BOOK CHAPTER | The More You Look !

Image-assisted Biometric Identification

Rasheed Abubakar Ayanaba
Digital Forensics and Cyber Security Graduate Programme
Department of Information Systems & Innovations
Ghana Institute of Management & Public Administration
Greenhill, Accra, Ghana
E-mail: rasheed.ayanaba@st.gimpa.edu.gh
Phone: +233246997782

ABSTRACT

Biometrics is a rapidly developing technology that has seen widespread use in forensics applications such as criminal identification, secure access, and prison security. A biometric system is a pattern recognition system that recognizes a person by determining the authenticity of a physiological and/or behavioural feature that that person possesses. One of the most widely accepted biometrics utilized by humans in their visual interactions is image- assisted based (facial) biometric. Image-assisted biometric identification is the use of face recognition technology in capturing image of a unique feature of an individual such as an eye or face, and comparing it with a template captured earlier and stored a database. Face recognition is one of the more recent biometrics technologies. The system examines face features and tries to match them to a database of digitized images. This technology is quite new, having only been available commercially since the 1990s. Face recognition has gotten a lot of press after the 9/11 attacks because of its capacity to identify known terrorists and criminals. [1]. Although the technology is mostly utilized for security and law enforcement, there is growing interest in other applications.

Keyword: Image-assisted based biometric identification, Face recognition technology, Image

BOOK Chapter | Research Nexus in IT, Law, Cyber Security & Forensics. Open Access. Distributed Free

Citation: Rasheed Abubakar Ayanaba (2022): Image-assisted Biometric Identification
Book Chapter Series on Research Nexus in IT, Law, Cyber Security & Forensics. Pp 131-138
www.isteams.net/ITlawbookchapter2022. dx.doi.org/10.22624/AIMS/CRP-BK3-P22

1. INTRODUCTION

Image-assisted biometric identification is a facial recognition technology used in verifying a person's identity by using their face. People can be identified in pictures, films, or in real time using facial recognition technology. [1] Similar systems were first developed in the 1960s as a type of computer application. Facial recognition systems have been used on smartphones and in other types of technology, such as robotics, since their beginnings. Computerized facial recognition systems are classified as biometrics since they involve the measurement of a person's physiological properties.

Although facial recognition systems are less accurate than iris and fingerprint recognition as biometric technologies, they are commonly used due to their contactless nature. Advanced human–computer interface, video surveillance, and automatic picture indexing have all used facial recognition systems.

Governments and private organizations use facial recognition technologies all around the world nowadays. Their performance varies, and certain solutions have been abandoned in the past due to inefficiency. Face recognition systems have also sparked debate, with concerns that they breach residents' privacy, frequently make inaccurate identifications, promote gender stereotypes and racial profiling, and fail to secure crucial biometric data. Face recognition technology have been banned in some US localities as a result of these allegations. Meta announced that it planned to shut down Facebook's facial recognition system, wiping the face scan data of over one billion users, in response to mounting societal concerns. This move will be one of the most significant in the history of facial recognition. [2]

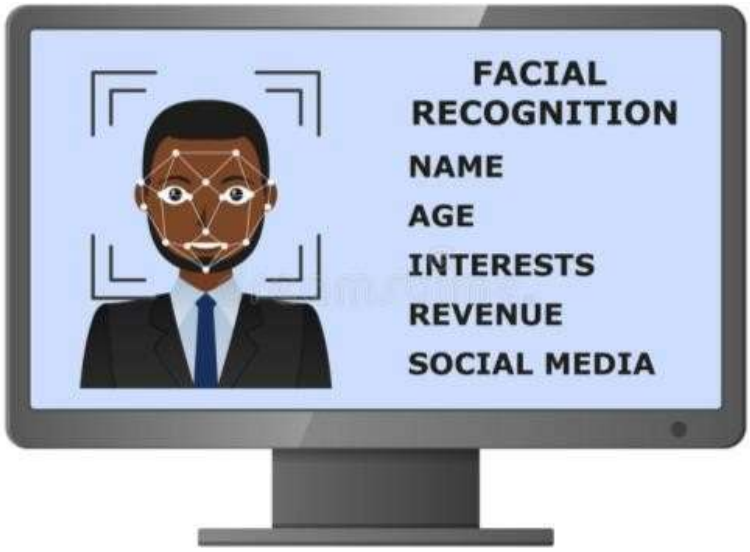

Figure 1: facial recognition Systems Components
Source: https://www.dreamstime.com/

1.1 Background to the Study

Face recognition has gotten a lot of attention in recent decades because of the growing demand for it in security applications like video surveillance and biometric surveillance. Security systems with facial recognition capacity are being installed in modern facilities such as hospitals, airlines, banks, and many other organizations. Despite its current success, research into making facial recognition systems faster and more accurate is still underway. Any face recognition system's accuracy is highly dependent on the face detection mechanism. The recognition system would be better if the facial detection mechanism was stronger. A face detection system can successfully detect a human face from a given image comprising one or more faces, as well as from live video with human presence. The most common methods for detecting faces nowadays. Image-based technique employed some face patterns and processed training photos to distinguish between face and non-face.

The feature-based method was chosen since it is both faster and easier to implement than the image-based method. Image processing is used to recognize faces in a photograph. Because photos contain not only human faces but also non-face items in clutter settings, locating faces from images is not an easy task. There are many other challenges with face recognition, such as illumination, facial orientations, and skin colours. Because of these factors, no face recognition system can be completely accurate. One of the most essential biometrics methods is face recognition. Despite the fact that more reliable biometric recognition techniques, such as fingerprint and iris recognition, exist, these techniques are obtrusive and rely heavily on user participation for success. As a result, it appears that facial recognition is the most global, non-intrusive, and accessible technology. It is simple to operate and can be used effectively for mass scanning, which is problematic with conventional biometrics. It's also natural and socially acceptable. [3]

Furthermore, technologies that need numerous people to utilize the same equipment to collect their biological traits are likely to expose the user to infections and pollutants from other people. Face recognition, on the other hand, is absolutely non-intrusive and has no health risks. Biometrics is an area of information technology that is quickly evolving. Biometric technologies are computer- assisted methods of identifying people based on their biological and behavioural traits. When compared to traditional means of identification, biometric technologies have significant advantages. Countries are examining these benefits and transitioning to new generation identification systems based on biometric technologies to take necessary safeguards against rising security dangers in the modern world. [3]

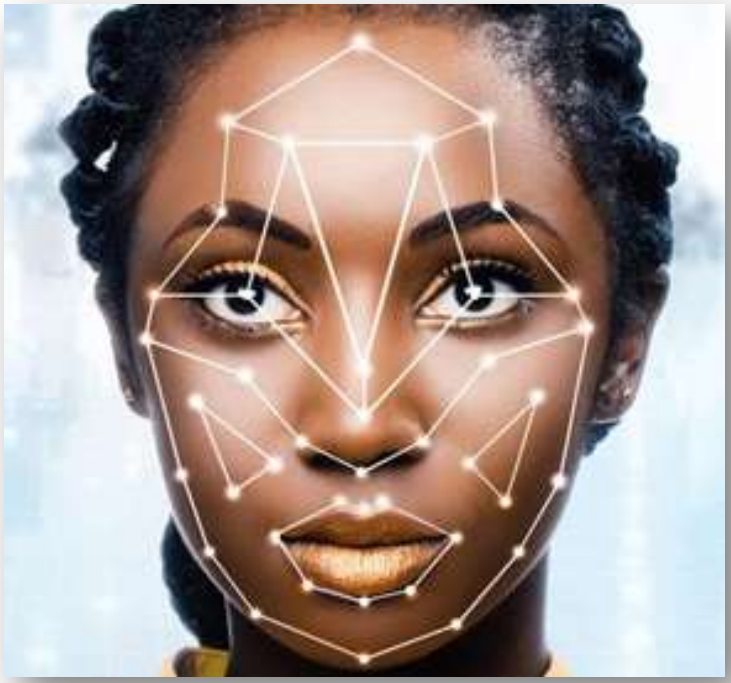

Fig 2: Nodal Face Sections in the Recognition Process
Source: TD-Face-recognition Technology

2. RELATED LITERATURE

What follows is a tabular outlook for reviewed literature

Table 1: Related Works and Findings

Documents	Authors	Works on Image-assisted based Biometric Identification
Facial Recognition: An Introduction	Elena Beretta & Nasir Muftić	This article provides a brief history of facial recognition system and also describes how the technology works.
FERET (Face Recognition Technology) Recognition Algorithm Development and Test Results	P. Jonathon Phillips, Patrick J. Rauss, and Sandor Z. Der	The US Army Research Laboratory (ARL) conducted supervised government tests and evaluations of automatic face recognition algorithms as part of the Face Recognition Technology (FERET) program. The tests were designed to give an objective technique for evaluating algorithms and determining the state of the art in automatic facial recognition. The FERET tests were conducted in August 1994 and March 1995, and the results are presented in this report. The results of ARL's FERET tests conducted between August 1994 and August 1996 are presented.
Facial Recognition Technology	Lucas D. Introna and Helen Nissenbaum	Facial recognition technology (FRT) has emerged as an attractive solution to address many contemporary needs for identification and verification of identity claims. This report develops a socio-political analysis that bridges the technical and social-scientific perspectives on FRT. It highlights the potential and limitations of the technology.
Research on Face Recognition and Privacy in China—Based on Social Cognition and Cultural Psychology	Tao Liu*, Bijiao Yang, Yanan Geng and Sumin Du	The privacy concerns of face recognition have become the most critical social issue in the era of information sharing. Most users will still choose to provide personal information in exchange for services and applications they need. Trust in technology and platforms can reduce users' intention to put up guards against them.
Literature Review : Implementation of Facial Recognition in Society'	M I Zarkasyi , M R Hidayatullah and E M Zamzami	Facial recognition technology (FRT) has emerged as an attractive solution to address many contemporary needs. This report develops a socio-political analysis that bridges the technical and social scientific literature on FRT. It highlights the potential and limitations of the technology, noting those tasks for which it seems ready for deployment.

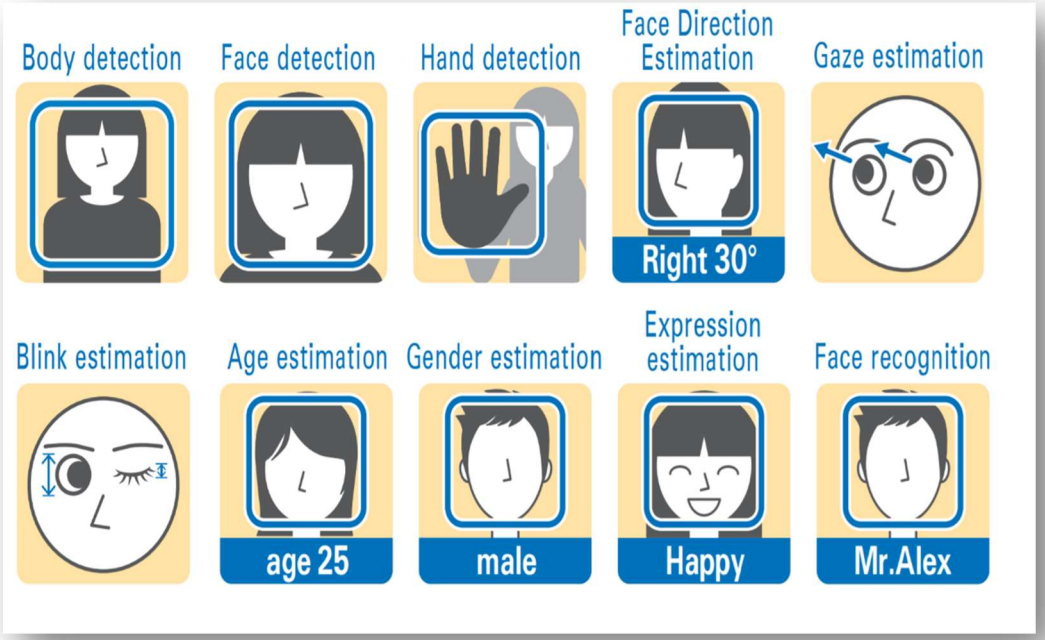

Fig 3: Sequences of the Face Recognition Process
Source:https://www.electronicsweekly.com/market-sectors/internet-of-things/farnell-ships-omrons-facial-recognition-system-2019-06/

3. RESEARCH GAP/FINDINGS

Face recognition privacy problems have become the most pressing societal issue in the age of information sharing, thanks to the advancement of big data technology. This study examines the privacy of face recognition and influencing factors based on perceived ease of use, perceived usefulness, social cognition, and cross- cultural features. My findings show that when consumers believe their personal information is at risk via face recognition, they are more concerned about privacy. However, the majority of users will prefer to exchange personal information. [20]

4. CONCLUSION

Although face recognition technology has a number of advantages for society, federal legislation is needed to maintain uniformity across the country and to ensure that all citizens have their privacy protected from unwelcome government or commercial interference. The current state legislation is a step in the right direction, but there is still a growing need for federal legislation that ensures that all individuals have an equal right to privacy. Only federal regulations that directly address the troubling aspects of facial recognition technology and provide citizens with responsibility, transparency, and privacy will be able to do this.

5. RECOMMENDATION FOR POLICY AND PRACTICES

To ensure proper use of facial recognition technology, the following recommendations should be considered;

Recommendation 1: The security and law enforcement agencies should test its facial recognition system for accuracy and racially discriminatory mistake rates and publish the results. All persons should be treated equally by facial recognition technology. [5]

Recommendation 2: Check for algorithmic bias based on race, gender, and age internally. [5]

Recommendation 3: Call on local, state, tech companies and law enforcement agencies, as well as the FBI, to be more transparent and to implement policies that respect privacy, civil liberties, and civil rights. The capabilities and limitations of technology should be documented by tech businesses, security and law enforcement agencies. [5]

Recommendation 4: Any use of facial recognition by law enforcement should be subject to public reporting and internal examinations. [5]

Recommendation 5: A facial recognition system act should be enacted to regulate all activities of facial recognition technologies [5]

Recommendation 6: To ensure responsible use of facial recognition technology, Tech companies, security and law enforcement agencies must adhere to the framework documented by the World Economic Forum, in partnership with the International Criminal Police Organization (INTERPOL), the Centre for Artificial Intelligence and Robotics of the United Nations Interregional Crime and Justice Research Institute (UNICRI) and the Netherlands police,

6. DIRECTION FOR FUTURE WORKS

Face recognition is a new technology that has a lot of potential. Face recognition may help businesses save money and time, as well as establish new revenue streams, if done correctly. What does the future hold for this technology? It's tough to know for sure. According to some experts, our faces will eventually replace IDs, passports, and credit card pin numbers. This prediction is not far-fetched, given how easy and cost-effective this technology is.
If this prediction comes true, any company that adopts the technology now will have a competitive advantage in the future.

7. IMPLICATIONS FOR CYBER SAFETY IN AFRICA

Africa is among the world’s fastest-growing economies. In terms of population, economics, and worldwide importance, it is rapidly expanding. Africa now has a population of 1.21 billion people (up from 800 million in 2000), with the world's youngest population at 19.5 years. With the rise of youth comes a diversified population seeking meaningful work, social participation, freedom of expression, and enhanced global connectivity. Mobile device ownership is increasing at an exponential rate, social media usage is increasing, and the Internet of Things (IoT) is rapidly becoming a reality. [21]

The development of the Internet in Sub-Saharan African countries is crucial for the region's economic development. However, as Internet connectivity improves, so does cybercrime. Cybercriminals have additional opportunity to participate in online crime as Internet connectivity becomes more widely available, faster, and cheaper. Fraudsters who participate in Nigerian-style scams or romantic fraud, for example, can reach a larger number of prospective victims all over the world. [20] Furthermore, many computers in the region are not patched on a regular basis and lack antivirus protection, resulting in a swarm of unprotected or underprotected workstations that fraudsters can easily herd together into botnets. Cybercrime cost African nations $3.5 billion in 2017, according to Kenya-based IT and business advice firm Serianu. Nigeria's yearly cybercrime damages were assessed to be $649 million in that year, while Kenya's losses were anticipated to be $210 million. South Africa loses $157 million each year due to cyberattacks, according to the South African Banking Risk Information Centre (SABRIC). [19]

Most common cybercrime incidents in Africa includes; cyber fraud, mobile money (momo) fraud, identity fraud (romance fraud), blackmail, hacking, Ransomware attacks, sim box fraud, phishing, fake gold dealers, cyber bullying, Child pornography, insider attackers, network attacks etc. [19]

Vulnerable systems and insufficient cybersecurity policies are to blame for the continent's rising cyberattacks. According to the Business Software Alliance, the two African countries with the greatest rates of software piracy in 2017 were Libya and Zimbabwe. In both countries, the percentages of unlicensed software were 90% and 89 percent, respectively. Because pirated software packages are unable to receive manufacturer updates, malware transmission is accelerated. Another issue is that Internet users lack the necessary abilities to protect themselves from fast evolving cyber-threats. Many African Internet users, like those in other developing nations, lack experience and technical knowledge. The surge in cybercrime activities in Africa is also due to weak regulation and law enforcement. Most African economies are characterized by regulatory frameworks that are lax, providing ideal ground for cybercrime. [19] Cyber-threats are becoming more prevalent in African economies. This development emphasizes the significance of bolstering cybersecurity safeguards. This means that businesses must invest more in cybersecurity technologies, provide cybersecurity training to staff, and hire CISOs. It's also critical to raise customer awareness about cybersecurity. [19]

Policymakers on the continent should work on raising public knowledge of cybersecurity practices as well as boosting regulatory and enforcement capacities. Policymakers on the continent should concentrate on raising public knowledge of cybersecurity practices as well as boosting regulatory and enforcement capacities. Organizations must be required to implement and amend regulations requiring effective cybersecurity safeguards. Initiatives should also concentrate on improving law enforcement capabilities in order to strengthen the certainty of punishment for cybercriminals. [19]

REFERENCE

[1] https://www.kaspersky.com/resource-center/definitions/what-is-facial-recognition
[2] https://en.wikipedia.org/wiki/Facial_recognition_system
[3] Elena Beretta & Nasir Mufti? https://www.internetjustsociety.org/cosmonaut/facial-recognition-an- introduction
[4] Blaine Frederick https://www.techopedia.com/definition/32071/facial-recognition
[5] Clare Garvie https://www.perpetuallineup.org/recommendations
[6] http://what-when-how.com/face-recognition/introduction-to-face-recognition-part-1/
[7] Lucas D. Introna and Helen Nissenbaum, Facial Recognition Technology A Survey of Policy and Implementation Issues
[8] Insaf Adjabi, Abdeldjalil Ouahabi , Amir Benzaoui and Abdelmalik Taleb-Ahmed, Past, Present, and Future of Face Recognition: A Review. https://hal.archives-ouvertes.fr/hal-03140632
[9] Mattias Junered, Face Recognition in Mobile Devices. http://www.diva-portal.org/smash/record.jsf?pid=diva2%3A1030155&dswid=-1034
[10] M I Zarkasyi et al 2020 J. Phys, Literature Review : Implementation of Facial Recognition in Society. https://iopscience.iop.org/article/10.1088/1742-6596/1566/1/012069/meta
[11] https://www.frontiersin.org/articles/10.3389/fpsyg.2021.809736/full
[12] Cahit Gürel (2011), Development Of A Face Recognition System. https://www.researchgate.net/publication/265026957_DEVELOPMENT_OF_A_FACE_RECOGNITION_SYSTEM
[13] https://us.norton.com/internetsecurity-iot-how-facial-recognition-software-works.html
[14] https://www.nytimes.com/wirecutter/blog/how-facial-recognition-works/
[15] https://www.aclu.org/issues/privacy-technology/surveillance-technologies/face-recognition-technology
[16] https://www.itpro.com/security/privacy/356882/the-pros-and-cons-of-facial-recognition-technology
[17] https://www.nec.co.nz/market-leadership/publications-media/a-brief-history-of-facial-recognition/
[18] Mohammad Ahmadi, Ph.D. Global Privacy Concerns of Facial Recognition Big Data". https://scholar.utc.edu/cgi/viewcontent.cgi?article=1299&context=honors-theses
[19] Nir Kshetri, Cybercrime and Cybersecurity in Africa https://www.tandfonline.com/doi/full/10.1080/1097198X.2019.1603527
[20] Caroline Baylon and Albert Antwi-Boasiako, Increasing Internet Connectivity While Combatting Cybercrime: Ghana as a Case Study. https://www.cigionline.org/publications/increasing-internet-connectivity-while-combatting-cybercrime-ghana-case-study/
[21] Cyber Crime & Cyber Security Trends In Africa, https://securitydelta.nl/media/com_hsd/report/135/document/Cyber-security-trends-report-Africa-en.pdf