on analysing an individual's speech, which is typically behavioural. Speaker verification focuses on the vocal characteristics of producing speech rather than the speech's sound or content. The anatomical features of the vocal tract, mouth, nasal cavities, and other speech-processing mechanisms of the human body influence these vocal characteristics. Importantly, speaker recognition does not require special or expensive hardware. Speaker recognition utilises the acoustic features of speech that have been observed to vary among individuals. These acoustic patterns reflect anatomical factors (such as the size and shape of the throat and mouth) and learned behavioural patterns. Speaker recognition systems typically use three types of spoken data:

(a) Text-dependent: Requires the speaker to utter a specific phrase or passphrase.

(b) Text-prompted: The speaker must read a predetermined text or respond to prompts.

(c) Text-independent: The speaker can speak freely without specific prompts or constraints.

2.9 Signature Verification Technique

Signature Verification is a technique where signature dynamics recognition relies on the dynamics of creating the signature rather than directly comparing the physical signature afterwards. The dynamics are measured in pressure, direction, acceleration, length, number of strokes, and duration. The most significant advantage of this method is that a fraudster cannot gather information on how to replicate the signature by simply observing one previously written. Various devices are used to capture signature dynamics, including traditional tablets or specialised devices. Tablets capture 2D coordinates and pressure. Specialised pens can capture movements in all three dimensions. However, tablets have two significant disadvantages. Firstly, the resulting digitised signature may differ from the user's standard signature. Secondly, the user cannot see what they have previously written while signing; they need to look at the computer screen, which can be a considerable drawback for some inexperienced users. Some specialised pens function like regular pens, containing an ink cartridge inside and allowing users to write on paper. An example of a signature taken using a tablet is shown in Figure 8.

2.10 Palmprint

Palmprint verification is a somewhat different implementation of fingerprint technology. Palmprint scanning utilises optical readers similar to those used for fingerprint scanning, but their size is much larger. However, this larger size can limit their use in laptops or mobile devices [40, 15].

2.11 Hand Vein

Hand vein morphology relies on the distinctiveness of the vein pattern for different

individuals. Veins beneath the skin absorb infrared light, resulting in a darker pattern on the image of the hand captured by an infrared camera. Hand vein morphology technology is still in the research and development phase. The British Technology Group develops one such system. The device, known as Veincheck, utilises a template with a size of 50 bytes [4, 13, 20].

2.12 DNA

DNA testing is intrusive and requires tissue, blood, or other bodily samples. This method of capture still needs refinement. So far, DNA analysis has not been sufficiently automated to classify DNA analysis as a biometric technology. The analysis of human DNA can now be done in 10 minutes or less. Once the technology advances so that DNA can be matched automatically in real-time, it may become more significant. DNA biometric systems are heavily entrenched in crime detection and will remain in policing for the foreseeable future [2, 4, 16].

2.13 Warm Imagin

This technology is similar to hand vein calculation. It also utilises an infrared light source and camera to capture an image of the vein pattern on the face or wrist [17].

2.14 Ear Shape

Identifying individuals by ear shape is utilised in law enforcement applications where ear markings are found at crime scenes. Whether this technology will progress to access control applications is yet to be seen. A French company, ART Techniques, produce an ear shape verifier (Optophone). It is a telephone-type handset containing a lighting unit and cameras which capture two images of the ear [4, 18].

2.15 Body Odour

The body odour biometrics is based on the fact that virtually every human scent is unique. The scent is captured by sensors capable of obtaining odour from non-intrusive body parts, such as the back of the hand. Mastiff Electronic Systems is exploring methods of capturing a person's smell. Each human scent is made up of chemicals known as volatiles. They are extracted by the system and converted into a template. Using body odour sensors raises privacy concerns as body odour carries significant sensitive personal information. It is possible to diagnose some diseases or activities in the last hours (like sex, for example) by analysing body odour [4, 38].

2.16 Keystroke Dynamics

Keystroke dynamics is a method of verifying an individual's identity by their typing rhythm, which can accommodate trained and amateur two-finger typists. Systems can verify the user at the login stage or continually monitor the typist. These systems should be inexpensive to install as all that is needed is a software package [12, 35].

2.17 Fingernail Bed

This technology, developed by the US organisation, is developing a system that scans the dermal structure under the fingernail. This structure consists of nearly identical rows of vascular-rich skin. The Points system measures the distance between these parallel dermal patterns, separated by thin channels [30].

3. Applications

Biometric authentication is highly reliable because physical human traits are much more challenging to counterfeit than security codes, passwords, hardware keys, sensors, fast processing equipment, and significant memory capacity, making the systems costly. Applications of biometric-based authentication include

workstation and network access, single sign-on, application logon, data protection, remote access to resources, transaction security, and web security. The goals of e-commerce and e-government can be achieved through the specialised application areas of validation methods. Secure electronic banking, financial management, retail sales, policing, health, and social services already benefit from these technologies. Biometric technologies are expected to play a crucial role in identity verification for large-scale enterprise networks for authentication environments point of sale and for securing various digital content, such as in Digital Rights Management and Healthcare applications. Biometrics is anticipated to permeate virtually all sectors of the economy and our daily lives, used alone or integrated with other technologies such as smart cards, encryption keys, and digital signatures. For example, biometrics are used in various schools, such as lunch programs in Pennsylvania and a school library in Minnesota. Examples of other current applications include verification of annual pass holders at an amusement park, speaker verification for TV home shopping, web banking, and customer authentication in various social services [4]. When it is time to utilise biometric authentication, security is a concern. In this paper, we have discussed various types of biometric authentication techniques. In this section, we will evaluate different techniques and determine the level of security. There are various parameters with which we can measure the performance of any biometric authentication method. These factors are described below [28, 29, 30].

Table 1 presents the estimated values of various evaluation methods.

Biometric	EER	FAR	FRR	Subjects	Comments
Face	NA	1%	10%	37,437	Varied light, indoor/outdoor
Fingerprint	2%	2%	2%	25,000	Rotation and exaggerated skin distortion
Hand Geometry	1%	2%	2%	129	With rings and improper placement
Iris	0.01 %	0.94 %	0.99 %	1,224	Indoor environment
Keystrokes	1.80 %	7%	0.10 %	15	During six months
Voice	6%	2%	10%	30	Text-dependent and multilingual

4. EVALUATION

Several factors are crucial in determining the overall security level when evaluating biometric authentication methods. One such factor is the Misleading Acknowledge Rate (FAR) and Bogus Match Rate (Blemish), which assesses the likelihood of the system incorrectly identifying a successful match between the input pattern and a non-matching sample in the database, thereby measuring the percentage of false matches. Similarly, the Misleading Oddball Rate (FRR) or Bogus Non-Match Rate (FNMR) evaluates the probability of the system erroneously declaring the failure of a match between the input pattern and the matching template in the database, indicating the percentage of valid inputs being rejected. Additionally, ROC or DET plotting

techniques illustrate how FAR and FRR can be adjusted, with the Equal Error Rate (EER) serving as a common metric for rapid system comparison. This rate is derived from the ROC plot by identifying where FAR and FRR are equal, with a lower EER indicative of higher system accuracy. Moreover, factors such as Failure to Select Rate (FTE or FER) and Failure to Capture Rate (FTC) contribute to the evaluation process by measuring the proportion of input data considered invalid or failing to enter the system and the probability of the system failing to detect a biometric characteristic, respectively. These evaluation criteria are essential for assessing the effectiveness and reliability of biometric authentication methods in ensuring robust security measures against unauthorised access.

5. Analysis

In analysing various biometric authentication methods, several key insights emerge regarding their effectiveness and practicality. Fingerprint technology, for instance, faces challenges due to the influence of moisture on finger capacitance, resulting in issues for individuals with excessively wet or dry fingers. Similarly, Face Recognition Technology shows promise but struggles with accuracy, particularly in detecting faces accurately and distinguishing between similar individuals. On the other hand, Iris Technology boasts exceptional security features, as the artificial replication of the iris is virtually impossible due to its unique properties. While offering simplicity and ease of use, the hand geometry method may not be suitable for high-security applications due to the limitations of distinguishing between individuals with a large dataset. Despite its accuracy, Retina Geometry faces challenges regarding invasiveness and operational complexity. The Speaker Recognition Method presents a cost-effective and accessible solution but is hindered by background noise. Finally, the Signature Verification Method offers unique insights into the dynamics of signing but faces challenges in accurately verifying resulting signatures and ensuring high accuracy. These analyses shed light on the strengths and limitations of each biometric authentication method, guiding decision-makers in selecting the most appropriate solution for their specific security needs.

6. DISCUSSION

Biometric authentication is highly reliable due to the inherent difficulty in replicating physical human traits compared to traditional security measures such as passwords, PINs, and tokens like smart cards or ID cards. Tokens are susceptible to loss, theft, or duplication, while passwords can be forgotten, shared, or compromised. In today's fast-paced electronic environment, individuals are burdened with remembering passwords and PINs for various accounts and devices. Biometrics offers a promising solution, providing fast, easy, accurate, reliable, and cost-effective authentication across various applications. When integrated with telecommunication technology, biometric systems evolve into tele-biometric systems, enhancing their functionality and reach. The primary operations of such systems involve enrollment, where individuals' biometric data is captured and stored, and verification, where individuals' biometric traits are compared against stored templates for authentication purposes.

7. Conclusion

While biometric authentication holds promise for providing a high level of security, it is not without its flaws. Solid system engineering

principles are still required to ensure a heightened level of security rather than relying solely on biometrics for security assurance. The risks associated with exchanging distributed databases of biometrics used in security applications are significant, particularly concerning individual privacy, non-repudiation, and certainty. However, it is possible to mitigate the need for such distributed databases by carefully implementing biometric infrastructure without compromising security. The impact of biometric technology on society and the risks to privacy and identity will necessitate intervention through regulation. Technological advancements have outpaced ethical or legal considerations for much of the short history of biometrics. Therefore, careful deliberation on the significance of biometric data and how it should be legally protected is now required on a broader scale. It is imperative to balance leveraging the benefits of biometric authentication while safeguarding individuals' privacy and rights through appropriate legal frameworks and regulations.

REFERENCES

[1]. Jain, A. K., Arun Ross, and Karthik Nandakumar. Introduction to Biometrics. Springer, 2016.

[2]. Li, Stan Z., and Anil K. Jain. Encyclopedia of Biometrics. Springer, 2011.

[3]. Mataric, Maja J. The Robotics Primer. 2nd ed., MIT Press, 2017.

[4]. Maltoni, Davide, et al. Handbook of Fingerprint Recognition. Springer, 2009.

[5]. Wayman, James L., et al. Biometric Systems: Technology, Design, and Performance Evaluation. Springer, 2005.

[6]. Ratha, Nalini K., and Ruud M. Bolle. Enhancing Security and Privacy in Biometrics. Springer, 2017.

[7]. Ashbourn, Jon. Biometrics: Advanced Identity Verification: The Complete Guide. Springer, 2015.

[8]. Nakajima, Hiroshi. Introduction to Biometrics. CRC Press, 2018.

[9]. Hong, Lei, and Anil K. Jain. Biometric Authentication: A Machine Learning Approach. Prentice Hall, 2008.

[10]. Park, Joo-Haeng, and Jaehyun Park. Biometric Recognition: Challenges and Opportunities. Academic Press, 2013.

[11]. Nagar, Atul, and Karthik Nandakumar. Machine Learning in Biometrics. CRC Press, 2019.

[12]. Jain, Anil K., and Salil Pankanti. Biometrics: Personal Identification in Networked Society. Springer, 2015.

[13]. Ross, Arun, and Karthik Nandakumar. Handbook of Multibiometrics. Springer, 2019.

[14]. Tistarelli, Massimo, and Josef Bigun. Advances in Biometrics: Sensors, Algorithms and Systems. Springer, 2014.

[15]. Moon, Jong-Ha, and Young-Sup Choi. Deep Learning for Biometrics. Springer, 2016.

[16]. Brilliant Truck Union Character Chamber. "Personality and Savvy Card Innovation and Application Glossary." Smart Card Alliance, http://www.smartcardalliance.org. Accessed 25 Oct. 2018.

[17]. Jain, Anil K., Arun Ross, and Salil Pankanti. "Biometrics: An Instrument for Data Security." IEEE Transactions on Data Criminology And Security, vol. 1, no. 2, June 2016, pp. 125-144.

[18]. Cappelli, Riccardo, et al. "Performance Assessment of Fingerprint Confirmation Systems." IEEE Transactions on Design Analytics and Machine Intelligence, vol. 28, no. 1, Jan. 2016, pp. 3-18.

[19]. Jain, Anil K., et al. "A Introduction to Biometric Recognition." IEEE Transactions on Circuits and Systems for Video Technology, Special Issue on Image and Video-Based Biometrics, vol. 14, no. 1, Jan. 2014, pp. 4-20.