An Exploratory Study Into The Face Detection And Recognition System To Strengthen Security Precautions Using An Artificial Intelligence System

Ibrahim Ali Mohammed
DevOps Consultant
Dell, India

Abstract— The main aim of this study is to explore how AI can be implemented in Face Detection and Recognition Systems for security purposes. Security is an important aspect of everyday activities. Every organization, institution, or residential place needs security to protect its property, business, and people. Technology has been an important resource in ensuring there is high security in many places. The use of technology has rapidly changed from not only solving problems but also acting as a purpose-driven entity in everyday operations. Decades ago, technology only revolved around computer networks, wired telephones, emails, and the internet. However, advances in technology have seen tremendous progress in its roles in our communities [1]. Artificial intelligence and facial recognition are emerging as indispensable resources in the advancement of technology in security. They are already replacing the often-burdensome human resources in critical security applications. This paper hopes to explore how AI and face recognition work together to ensure there is high security in various places. Face recognition has proven to be an important resource in many areas especially in law enforcement. The police can use face recognition to identify victims of human trafficking and missing persons [1,2]. Criminals can also be added to a facial recognition database to identify them when they appear in public places where there are CCTV cameras especially the airports and public stores. Other roles that facial recognition can play are the identification of shoplifters, fraudulent people in stores, and organized criminal gangs [3]. There is no doubt that technology is playing a significant role in recognizing potential criminals and helping protect our communities.

Keywords— Face recognition, artificial intelligence, face detection, predictive analytics, Authentication

I. INTRODUCTION

Facial recognition can be described as a method of identifying people using their facial features. It is not just a mere science fiction that we see in many movies because its role in real life is gaining a lot of attention. Many businesses are embracing the use of facial recognition to protect their property in various ways. The use of CCTVs has been impactful in recognizing criminals and deterring any attacks. The integration of artificial intelligence has made advanced changes to the facial recognition system through the identification and verification of persons from videos and digital images. These systems can quantify various aspects of human faces, analyze their expressions, and the extraction of their demographic information. It is also capable of managing the security systems and giving interactive engagement to the user especially communicating the match through an audio system[3]. Face recognition is becoming popular in image analysis. Face detection is one aspect that is most promising in face recognition owing to its computation mechanisms that utilize advanced algorithms in identifying people [4].

Face detection can be described as a computational technique integrated with artificial intelligence to identify people using their facial expressions and behaviours. This technique is effective in tracking and monitoring facial features from many angles and relaying the information through a video or image display in real-time. It is also very effective when connected to a biometric detection system [4,5].

Face detection is only the first step in identifying people captured by cameras. The full process involves other applications and algorithms in tracking, analyzing, and matching the identified person with the information in the database. Face detection generally has a substantial impact on the subsequent processes and the results in the recognition system. Its accuracy can be improved by focusing on specific areas of an image or video and other aspects especially the emotions, gender, or age [5]. The most important thing is to build a faceprint by mapping a person's facial features with the data already stored in the database. Algorithms play an important role in matching the facial features from the video or image to the data in the database t[6]. A human face has a lot of variability that can make it difficult to detect their features using photographs. Some of these variabilities include their pose, skin color, image resolution, facial hair, orientation, lighting conditions, wearing glasses, position, and expression [6].

This paper will help in understanding how Artificial intelligence can work in improving the capabilities of facial recognition systems, especially in security applications. Artificial intelligence simplifies the process of facial recognition through its algorithms scanning and verifying facial features. Many companies have already utilized face recognition systems in identifying people. These include Google, Facebook, and Microsoft. The use of face recognition is important in online transactions, banking systems, security, business transactions, and criminal systems [7].

II. RESEARCH PROBLEM

The main problem that this study will solve is to explore how AI can be integrated into face recognition systems for security purposes. With an increase in criminal activities in many areas of the world, facial recognition is proving to be an important resource in deterring and minimizing these challenges. Cyber security is now grubbing with a lot of security problems involving billions of losses in resources and financial burdens to many businesses, people, and the globe as a whole.IT systems are becoming vulnerable every day as criminals identify new ways of penetrating them with ease. Some of these systems are sensitive especially the banks, intellectual property, and businesses. The application of face recognition is proving to be significant but more needs to be done to reinforce its capabilities [8]. One of these reinforcements is the use of artificial intelligence which utilizes sophisticated algorithms in computational tasks of matching the captured information with that in the database system. Law enforcement is finding it easy to match mugshots using facial recognition database systems. This has allowed a seamless partnership between the local, state, and federal agencies in the fight against criminal activities [8].

III. LITERATURE REVIEW

A. What Is Facial Recognition?

Face recognition is a technological advancement utilizing AI to identify people based on their facial features. It can be described as an advanced form of biometric identification of people using their facial features and matching them to images and videos already stored in a biometric database. This technology is common in law enforcement especially the FBI database for criminals. This has become popular in many jurisdictions in the U.S. owing to its efficiency in identifying and arresting criminals captured by many cameras installed in streets and buildings [9]. For many decades, law enforcement officers have used mugshots to match criminals with profiles stored at the local, state, and federal level databases. Every time a criminal is arrested, their profiles are stored in facial recognition databases to identify them the next time they commit a crime. This will be scanned and stored for future reference against any criminal activities. Law enforcement officers are also collecting criminal data using their mobile face recognition. Devices like tablets, and smartphones are proving to be effective in identifying traffic offenders by matching them with profiles of frequent offenders in the database [10]. Facial recognition is also common in public places like airports, shopping centres, and recreational facilities. The increase in the number of travellers can be a nightmare in the fight against criminal activities on a national and international level. Facial recognition allows for easy identification of people who are targeted by national and international law enforcers. With the increased popularity of biometric passports, facial recognition systems are helping security personnel in airports to identify any suspicious people [11]. What makes facial recognition unique is its security features which can be changed easily. It's not easy to change someone's facial features once it is captured on camera. Face recognition systems are also highly sophisticated and with high accuracy especially when used on smartphones and unlocking personal devices [11].

B. How Facial Recognition Works

Facial recognition works by capturing and matching the facial features of a person using AI and ML algorithms. Once the image of a person is captured, they are sent to a detection system where the algorithms search for unique features from the background [11,12]. Some of the facial features that are usually checked include the nose, eyebrows, nostrils, mouth, and iris. The captured features are then validated utilizing large datasets which will start by confirming that the captured image is that of a human being. In addition to feature-based facial recognition, other aspects are considered which are knowledge-based and template matching. For feature-based methods, common features of a face are captured especially, the eyes and nose. Its outcome may have variabilities especially when there is noise and light in the system. A statistical analysis will be applied utilizing machine learning algorithms which will identify any characteristics that can match those in the database system [12]. A knowledge-based method utilizes predefined rules in making a match between a captured image to that in the database system. One challenge with this approach is the need for well-defined rules. Lastly, template matching utilizes a correlation mechanism to compare the captured face to those stored in the database system. Some of the challenges facing this method are the variations in results due to scalability, posing, and shape of a face.

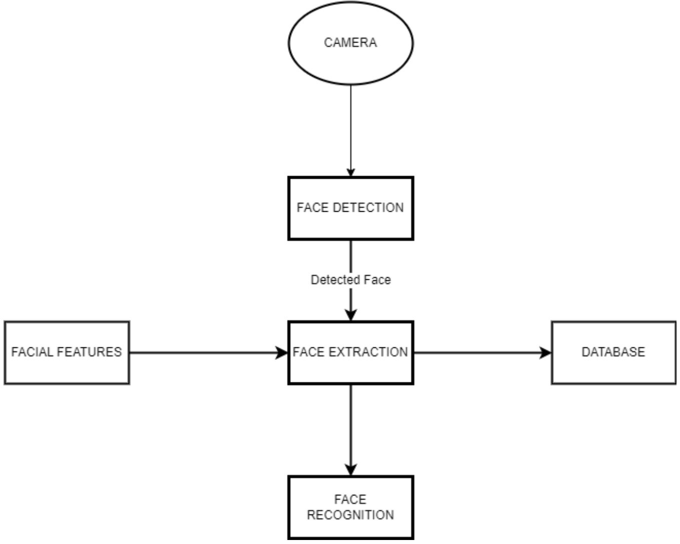

Fig i: Steps in a facial recognition system

C. Artificial intelligence in facial recognition systems

Artificial intelligence is becoming an important technological advancement in security systems. This resource is advancing the capabilities of human intelligence through algorithms and machine learning in making decisions. This technology is gaining a lot of attention in facial recognition systems, especially on mobile devices, smart homes, CCTVs, and self-driving vehicles [12,13]. AI leverages unstructured data in making informed patterns on the information captured from external resources like cameras and sensors. This information is then correlated to the information already stored in the database systems to provide the match. The AI system is programmed to compute, analyze, and make cognitive decisions. It utilizes other automated resources like machine learning, neural networks, and deep learning in making these cognitive decisions[14].

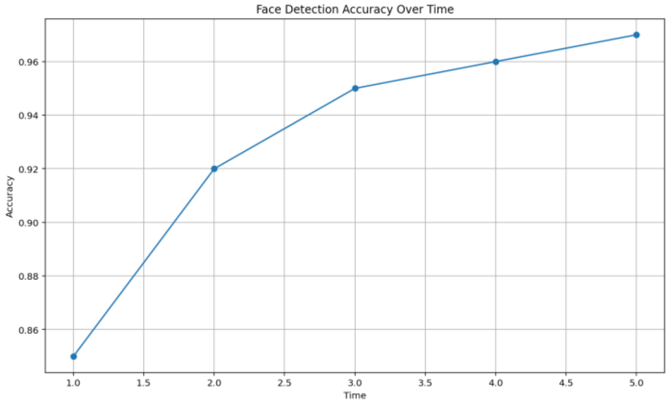

Fig ii: Facial recognition accuracy over time

Many studies have shown how AI can be an important technology in many areas and applications. Image recognition is one of the areas where AI is gaining a lot of popularity. Some of the other applications include speech recognition, chatbots, sentiment analysis, and natural language recognition. AI is a technology that will change the future in many aspects. It can be useful in automating systems to increase the speed of processes and handling large volumes of tasks in real-time.

Next is the fact that AI increases the intelligence of many systems by introducing automation, bots, and smart technology that can learn and produce results rapidly. AI is also proving to be efficient and effective in self-learning through its algorithms which can identify any structures and regularities. Facial recognition systems need AI to analyze complex datasets. Through its deep learning capabilities, AI ensures there is a high accuracy in the inputs it produces [14]. Finally, AI is an important technology in monetizing many aspects of businesses and thereby helping companies to be on top of the game.

D. Facial biometrics system used For Security

Security is the most important aspect for many businesses, governments, and facilities. The use of facial recognition systems advances security measures for many institutions and workplaces. This technology is preferred because of its high accuracy and advanced identification mechanism [14,15]. The integration of AI and ML algorithms enables this system to complete computations in seconds. Its software can conduct both geometric and photometric computations and produce results in seconds. The biometric system is emerging as a novel idea that is changing the detection of many people at once without leaving any chance for human errors. Its applicability and low cost make it the best detection system and storage for many profiles [16]. An added feature is the fact that the stored information can only be accessed by the owners especially the law enforcement personnel [16,17].

IV. SIGNIFICANCE AND BENEFITS

Facial recognition systems are significant in improving the security of many facilities in many places. Governments are working on advancing these systems by introducing sophisticated AI and ML algorithms to secure many sensitive facilities like airports, government premises, and businesses. Law enforcement is also utilizing facial recognition systems to arrest criminals and major threats to national security like terrorism [17]. These benefits are also helping people on a personal level by providing security improvements to their devices and properties. For instance, facial recognition systems are common in smartphones, smart homes, and personal computers. No one can access these devices and property without face verification and unlocking mechanisms. Law enforcement can track burglars, thieves, and trespassers using surveillance cameras that capture every movement in an invaded property. Companies have also replaced the need for passwords in accessing their computers with facial recognition systems to deter any unauthorized entry into their sensitive information. This is necessary in securing many facilities and ensuring that hackers are deterred from accessing, stealing, or destroying sensitive information, stealing money, and documents [17].

V. FUTURE

Criminals get advanced every day by finding new ways of penetrating systems. Facial recognition systems will become more intelligent in the future as more technologies like artificial intelligence and machine learning become more sophisticated. There will be an advancement of interconnected facial recognition systems to form a neural network of sophisticated security systems. The U.S. will be at the forefront of advancing this technology to shape the development and implementation of better security systems. There will be more accuracy as facial recognition is used by many facilities due to the advancements of machine learning algorithms. There will also be large datasets and more advanced tools that can capture facial features with ease. However, ethical concerns may arise in the future as recognition systems may invade people's privacy. With constant surveillance, this technology has the potential to be misused [18]. This will demand more regulations and guidelines on the proper use of the technology for the benefit of the society. A facial recognition system should not be biased but must be transparent when deployed to ensure it meets its intended use. There should be a need for more cybersecurity measures to increase attention to security lapses in systems because of vulnerabilities and potential hacks.

V. CONCLUSION

The focus of this paper was to assess the facial recognition system and how AI plays a role in its working mechanisms. The finding shows that facial recognition is becoming a necessity in many security measures. Law enforcement and businesses are utilizing these systems to secure many places by detecting any suspicious people before and after they commit a crime. Artificial intelligence has improved the working mechanism of facial recognition systems. As more data is collected, the integration of AI increases the automation and computational power of the system. The future of security looks set to be relying on AI and machine learning. Many companies are already personalizing security features on smartphones, smart homes, and online platforms. Facial recognition systems collect a vast amount of data which is important in making a resourceful database. Many applications are also integrating facial recognition systems to increase the security of their applications. The future looks good for the security sector as technology will play an important role in detecting any suspicious activities in many sectors. However, ethical concerns may arise which will need to be addressed to avoid jeopardizing the tremendous gains made in adopting facial recognition systems.

REFERENCES

[1] X. Cai, C. Wang, B. Xiao, X. Chen, and J. Zhou, "Deep nonlinear metric learning with independent subspace analysis for face verification," Proceedings of the 20th ACM international conference on Multimedia - MM '12, 2012, doi: 10.1145/2393347.2396303.

[2] K. Gates and New York University Press, Our biometric future : facial recognition technology and the culture of surveillance. New York; London: New York University Press, Cop, 2011 [Online]. Available: https://muse.jhu.edu/book/11103

[3] Joaquim Filipe, M. S. Obaidat, and Springerlink (Online Service, e-Business and Telecommunications : International Conference, ICETE 2008, Porto, Portugal, July 26-29, 2008, Revised Selected Papers. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009.

[4] Joaquim Filipe, M. S. Obaidat, and SpringerLink (Online Service, E-Business and Telecommunication Networks: Third International Conference, ICETE 2006, Setúbal, Portugal, August 7-10, 2006, Selected Papers. Berlin, Heidelberg: Springer Berlin Heidelberg, 2008.

[5] B. Karimi, Comparative Analysis of Face Recognition Algorithms and Investigation on the Significance of Color. 2006.

[6] S. Gong, S. J. Mckenna, and A. Psarrou, Dynamic Vision: From Images To Face Recognition. World Scientific, 2000.

[7] G. Bebis et al., Advances in Visual Computing: 7th International Symposium, ISVC 2011, Las Vegas, NV,

USA, September 26-28, 2011. Proceedings, Part II. Berlin, Heidelberg: Springer Berlin Heidelberg, 2011.

[8] T. Pajdla, J. Matas, and SpringerLink (Online Service, Computer Vision - ECCV 2004: 8th European Conference on Computer Vision, Prague, Czech Republic, May 11-14, 2004. Proceedings, Part I. Berlin, Heidelberg: Springer Berlin Heidelberg, 2004.

[9] A Campilho and M. Kamel, Image analysis and recognition: 5th international conference, ICIAR 2008, Póvoa de Varzim, Portugal, June 25-27, 2008: proceedings. Berlin ; New York: Springer, 2008.

[10] K. Saeed, Jerzy Pejas, and Romuald Mosdorf, Biometrics, Computer Security Systems, and Artificial Intelligence Applications. Springer Science & Business Media, 2007.

[11] Jerzy Pejas and Andrzej Piegat, Enhanced Methods in Computer Security, Biometric and Artificial Intelligence Systems. Springer Science & Business Media, 2006.

[12] L. Rutkowski, R. Scherer, Ryszard Tadeusiewicz, L. A. Zadeh, and J. M. Zurada, Artificial Intelligence and Soft Computing, Part I. Springer, 2010.

[13] Athman Bouguettaya, Ingolf Krüger, Tiziana Margaria, and Springerlink (Online Service, Service-Oriented Computing - ICSOC 2008: 6th International Conference, Sydney, Australia, December 1-5, 2008, Proceedings. Berlin, Heidelberg: Springer Berlin Heidelberg, 2008.

[14] Leszek Rutkowski, Artificial intelligence and soft computing - ICAISC 2006: 8th international conference, Zakopane, Poland, June 25-29, 2006: proceedings. Berlin; New York: Springer, 2006.

[15] S. K. Rogers and M. Kabrisky, An introduction to biological and artificial neural networks for pattern recognition. Bellingham, Wash.: Spie Optical Engineering Press, 1991.

[16] L. Rutkowski, R. Scherer, Ryszard Tadeusiewicz, L. A. Zadeh, and J. M. Zurada, Artificial Intelligence and Soft Computing, Part II. Springer, 2010.

[17] C. Lanchner, Fernand Léger, Art, and Exhibition Fernand Léger. <1998, New York, NY, Fernand Léger : [in conjunction with the exhibition Fernand Léger, at the Museum of Modern Art, New York, February 15 - May 12, 1998]. New York, Ny: Museum Of Modern Art, 1998.

[18] I. G. Maglogiannis and E. Al, Emerging artificial intelligence applications in computer engineering: real word AI systems with applications in eHealth, HCI, information retrieval and pervasive technologies. Amsterdam; Oxford: Ios Press, 2007 [Online]. Available: https://dl.acm.org/citation.cfm?id=1566770.1566773.

[19] Lazaros Iliadis, Ilias Maglogiannis, Grigorios Tsoumakas, Ioannis Vlahavas, M. Bramer, and Springerlink (Online Service, Artificial Intelligence Applications and Innovations : Proceedings of the 5th IFIP Conference on Artificial Intelligence Applications and Innovations (AIAI'2009), April 23-25, 2009, Thessaloniki, Greece. New York, NY: Springer Us, 2009.