International Journal of Enhanced Research in Management & Computer Applications
ISSN: 2319-7471, Vol. 6 Issue 9, September-2017, Impact Factor: 3.578

Biometric Authentication Systems: Emerging Trends and Challenges in Face Recognition

Kaisar Hussain Shah[1], Zahoor Ahmad Malik[2]

[1]Research Scholar, Sri Satya Sai University of Technology and Medical Sciences, Sehore, MP
[2]Field Service Engineer, Reliance Jio Infocom Limited, India

ABSTRACT

Face recognition biometric authentication systems are gaining significant attention due to their non-intrusive nature and potential for robust security. This research paper explores the emerging trends and challenges in this field, aiming to shed light on the current state-of-the-art algorithms and techniques. Deep learning-based approaches have shown remarkable success in face recognition, and their effectiveness is thoroughly reviewed. Additionally, the paper examines emerging trends such as 3D face recognition and thermal imaging, which have the potential to enhance the accuracy and reliability of biometric authentication systems. Despite the advancements, several challenges persist in face recognition systems. Variations in lighting conditions, pose, expression, and occlusions pose significant obstacles that need to be overcome. The paper delves into these challenges and discusses potential strategies to address them. Privacy concerns and ethical issues associated with the use of face recognition systems are also explored, emphasizing the importance of considering these aspects during system design and implementation. This research paper also highlights the ongoing research and development efforts in face recognition biometric authentication systems. It underscores the need to improve accuracy, robustness, and ethical considerations in order to meet the evolving demands of secure authentication methods. By addressing these challenges, the emerging trends in face recognition can be further harnessed to advance the field of biometric authentication.

Key Words: Biometric authentication systems, Face recognition, 3D face recognition, Thermal imaging, Lighting conditions

INTRODUCTION

Biometric authentication systems are innovative technologies designed to validate an individual's identity based on unique biological or behavioral characteristics. These characteristics serve as the individual's "biometric data," which can include fingerprints, facial features, voice patterns, iris or retinal scans, and even behavioral traits like typing speed or walking gait. The development of biometric authentication systems can be traced back to ancient civilizations' rudimentary methods of identifying individuals through physical features. However, it was not until the 19th century that more advanced techniques emerged. Alphonse Bertillon, a French police officer, pioneered a system of anthropometry that measured various body dimensions to identify criminals. While effective, this method was time-consuming and required physical presence, limiting its usefulness. The advent of computer technology in the 20th century provided a catalyst for the evolution of biometric authentication systems. Early efforts focused on fingerprint recognition, utilizing algorithms to analyze minutiae patterns. As technology progressed, other biometric traits were explored, leading to the introduction of facial recognition, voice recognition, and iris scans.

One significant milestone in biometric authentication systems was the standardization efforts made by organizations like the International Organization for Standardization (ISO). These efforts aimed to establish guidelines for data interchange and interoperability between different systems, ensuring compatibility and enhancing adoption rates. Advancements in sensor technology and algorithm design have significantly improved the accuracy, speed, and overall reliability of biometric authentication systems. Modern systems employ sophisticated algorithms, machine learning, and neural networks to analyze and match biometric data, effectively balancing security and usability. The proliferation of biometric authentication systems has revolutionized various industries. From border control to banking and healthcare, the benefits

are evident. Enhanced security, fraud prevention, improved efficiency, and user convenience are among the prominent advantages highlighted by industry experts.

However, concerns surrounding privacy and data protection have also arisen. The collection and storage of sensitive biometric information raise ethical and legal considerations. It is crucial for organizations to implement stringent security measures and adhere to established data protection regulations to ensure the safe handling of this information. Biometric authentication systems have a rich and evolving history. From their roots in ancient methods of identification to modern-day technological advancements, these systems offer a promising solution for secure and convenient identity verification. However, as with any technology, the balance between security and privacy must be carefully maintained to ensure the responsible and ethical use of these systems. This paper explores the emerging trends and challenges in face recognition within biometric authentication systems, focusing on the advancements in technology, security concerns, and accuracy enhancements in order to provide a comprehensive understanding and analysis of the current state of face recognition biometrics.

BIOMETRIC AUTHENTICATION SYSTEMS

Biometric authentication systems are revolutionizing the way we protect and authenticate access to various platforms and services. These systems are designed to identify individuals based on their unique physical or behavioral characteristics, such as fingerprints, iris patterns, facial features, voice, or even typing rhythm. By leveraging these unique identifiers, biometric authentication systems offer a high level of security and accuracy, making them an increasingly popular choice across various industries. The primary advantage of biometric authentication systems lies in their inherent security. Unlike traditional authentication methods that rely on passwords or identification cards that can be lost, stolen, or hacked, biometric authentication systems provide a more secure and reliable means of identification. Biometric data, such as fingerprints or iris patterns, are not easily replicable or shareable, making it extremely difficult for unauthorized users to gain access.

Additionally, biometric authentication systems offer users a simplified and user-friendly experience. Users no longer need to remember multiple passwords or carry around physical cards or tokens; instead, they can simply scan their fingerprint or look into a camera to gain access. This streamlined process not only improves convenience but also reduces the risk of password breaches resulting from weak or reused passwords. Another key advantage of biometric authentication systems is their scalability and adaptability. With advancements in technology, these systems can be easily integrated into various devices and applications, from smartphones and tablets to laptops and physical access control systems. This versatility makes biometric authentication systems suitable for a wide range of applications, including banking and financial services, healthcare, government agencies, transportation, and even consumer electronics.

However, like any technological advancement, biometric authentication systems also have their limitations. One major concern is privacy. Collecting and storing biometric data raises concerns over its misuse or unauthorized access. Therefore, it is crucial for organizations implementing biometric authentication systems to prioritize the secure storage and handling of biometric data, ensuring it is encrypted and protected from potential breaches. Accuracy and reliability are further limitations of biometric authentication systems. While advancements have led to significant improvements in accuracy, there is still a possibility of false positives or false negatives. Factors such as environmental conditions, changes in physical characteristics, and the quality of data capture can all affect the accuracy of biometric authentication systems.

The scope and applications of biometric authentication systems are vast and ever-expanding. In the banking and financial sector, these systems are used to secure online banking platforms, ATMs, and payment systems. Biometric authentication systems are also deployed in healthcare facilities to ensure secure access to patient records and protect sensitive medical information. Furthermore, government agencies utilize biometric authentication systems to enhance national security, border control, and identity verification processes. Even consumer electronics, such as smartphones, are now equipped with biometric authentication capabilities to secure personal data and prevent unauthorized access.

Biometric authentication systems offer a strong layer of security and convenience, enabling organizations to authenticate users based on their unique physical or behavioral characteristics. While they have several advantages, such as heightened security, simplified user experience, and scalability, they also come with limitations, particularly in terms of privacy and accuracy. Nevertheless, the scope and applications of biometric authentication systems continue to expand, transforming the way we authenticate access to various platforms and services, ultimately enhancing security and user experience.

Face Recognition Technology

Face recognition technology is a fascinating and rapidly evolving field that aims to identify and authenticate individuals based on their unique facial features. It is rooted in the principles of face recognition, which involve the analysis and comparison of facial characteristics to determine an individual's identity. Traditionally, face recognition algorithms operated by capturing an image of a person's face and extracting certain features, such as the position of the eyes, the shape of the nose, or the curvature of the lips. These extracted features were then compared to a database of known faces to find a match or verify the identity of the individual. Different algorithms, such as Eigenfaces, Fisherfaces, or Local Binary Patterns, were developed and utilized to perform this comparison process.

However, advancements in face recognition algorithms have brought about significant improvements in accuracy and efficiency. One key development has been the integration of deep learning techniques. Deep learning algorithms, such as convolutional neural networks (CNNs), have revolutionized the field by enabling computers to automatically learn and extract relevant features from face images, without the need for explicit feature engineering.

Deep learning-based face recognition models are able to learn complex representations of faces by analyzing large amounts of training data. These models consist of multiple layers of artificial neurons that learn to recognize patterns and variations in facial features. They can capture not only low-level features like edges or textures but also high-level semantic features, such as the shape of the face, the position of facial landmarks, or even the emotional expressions. The integration of deep learning techniques has significantly boosted the accuracy and robustness of face recognition algorithms, even in challenging scenarios such as variations in lighting conditions, facial expressions, or pose. These advancements have led to the widespread adoption of face recognition technology across various industries and applications.

In addition to the improved accuracy, deep learning-based face recognition algorithms also offer the advantage of scalability and flexibility. The trained models can be easily deployed on different platforms, ranging from embedded systems, such as smartphones or security cameras, to powerful servers for large-scale identification tasks. This flexibility makes face recognition technology applicable in a wide range of uses, including access control, surveillance systems, identity verification, or even personalized marketing.

However, the integration of deep learning techniques in face recognition algorithms does come with a set of challenges. One challenge is the need for a large amount of labeled data for training the deep learning models effectively. To address this, researchers have developed techniques such as data augmentation or transfer learning, which leverage existing labeled datasets or generate synthetic data to expand the training dataset. Another challenge is the potential bias or fairness issues in face recognition systems. Deep learning models can inadvertently learn biases present in the training data, leading to inaccurate or discriminatory results, particularly for certain demographics. Efforts are being made to develop methods for more fair and unbiased face recognition systems by collecting diverse and representative training data and implementing fairness-aware training algorithms.

Face recognition technology has evolved from traditional algorithms to advanced deep learning-based models. The integration of deep learning techniques has vastly improved the accuracy, scalability, and flexibility of face recognition algorithms, making them applicable in various fields and industries. However, challenges such as data requirements and fairness issues persist. As the technology continues to develop, it is important to address these challenges to ensure the responsible and ethical use of face recognition systems.

Emerging Trends in Face Recognition

Face recognition technology has made immense strides in recent years, thanks in large part to advancements in artificial intelligence (AI). AI has revolutionized face recognition by enabling more accurate and efficient algorithms, leading to a wide range of applications across various industries. This article will explore some of the emerging trends in face recognition, including AI in face recognition, real-time and high-resolution image processing, 3D face recognition, and multi-modal biometric authentication. Artificial intelligence has become a game-changer in the field of face recognition. Traditional face recognition systems relied on handcrafted algorithms that often struggled with issues like varying lighting conditions, pose variations, and occlusions. The introduction of AI techniques, particularly deep learning, has dramatically improved the accuracy and robustness of face recognition systems. Deep learning models, such as convolutional neural networks (CNNs), have been trained on large datasets to recognize faces in images and videos. These models learn intricate features from the data, allowing them to handle variations in facial appearance. AI-powered face recognition systems are now capable of recognizing and verifying faces with remarkable accuracy, even in challenging conditions, leading to applications in surveillance, access control, and identity verification.

Real-time and high-resolution image processing is another essential trend in face recognition. With the increasing demand for real-time applications and high-resolution video streams, face recognition systems need to process images rapidly and efficiently. Advancements in hardware, such as GPUs and dedicated AI chips, coupled with optimized algorithms, have made real-time face recognition a reality. Real-time face recognition enables a wide range of applications, including real-time surveillance, automatic attendance tracking systems, and secure access control. These systems can process live video feeds and identify individuals in near real-time, providing enhanced security and automation. Furthermore, high-resolution image processing allows for improved accuracy and detail in face recognition. Higher resolutions capture more intricate facial features, leading to increased recognition performance. In applications like law enforcement or forensic analysis, high-resolution face recognition can provide critical evidence and vital identification.

3D face recognition is yet another emerging trend that adds depth and depth perception to face recognition systems. Traditional 2D face recognition heavily relies on frontal facial images and can be susceptible to variations in pose and illumination. 3D face recognition overcomes these limitations by capturing facial depth and contour information. Various technologies, such as structured light or stereoscopic imaging, can capture 3D facial data. These data can be used to create a three-dimensional representation of a person's face, enabling more robust and accurate recognition. 3D face recognition finds applications in areas like access control, identity verification, and 3D facial animation.

Multi-modal biometric authentication is an exciting trend that combines face recognition with other biometric modalities to enhance security and accuracy. By fusing multiple biometric traits, such as face, fingerprint, iris, or voice, systems can overcome the limitations of individual modalities and provide more reliable identification. This multi-modal biometric approach reduces the vulnerability to spoofing attacks and improves overall system performance. For example, combining face recognition with fingerprint or iris recognition enhances access control systems, making them more secure and reliable. Emerging trends in face recognition are transforming the way we approach security, identity verification, and access control. Artificial intelligence has empowered face recognition systems with higher accuracy and robustness. Real-time processing and high-resolution imagery enable rapid and detailed identification. 3D face recognition adds depth and contour information for improved performance, while multi-modal biometric authentication enhances security and reliability. With these advancements, face recognition technology continues to evolve, opening up new possibilities across various industries.

Challenges in Face Recognition

Face recognition technology has come a long way, but it still faces several challenges that researchers and developers continuously strive to overcome. These challenges primarily stem from the inherent variability in facial appearance, illumination and pose variations, occlusion and expression changes, as well as spoofing and anti-spoofing techniques. Understanding and addressing these challenges is crucial for developing accurate and reliable face recognition systems. One of the fundamental challenges in face recognition is the variability in facial appearance. People exhibit a wide range of facial characteristics, including different skin tones, facial structures, and ethnicities. Additionally, factors like age, facial hair, and hairstyle contribute to the diversity in facial appearance. Such variability poses a significant challenge to face recognition systems, as they must be robust enough to accurately match faces across these differences.

Another challenge is the impact of illumination and pose variations. Lighting conditions can vary significantly, leading to changes in facial shadows, highlights, and color distributions. These variations can significantly affect the accuracy of face recognition algorithms since they rely on consistent and reliable patterns in facial appearance. Similarly, pose variations, such as changes in head orientation, pose angles, and facial expressions, make the recognition task more challenging. Recognizing a face under extreme pose angles or unusual expressions requires sophisticated algorithms capable of handling these variations.

Occlusion and expression changes are additional challenges faced by face recognition systems. Occlusion occurs when an object or another person partially blocks the view of a face, making it difficult for the system to capture all the necessary facial features for recognition. Common examples include wearing glasses, headwear, or facial masks. Expression changes are another challenge, as individuals can exhibit a wide range of emotions and facial expressions that alter the appearance of key facial features. Addressing occlusion and expression changes requires the development of algorithms that can handle incomplete or distorted facial data and robustly recognize faces despite these challenges.

Spoofing, or presentation attack, is a significant security concern in face recognition. Spoofing refers to fooling the system by presenting fake biometric traits, such as photographs, videos, or masks, with the intention of impersonating someone else. This vulnerability jeopardizes the security and integrity of face recognition systems. To counteract spoofing, anti-spoofing techniques have been developed. These techniques aim to detect the difference between a live face and a fake one by analyzing various factors like texture, motion, or infrared heat signatures. However, developing effective anti-spoofing

techniques that can reliably distinguish between real and fake faces remains an ongoing challenge. Face recognition technology faces various challenges that researchers and developers continuously work on to improve accuracy, reliability, and security. Variability in facial appearance, illumination and pose variations, occlusion and expression changes, and spoofing and anti-spoofing techniques pose significant hurdles. Addressing these challenges is essential for advancing face recognition technology and enabling its seamless integration into various domains like security, access control, and identification systems. By overcoming these challenges, we can develop more robust and reliable face recognition systems that can operate effectively in real-world scenarios.

Security and Privacy Concerns

As face recognition technology becomes more prevalent in our society, it brings about various security and privacy concerns that need to be carefully addressed. This passage will discuss the vulnerabilities and threats faced by face recognition systems, the privacy implications and ethical considerations associated with their usage, as well as the legal and regulatory aspects that govern their deployment.

One of the primary concerns regarding face recognition systems is the potential vulnerabilities and threats they face. Like any technology, face recognition systems can be susceptible to attacks and exploitation by malicious actors. For instance, attackers may attempt to spoof the system by presenting a fake face or using manipulated images or videos to gain unauthorized access. Such vulnerabilities highlight the importance of robust anti-spoofing techniques and continuous system updates to counteract potential attacks. Moreover, privacy implications pose a significant concern when deploying face recognition systems. These systems generate extensive datasets containing people's biometric information, raising questions about the collection, storage, and usage of such data. The potential of unauthorized access or misuse of this data can result in significant privacy breaches, leading to identity theft or unlawful surveillance. Therefore, it is crucial to implement stringent security measures to protect this sensitive data, such as encryption and secure storage protocols.

Ethical considerations also come into play when discussing face recognition technology. There are concerns related to consent, surveillance, and the potential for discrimination or bias in the decision-making process. Individuals may not always be aware that their faces are being captured and processed, leading to a lack of informed consent. Additionally, excessive or indiscriminate use of face recognition for surveillance purposes can undermine privacy rights and create a culture of constant tracking. The reliance on algorithms for decision-making may also introduce biases, leading to unfair treatment or discrimination against certain individuals or groups. Developers and organizations need to address these concerns by ensuring transparency, accountability, and fairness in the design and deployment of face recognition systems.
From a legal and regulatory perspective, the use of face recognition technology is subject to jurisdiction-specific laws and guidelines. Some countries have enacted legislation to govern the collection, processing, and storage of biometric data. These laws aim to strike a balance between promoting innovation and protecting individual privacy rights. Organizations deploying face recognition systems must comply with applicable regulations, obtain necessary permissions, and implement privacy-by-design principles from the inception of their systems. Furthermore, legal frameworks must also consider the potential misuse and consequences of face recognition technology. Regulations should address issues like data sharing, data retention policies, and the need for user consent. Additionally, laws should encompass strict accountability measures for any breaches or misuse of data, as well as clear protocols for individuals to exercise their rights regarding their biometric information.

The security and privacy concerns surrounding face recognition technology are multifaceted and crucial to address for its responsible deployment. Vulnerabilities and threats associated with spoofing and unauthorized access need continuous mitigation. Privacy implications and ethical considerations, such as consent, surveillance, and bias, must be carefully explored and addressed in the design and deployment of face recognition systems. Furthermore, legal and regulatory frameworks need to provide clear guidelines to protect individual privacy rights, govern data collection and usage, and establish accountability measures. By addressing these concerns comprehensively, we can ensure the responsible and secure use of face recognition technology while upholding privacy rights and ethical principles.

Future Directions and Research Opportunities

Face recognition technology has made significant strides in recent years, transforming various aspects of our lives, from unlocking our smartphones to improving surveillance systems. However, there are several avenues for future research and development that can further enhance this technology. One promising direction is the improvement of accuracy and robustness. While face recognition algorithms have achieved remarkable accuracy rates, they can still struggle in challenging real-world scenarios, such as low lighting conditions or occlusions. Researchers can delve into developing more advanced algorithms that can handle these complexities. Incorporating deep learning techniques and convolutional neural networks can potentially improve recognition accuracy and handle various environmental factors.

Another area of interest lies in the development of real-time face recognition systems. Current face recognition solutions often require pre-trained models or complicated offline processing, making them less suitable for real-time applications. Researchers can explore real-time algorithms that efficiently process and match faces in real-time, enabling applications like instant identity verification at airports or crowd monitoring at events.

Mitigation of Challenges and Vulnerabilities:
While face recognition technology offers substantial benefits, it also poses certain challenges and vulnerabilities that need to be mitigated. One pressing challenge is the issue of bias in face recognition algorithms. Studies have shown that these algorithms may be less accurate in correctly identifying individuals from minority groups or diverse ethnic backgrounds. Addressing this bias requires collecting diverse datasets, more comprehensive training approaches, and constant monitoring and evaluation of the algorithms for fairness. Another vulnerability in face recognition technology is spoofing or presentation attacks. These attacks involve presenting fake facial images or disguises to deceive the system. Researchers can focus on developing countermeasures to detect and prevent spoofing attempts, such as analyzing depth information, thermal imaging, or incorporating liveness detection techniques.

Integration with other Emerging Technologies:
Face recognition technology has the potential to synergize with other emerging technologies to create more powerful and effective solutions. Integration with augmented reality (AR) and virtual reality (VR) can enhance user experiences by enabling personalized interactions and immersive simulations. For example, AR glasses equipped with face recognition technology can provide real-time information about people surrounding the wearer, enhancing social interactions and information sharing. Furthermore, integrating face recognition with Internet of Things (IoT) devices can offer improved security and personalization in various settings. Smart homes can leverage face recognition to customize lighting, temperature, and entertainment preferences for different individuals. Similarly, integrating face recognition with autonomous vehicles can enhance safety by enabling driver identification for access control and personalization of settings.

Ethical Frameworks and Regulatory Measures:
With the rapid advancement of face recognition technology, it is crucial to establish ethical frameworks and regulatory measures to ensure responsible and accountable deployment. Privacy concerns arise due to potential misuse of face recognition for mass surveillance or unauthorized tracking. Setting clear guidelines regarding data collection, storage, and sharing will safeguard individuals' privacy rights while allowing legitimate uses of the technology for security or public welfare. Additionally, efforts should be made to safeguard against the potential misuse of face recognition technology for discriminatory purposes or invasive surveillance. Development of unbiased algorithms, transparency in system decision-making processes, and regular external audits are essential to prevent unintended consequences and maintain public trust.
Furthermore, collaboration between various stakeholders, including researchers, policymakers, industry leaders, and privacy advocates, is crucial to establishing comprehensive and globally accepted ethical standards. Regular discussions and international cooperation can help create a harmonized approach to face recognition technology regulation that balances security, privacy, and societal values. Future directions and research opportunities in face recognition technology encompass improving accuracy and real-time capabilities, mitigating challenges such as bias and spoofing, integrating with emerging technologies, and implementing ethical frameworks and regulatory measures. By addressing these areas, researchers and policymakers can ensure the responsible development and deployment of face recognition technology that benefits society while maintaining privacy and fairness.

CONCLUSION

This research paper has shed light on the current state and future possibilities of face recognition technology within biometric authentication systems. It has summarized key findings pertaining to advancements in algorithms, the integration of deep learning techniques, emerging trends, and the challenges faced by this technology. Biometric authentication systems, particularly face recognition technology, have become increasingly important in providing secure and user-friendly authentication solutions. The advancements in face recognition algorithms have led to improved accuracy and efficiency in recognizing and verifying individuals based on their facial features. The integration of deep learning techniques has further enhanced the performance of these systems, enabling them to learn from vast datasets and adapt to variations in facial appearance.

The paper highlighted emerging trends in face recognition, such as the application of artificial intelligence, real-time and high-resolution image processing, 3D face recognition, and multi-modal biometric authentication. These trends offer exciting possibilities in various domains, ranging from personalized experiences in gaming and communication to enhanced security measures in healthcare and smart homes. The challenges in face recognition, including variability in facial appearance, illumination and pose variations, occlusion and expression changes, as well as spoofing and anti-spoofing

techniques, have been identified. Addressing these challenges through research and innovation is crucial for the continued advancement and reliability of face recognition technology.

Furthermore, the paper emphasized the importance of considering security and privacy concerns associated with biometric authentication systems. Vulnerabilities and threats to face recognition systems should be mitigated, and privacy implications and ethical considerations must be addressed. The establishment of legal and regulatory frameworks is necessary to ensure responsible and accountable use of this technology, protecting individuals' rights and preventing potential misuse. Moving forward, future directions and research opportunities lie in advancing face recognition technology for increased accuracy, efficiency, and real-world performance. Mitigating challenges and vulnerabilities, such as bias, privacy invasion, and security risks, should be a priority. Additionally, integrating face recognition technology with other emerging technologies, such as artificial intelligence, augmented reality, virtual reality, and biometrics, will unlock new potentials and applications. This research paper has also provided valuable insights into the trends and challenges within this field. The findings underscore the importance of continued research and development to harness the benefits of this technology while

REFERENCES

[1]. Bowyer, K. W., Chang, K. I., Yan, P., & Flynn, P. J. (2007). Multi-Modal Biometrics: An Overview. IEEE Transactions on Information Forensics and Security, 2(3), 297-314.
[2]. Daugman, J. (2004). How Iris Recognition Works. IEEE Transactions on Circuits and Systems for Video Technology, 14(1), 21-30.
[3]. Espinoza, M., Champod, Ch., & Margot, P. (2011). Vulnerabilities of fingerprint reader to fake fingerprints attacks.
[4]. Jain, A. K., Hong, L., & Pankanti, S. (2000). Biometric identification. Communications of the ACM, 43(2), 90-98.
[5]. Jain, A. K., Ross, A., & Prabhakar, S. (2004). An introduction to biometric recognition. Volume: 14 Issue: 1, 4-20.
[6]. Jain, A. K., Ross, A., & Pankanti, S. (2006). Biometrics: A tool for information security. Volume: 1 Issue: 2, 125-143.
[7]. Matyas, V., & Riha, Z. (2010). Security of biometric authentication systems.
[8]. Prabhakar, S., Pankanti, S., & Jain, A. K. (2003). Biometric Recognition: Security and Privacy Concerns. IEEE Security & Privacy, March/April, 33-42.
[9]. Ratha, N. K., Connell, J. H., & Bolle, R. M. (2006). Recent advances in biometrics: a survey. IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews, 36(3), 303-316.
[10]. Ross, J. D., Jain, A., & Bolle, R. (2006). The ideal biometric trait. IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews, 36(3), 303-316.
[11]. Schuckers, M. E. (2001). Some Statistical Aspects of Biometric Identification Device Performance.
[12]. Saeed, K., Pejas-Romuald, J., & Mosdorf, R. (2006). Biometrics, Computer Security, Systems and Artificial Intelligent Applications.
[13]. Sharma, S. K., Plataniotis, K. N., & Venetsanopoulos, A. N. (n.d.). Recent developments in biometrics on edge: a review.
[14]. Tistarelli, M., & Nixon, M. (2009). Advances In Biometrics. Springer-Verlag Berlin Heidelberg 2009.
[15]. "Biometric recognition: challenges and opportunities" (2010). Retrieved from http://www.nap.edu/openbook.php?record-id=12720&page=2