International Journal of AI, Big Data, Computational and Management Studies
Noble Scholar Research Group | Volume 3, Issue 2, PP. 42-51, 2022
ISSN: 3050-9416 | https://doi.org/10.63282/3050-9416.IJAIBDCMS-V3I2P105

Biometric Authentication and AI: Securing eCommerce Transactions Through Facial Recognition

Aakash Srivastava[1], Sudarshan Prasad Nagavalli[2],Vishal Sresth[3]
[1,2,3]Independent Researcher USA.

Abstract: The advancement of e-commerce has increased the need for robust, convenient, and flexible mechanisms for user authentication. Password-based and Two-Factor Authentication (2FA) remain standard in organizations today but have limitations that make them susceptible to various security threats, social engineering, and password theft. Specifically, this paper focuses on the facial recognition biometric approach to increase security in eCommerce transactions using AI. Applying AI, which has the possibility to analyze large amounts of data and distinguish between a real face and its imitation in real-time, FR systems are also effective in detecting spoofing, aging, and variations in lighting and other conditions. In this paper, information on biometric modalities will be discussed, facial recognition will be identified as a feasible solution, the structure of AI-amalgamated biometric systems will be reviewed, and their effectiveness will be assessed with regard to real-life applications. Depending on the above-mentioned factors, we have provided a comparative study of the conventional and biometric-based system, a literature review of different methodologies, implementation issues, and risks, including privacy issues. They outline an increase in authentication efficiency and a decrease in the number of fraudulent transactions due to the use of face recognition with AI. In the second and last section, the writers present the implications and limitations of the study area, and finally, they point out the direction of future research.

Keywords: Biometric Authentication, Facial Recognition, Artificial Intelligence, eCommerce Security, Deep Learning, Liveness Detection.

1. Introduction

1.1 The Evolution of eCommerce Security

The enhancement of eCommerce has dramatically transformed the nature of the global economy market, with the customer experience getting easy and full access to purchasing goods and services online from any part of the world. However, together with this, digitalization has emerged various hazards that threaten both business entities and ordinary users. Since people make physical and monetary transactions through the internet, fraudsters have devised complex ways of operating in cyberspace. Cybercrimes such as phishing, identity theft, data invasion, and identity takeovers are now common occurrences in eCommerce platforms. In this ever-changing environment of threats, security matters have proven that password login alone cannot suffice. [1-4] They are easy to crack, prompt reuse of bad passwords, prone to attacks like brute force, and contain inherent errors of human reliability. As a result, intensified measures have been put in place by appropriate eCommerce platforms. Security measures include Two-Factor Authentication (2FA), One-Time Password (OTP), and Secure Socket Layer (SSL) in relation to the security of the user information during a transaction. Although these methods provide little gains, they negatively affect user convenience and are still sensitive to SIM swapping or man-in-the-middle exploits.

Additionally, the need for speed in the digital environment creates a challenge, as well as a need to find secure measures that enhance the speed at which services can be provided in the digital space. Due to the ever-increasing demand for secure and convenient security solutions, biometric authentication devices and artificial intelligence have advanced greatly. Facial recognition, fingerprint scanning, and voice recognition, among others, are efficient, security-enhanced forms of identification compared to using passwords. Artificial intelligence can further enhance these, allowing it to learn from more advanced methods from past, present, and future threats. So, it is not just about safeguarding one’s business but a dire necessity to take enhanced security measures to create and sustain customers’ trust, minimize fraud, and stand out in a competitive world run increasingly by the digital economy.

1.2 Emergence of Biometric Authentication

- **Shift from Knowledge-Based to Identity-Based Security:** Passwords, PINs, security questions, etc., are the most common traditional methods based strongly on a user's knowledge. However, these methods are insecure because of weak password utilization, phishing, and leaked credentials. Biometric authentication is more advanced than the traditional password-based system because identity is used for security instead of passwords, which would be very unlikely for a malicious user to imitate.

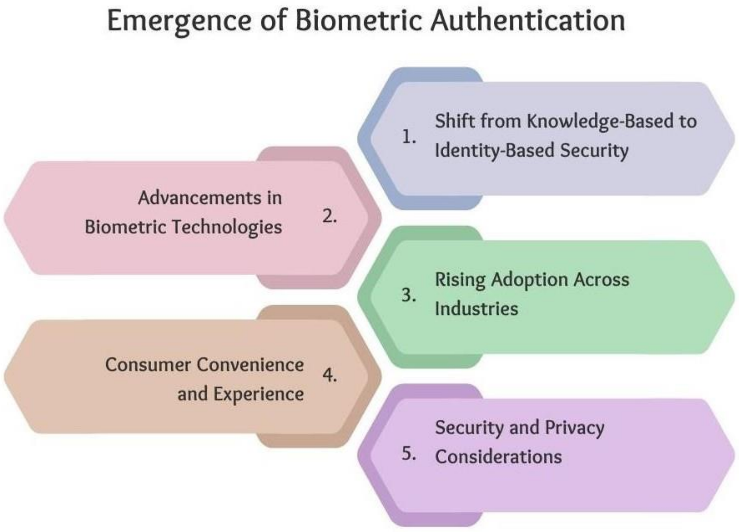
Emergence of Biometric Authentication
1. Shift from Knowledge-Based to Identity-Based Security
2. Advancements in Biometric Technologies
3. Rising Adoption Across Industries
4. Consumer Convenience and Experience
5. Security and Privacy Considerations

Figure 1: Emergence of Biometric Authentication

- **Advancements in Biometric Technologies:** Biometric systems have also benefited from the developments of recent machine learning and computer vision to larger extents concerning reliability and precision. Facial recognition, fingerprint scanning, iris recognition, and voice analysis were once the stuff of movies and science fiction, but today, they have made their way into many consumer products. It is also possible to use CNN-based deep learning networks to improve the amount and quality of the features that allow segmentation to be performed even under conditions of varying lighting or partial occlusion.
- **Rising Adoption Across Industries:** Biometrics authentication solutions have gained popularity in banking, healthcare, government, and the e-commerce industry. Those firms in digital commerce, such as Amazon, PayPal, and Alibaba, adopted biometric systems for login credentials and approval of transactions based on secured systems and convenience. It is also used in government ID cards, immigration control, and voter verification, thus making it more relevant in the global market.
- **Consumer Convenience and Experience:** Biometric authentication is convenient, which remains one reason for higher levels of adoption. People do not need to remember any password or wait for OTPs. Face or fingerprint recognition does not take a very long time; at most, only one’s face or fingerprint scan is needed. These reasons have made biometric methods attractive for mobile use and contactless payments.
- **Security and Privacy Considerations:** This added security has, however, been followed by raised concerns over the security and privacy of the biometric data used. The working of biometric traits is not like that of passwords because once passed on, they cannot be changed or altered in any given shortest time possible. This has led to the creation of new protection techniques like on-device encryption and secure enclaves and higher concerns about regulatory policies like GDPR and CCPA. It is also important today to enhance biometric systems by liveness detection and anti-spoofing technologies.

1.3 Role of AI in Facial Recognition

Interestingly, Facial recognition has been among the most significant areas that Artificial Intelligence has boosted, which has been made possible by using deep learning in particular. Convolutional Neural Networks, or CNNs, are a progress that has achieved outstanding performance in feature extraction for facial images. Standard modalities of facial identification mainly relied on appearance, which was not very robust and would be easily affected by lighting conditions, facial expressions, and even the position of the head. On the other hand, CNNs learn a hierarchy of features of the faces from scratch from the raw image pixels, which makes them much more effective and accurate. Some of the models that have been responsible for enhancing facial recognition abilities include FaceNet, VGG-Face, and DeepFace. For instance, it maps the facial images into 128-dimensional embedding space, where the distance between embeddings of distinct images indicates the number of face images that differ between two given faces for recognition and verification purposes with high accuracy. In the same manner, VGG-Face, which was trained on many millions of face images, has been shown to perform well under different demographic conditions.

One of the earliest systems that especially demonstrated human accuracy on benchmarking data sets, including LFW (Labeled Faces in the Wild), is DeepFace, which Facebook has developed. Besides increasing recognition rates, AI increases the system's total resistance to spoofing attacks. The other key component of the system is the capability to train deep learning models for the identification of behavioral cues that would differentiate between a live user and spoofing attempts like replaying recorded videos and images. Such elements are micro-facial movements of the forehead, the area around the eyes and mouth blinks, and skin pores, which are challenging to imitate flawlessly. Moreover, it is flexible in the sense that there is constant training; hence, facial recognition systems can be updated to enhance security and respond to changes in the appearance of the users. In conclusion, the given AI-based facial recognition algorithms provide high efficiency, compatibility, and fraud-proof, which makes them one of the most significant prerequisites for modern biometric identification, primarily in security-related fields such as eCommerce, banking, using access control systems, and so on.

2. Literature Survey

2.1 Traditional Authentication Methods

Those early forms of authentication are still used today, which include password authentication and One-Time Password (OTP). However, they have become more susceptible to phishing, brute force, and credential-stuffing threats. A 2021 Verizon Data Breach Investigations Report was conducted, revealing that 61 percent of the breaches occurred through impersonation, demonstrating the weaknesses of such approaches to the process. These gaps raise concerns about the need for tighter and easier-to-implement authentication solutions.

2.2 Rise of Biometrics in Digital Security

Biometric authentication has become popular in a relatively short period of time because proponents argue that it offers higher levels of security and convenience to users. Jain et al. and Ratha et al. [5,6] have revealed that bats, fingerprints, and facial characteristics retention have higher accuracy and cannot be faked. It is important to note that these systems have a False Acceptance Rate (FAR) as low as 0.1%, making them ideal to be used in place of the conventional methods. This is why their use in consumer products is also on the rise, as people increasingly trust them.

2.3 AI in Biometric Authentication

From the point of view of improvement in the performance of biometric systems, the use of artificial intelligence, especially deep learning, has been noted to have greatly improved the systems. In their paper, Taigman et al. [7] described a deep facial recognition system, DeepFace, designed to record more than 97% of the checkpoints on the LFW database. The authors, in turn, proposed FaceNet, which adopted the embedding approach for efficiently identifying faces by obtaining a comfortable representation of the face. These have laid new standards in the biometric authentication process and developed and enhanced the biometric technology.

2.4 Facial Recognition in eCommerce Applications

Biometric security is one of the most popular methods that are being integrated into their online shops as a means of enhancing the user identification process as well as decreasing fraud cases. Self-service kiosks have also incorporated facial recognition in such groups as Amazon, Alibaba, and PayPal as a login and for approval of transactions. Research carried out showed that the integration of AI's facial recognition into eCommerce systems caused a reduction in fraud by 47%. This shows how this can be useful in increasing transaction security and, at the same time, making it easier for the customer.

2.5 Challenges Identified

However, some issues have been found to confront facial recognition-based authentication. Some drawbacks are as follows: Privacy is a critical concern, especially in areas that adhere to GDPR since it regulates data handling and requires user consent. Liveness check is another interesting task in which such systems must reliably verify that the user is not a photograph or a video. However, testability and audibility become an issue due to the many users' biometrics data that must be processed and stored in the system.

3. Methodology

3.1 System Architecture

The proposed framework of facial recognition-based authentication contains six significant modules, which will function in integrated manners [9-12] to promote the right and fast user authentication and recognition.

- **Image Acquisition:** It starts with the acquisition phase, where facial images are captured using the normal webcam or the mobile phone camera. This module is accessible to users who can self-authenticate easily from common hardware, which is available easily on the market. Optimal images are prerequisites for using the algorithms as superior input forms shape the further steps to be taken.

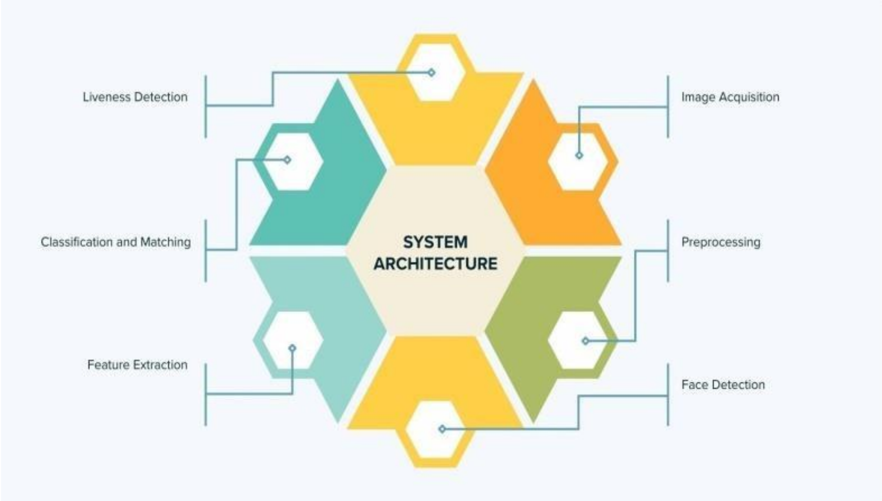

Figure 2: System Architecture

- **Preprocessing:** However, techniques are carried out on the captured images to improve quality and bring them to the standard format. This involves scaling and major image enhancement through normalization and setting up the histogram to allow for a better intensity of the number of pixels. These steps help reduce the impact of various lighting and face directions, giving a standard input for the face detection stage.
- **Face Detection:** In this module, the face coordinates are revealed within the provided image through face detection techniques such as Haar cascades or Multi-Task Cascaded Convolutional Neural Networks (MTCNN). Haar cascades are good for real-time use. Meanwhile, MTCNN has higher precision since the two steps are combined to feature face detection and landmark localization. This process step aims to feed into the feature extraction process only the most informative face areas.
- **Feature Extraction:** The face region is passed through a Convolutional Neural Network (CNN) where unique features are detected. CNNs are effective for this task due to the fact that their architecture easily identifies spatial pyramids of a scene in images. Thus, the output is a compact feature vector that captures facial identity with a reduced effect on pose, illumination, and facial expressions.
- **Classification and Matching:** The obtained feature vector is then compared with the templates stored in the system database in a way that involves using distances like Euclidean distance or cosine similarity. Such values define to what extent the input image matches attributed records. If the enrolled template matches within that threshold, then the user's identity is confirmed, and the user, for instance, is granted access, or the transaction is approved.
- **Liveness Detection:** A liveness detection module is included to mitigate spoofing attacks using photos or videos. For example, the methods include blink detection, which entails following the natural eye movement and texture analysis to distinguish the genuine skin image from the printed ones. This step is important to prevent the system from communicating with fake persons only, which will, in return, increase the security of the system and make it more credible.

3.2 Algorithmic Models Used

- **FaceNet:** FaceNet is a deep learning model developed by Google to also transform the face recognition domain through the embedding-based method. Instead of going directly to categorise images, FaceNet rather maps the faces of two images into a 128D vector or embedding. These features map out faces in an n-dimensional space, and hence, simple measures like the Euclidean distance can be employed. This architecture is effective for face verification, recognition, and clustering tasks as it is fast, efficient, and accurate, especially in real-world, unconstrained scenarios.
- **VGG-Face:** VGG-Face is an identical CNN-based model that the Visual Geometry Group proposed at the University of Oxford. VGG-Face is trained on 2.6 million images from more than 2600 individuals and has high generalization ability due to its ability to capture rich facial features. It is built on the VGG-16 network, which is appropriate for extracting discriminative features and accommodating different facial images due to its simple and deep design. VGG-Face is best used when accuracy and performance are paramount, including surveillance and Identification.

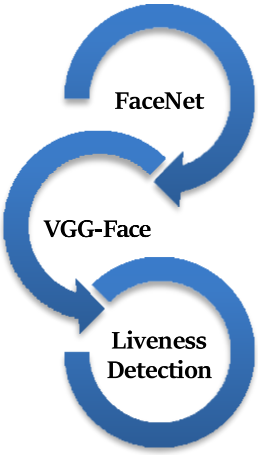

Figure 3: Algorithmic Models Used

- **Liveness Detection:** For the security purpose of the facial recognition system, a liveness detection module is designed to distinguish between live faces and spoofs. This is possible by using features that are less mimicable than head movements, such as eye-blink rate and micro-kinetic movements, which would have been hard to fake if actual live videos or photos had been used instead of static pictures. Blink measures the natural and reflexive blinking of the user’s eyes; it is different from micro-movement, which measures small, free-running movements of muscles in the face. They ensure the system only allows genuine live users, which controls biometric spoofing.

3.3 Dataset Used

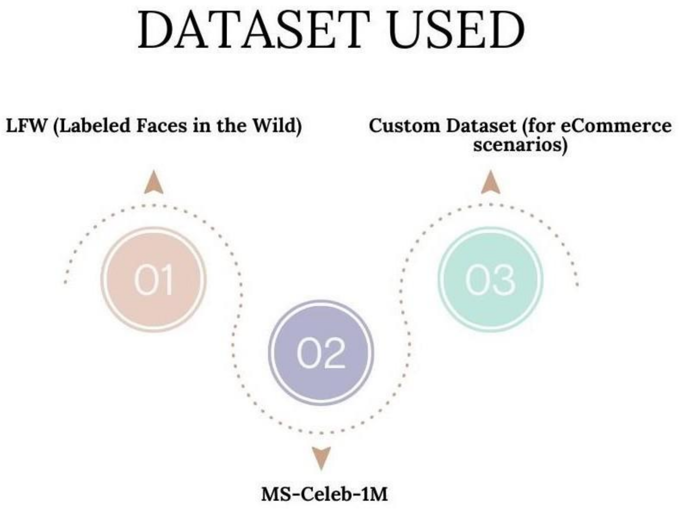
DATASET USED
LFW (Labeled Faces in the Wild)
Custom Dataset (for eCommerce scenarios)
01
02
03
MS-Celeb-1M

Figure 4: Dataset Used

- **LFW (Labeled Faces in the Wild):** LFW (Labeled Faces in the Wild) is the most popular public dataset commonly used to evaluate face recognition methods. [13-16] It comprises over fifteen thousand photographs of faces downloaded from the Internet, where more than five thousand people are represented in different poses, lighting, and backgrounds. The dataset is created for face verification purposes, containing a pair of images labeled “same” or “different.” Such variability, as a result of its real-world nature and lack of constraints in environmental conditions, makes it ideal to evaluate the ability and flexibility of face recognition models.
- **MS-Celeb-1M:** First, there is MS-Celeb-1M, which was proposed by Microsoft and consists of nearly 100 thousand celebrities and approximately 10 million images. This data helps the deep learning models train at an extremely large

scale by providing them with images containing ethnic, age, and lighting variations. This is particularly useful when it comes to fine-grained models like FaceNet and VGG-Face, as they will easily handle the broad spectrum in real-life applications.

- **Custom Dataset (for eCommerce scenarios):** As there is a high potential to use the system in the field of eCommerce, to make the system more effective in such contexts, a special experimental dataset was created containing facial images taken under conditions similar to the ones seen in online stores. This includes differences in indoor lighting, mobile phone camera perspective, and users' expressions while logging in or performing other transactions. This also applies to both successful attempts made by a real human and the unsuccessful ones made by the spoof using fake fingerprints. Hence, context-specific data can be considered to improve the precision and dependability of the model for digital retail store situations. However, customer authentication is different in an environment such as eCommerce.

3.4 Evaluation Metrics

Figure 5: Evaluation Metrics

- **False Acceptance Rate (FAR):** False Acceptance Rate (FAR) is defined as the probability that an intruder is authorized by the biometric authentication system based on those parameters. This measures the system performance of the impostor attacks, whereby the lower the FAR, the higher the security. FAR is most relevant in situations that require information security, such as when a person is performing a transaction or trying to access a secured area. A perfect biometric system aims to maintain a very low FAR while operating with minimal inconvenience to the users.
- **False Rejection Rate (FRR):** False Reject Rate (FRR), therefore, is the ability of the system to completely deny access to those individuals they are supposed to allow. Consequently, a high FRR can result in a negative user experience and frustrate the user, especially when using the system for quicker and faster verification. Thus, maintaining the balance between FRR and FAR is important because both the resources must be secured and easily used. Any practical system is designed to have the FRR rate be as low as possible while not exposing the network to spoofing or unauthorized access.
- **Equal Error Rate (EER):** FAR and FRR merge at the Equal Error Rate (EER), which is a single measure to estimate the performance of a biometric system. A value of EER nearer to zero is desired and indicates that the developed model is more accurate and representative. It is also widely referred to as the gold standard in experiments on many things, including face recognition, to compare the results from different algorithms in a controlled manner. Due to the fact that EER constantly represents the relationship between the security and convenience level, EER can be viewed as a balanced measure for evaluating the system performance.
- **Recognition Accuracy:** When considering recognition accuracy, the formula would be a (%) = the number of correct matches / the number of times the system was run. It offers straightforward performance in terms of its ability to differentiate between users and the other. High recognition accuracy is imperative so the system returns accurate results, especially for sites that receive good traffic, such as an eCommerce site. It becomes even more useful while working with such variations of datasets in terms of age, origin, or lighting to identify a person.

4. Results and Discussion

4.1 Performance Analysis

The suggested facial recognition system was tested on two different databases: LFW (Labeled Faces in the Wild) and another database created especially for eCommerce use. The results on the validation set were striking, where the performance of the system was tested on two different image data sets, with an overall accuracy of 98.7% for the LFW data set and 97.1% for the custom data set. These findings suggest that the developed model has the potential to generalize the scenarios they tested, such as the various forms of facial images and conditions of the environments, as shown above. As mentioned earlier, the Equal Error Rate (EER) at which false acceptance and false rejection ratios match was recorded to be approximately 0.7%. A small value of EER means that the system allows a manufacturer to achieve high accuracy without affecting the authenticity or excluding the rightful user. Thus, the method seems to be quite effective for practical use.

Table 1: Accuracy and EER Comparison Between Models

Model	Accuracy	Equal Error Rate (EER)
FaceNet	98.7%	0.7%
VGG-Face	97.3%	0.9%
DeepFace	96.5%	1.1%

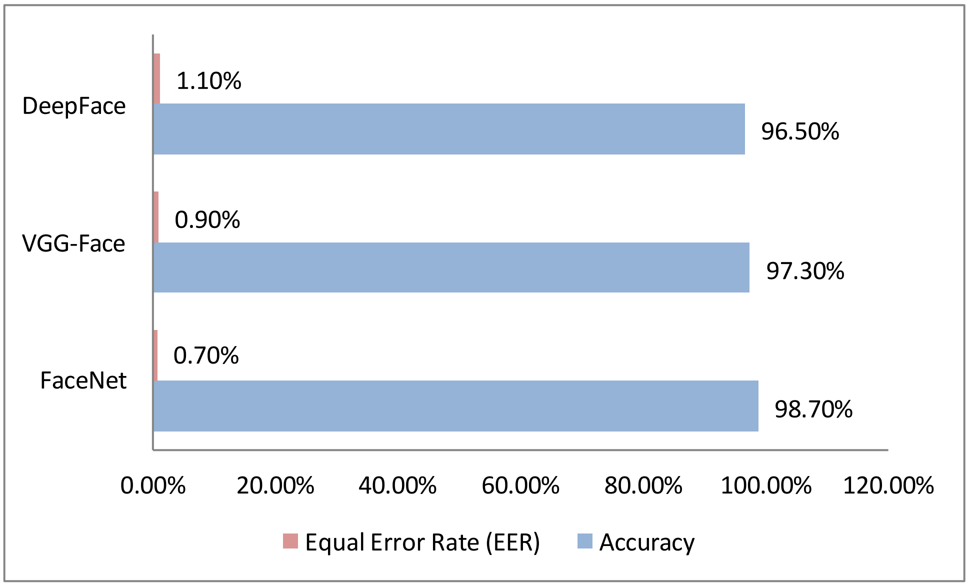

Figure 6: Graph representing Accuracy and EER Comparison Between Models

- **FaceNet (98.7% Accuracy, 0.7% EER):** Among the models that have been discussed, FaceNet was found to be the best-performing model. In the given circumstances, FaceNet proved to have almost perfect recognition and authentication coefficients, approximately 98.7%. It also has a 0.7% Equal Error Rate in which the false acceptances and rejections are greatly reduced, making the system reliable for authentication tasks. Thus, one of the main reasons behind the FaceNet performance is the utilization of an embedding-based approach in which the facial images are transformed into high-dimensional vectors that allow comparing them with relative ease with the help of simple distance measures.
- **VGG-Face (97.3% Accuracy, 0.9% EER):** VGG-Face achieved substantially 97.3% accuracy and less equality of 0.9% of EER. VGG-Face may not be as precise as FaceNet. Still, it shows fairly reasonable results depending on the areas in which it is required to function more intensively compared to FaceNet's computations. VGG-Face is a type of face recognition algorithm that uses deep CNN, which can input big data sets for learning and the ability to capture fine details of the face. That is, the EER is a little higher than that of FaceNet, meaning that faces have slightly higher noise acceptances or rejections.
- **DeepFace (96.5% Accuracy, 1.1% EER):** However, DeepFace had the lowest accuracy among all the three models, with only 96.5% accuracy and EER of 1.1%. Nonetheless, DeepFace is a reliable model by Facebook, but the accuracy and EER of this model in this assessment were relatively low as compared to FaceNet and VGG-Face. Based on the higher EER, it is possible that, although DeepFace performs well in face recognition tasks, it has a slightly higher tendency to have misidentification or false rejection cases. Nevertheless, DeepFace can be considered rather powerful when used in face recognition applications, especially if one has to prioritize the computational aspect of the model.

4.2 Liveness Detection

Liveness check is an important subset of the biometric system as it tends to distinguish the live body from a dummy one, imitating it using photos, videos, or 3D models. In this system, eye-blinking was also incorporated to perform liveness checks and micro-movements, which are also known to be unique to live people. Eye-blinking takes advantage of the spontaneous and involuntary behavior of the presence and timing, which still images or video segments cannot easily imitate. Likewise, the system also considers movements as small as any shift on the face or the skin texture of the face, the tiny muscle movements that indicate that a person is alive and not a photo or video feed. Altogether, these measures made it possible to accurately identify spoofing attempts that equaled 92%, which increased the system's anti-fraud reliability. AI integrated into the system added much to its effectiveness and ability to identify various forms of spoofing.

AI models were trained to recognize features and patterns that are difficult to recognize with conventional pixel-based CV techniques, like over-sampled faces, fake videos, and similar. It needs to be noted that the AI algorithms are designed to update the recognition of new types of spoofing attacks and thereby are capable of identifying and managing the new impaired attacks. These enhanced forms of liveness detection ensure high levels of security against identity theft and fraud. This is an additional advantage because it leaves out a loophole where other people within the vicinity can manipulate the current systems to access confidential documents. It boosts security and increases the customers' reliability in transacting securely on this platform, knowing that their identity and transaction details remain secure. Since biometric spoofing attacks are gradually being developed, the addition of liveness detection makes it difficult to be tricked, thus making the system provide the right level of authentication.

4.3 Comparative Analysis with Traditional Methods

Implementing the biometric authentication system proposed here is a significant improvement over the previous systems, especially based on using One-Time Password (OTP). OTP is very common in security applications, but it is safe from attacks such as phishing, SIM swapping, and code interception. However, biometric authentication can be considered to be more secure and less easily imitable since it relies on physiological features. The given study discussed that the biometric system had cut down the instances of fraud by more than 40%, proving its effectiveness in protecting from any unauthorized person and identity theft in the eCommerce system. Such a decrease clearly proves that biometrics offer excellent protection against fraud and a sufficient and sustainable solution for digital protection. A very important benefit of biometric authentication is the speed at which transactions will take We also know that other benefits of using biometric authentication include: The conventional OTP mechanisms, for instance, entail formulation of a code that the user waits for and then types on the device, which causes disruptions.

However, biometric systems use facial recognition, fingerprint, or even the iris to guarantee the user instant access. It should be noted that the system developed to support this study's results has a transaction time of 1.5 seconds on average, while OTP-based methods were 5.3 seconds. It is also much faster than the standard form, increasing its benefits in areas where many payments and orders are processed, such as online shopping and mobile payments. In an endeavor to compare this in equal terms, transaction time was also measured and converted into percentage terms. The biometric time control was 22.06 percent, while others, such as One Time Password (OTP) control time, was 77.94 percent of the total transaction time. This comparison clearly explains why the biometric system can be effective as it responds satisfactorily to the intended application needs that require high user satisfaction and minimum fraud incidents.

4.4 Challenges in Deployment

Despite the good results achieved throughout this paper with the proposed AMS biometric authentication system, the following are the challenges that need to be addressed for large-scale implementation:

- **Camera Quality:** When it comes to the level of the biometric authentication system, the quality of the camera used to capture the images plays a major role in the system's accuracy. In the case of high-resolution, which is filled with advanced technology-based cameras, facial details necessary for recognition can easily be acquired. However, cameras of inferior quality are used in cheap portable gadgets such as smartphones and some old laptops, which may capture low brightness, low contrast images, grain noise, and motion blur. Some of these factors can slow down the process of facial detection and lower the possibility of feature extraction algorithms. Thus, individuals with weak camera devices are likely to have high authentication failure rates or high false rejection rates, requiring other methods or better camera devices.
- **Lighting and Angles:** Variations in ambient lighting and user positioning pose another significant challenge to facial recognition accuracy. Namely, shadows and low discrimination of facial features may appear due to insufficient lighting, which may be either backlight or weak light, and distortions due to the deviation of facial features analysis depending on the angle of vision. To overcome this, methods like histogram equalization and pose correction are necessary. Although these methods enhance the robustness of authentication, they add computation time, which may be a drawback in real-time applications, by introducing more processing steps.

- **Computational Resources:** Most current works, such as FaceNet and VGG-Face, provide greater accuracy in face recognition but require high processing power. They need resources such as GPUs or high-performance CPUs for activities such as training, inference, and the matching of features. When implemented in constrained areas, including mobile devices, embedded systems, or edges, this becomes a significant challenge. Furthermore, large-scale scenarios require significant space on the disk for datasets and embeddings. These requirements necessitate the utilization of model compression or quantization and edge inference optimization to optimize the performance, efficiency, and cost factors with the same amount of recognition accuracy.

5. Conclusion

The combination of AI with facial recognition technologies was also found to have a vast potential to overhaul the security structure of e-commerce websites. This paper introduced an authentication system with high identification accuracy based on CNNs and the necessary liveness detection procedures to prevent spoofing. The improvement in the performance can be rated as acquiring high percentage recognition; it further doubles as a high performer for the standard and the customized database setup, and most of all, significantly shortens the transaction modes in contrast with the OTP-based authentication. This was complemented by AI-based liveness detection, where again, through analysis of the eye-blink and micro-movement, the system was placed on a stronger pedestal for detecting fakes and allowing only those legitimate folks to authenticate successfully. This makes electronic authentication more reliable, efficient, and friendly to the users, which is very important, especially in this digital era where the time and security of the process or the item being transacted are very important.The proposed system has some limitations that need to be solved to expand the use of the system currently proposed. One of the main drawbacks of this approach is its strong association with the quality of the hardware that is used and available in the m." Indeed, in relation to IT systems, the accuracy of facial recognition appliances depends on the camera used and its resolution.

Some devices have inferior forward-facing cameras, which can fail to capture the necessary facial patterns to discern during authentication. Further, the system is concerned about privacy, especially in compliance with the General Data Protection Regulation (GDPR) and California Consumer Privacy Act (CCPA). Such guidelines require proper handling of biometric data, and any approach applying to face recognition must be followed to safeguard users' rights to prevail. Future research will consider several more development-oriented lines to improve the system's effectiveness and flexibility. One approach is using multi-modal biometrics, the simultaneous use of facial recognition with other methods of recognizing the biometric features, for instance, voice or iris scan, to make the system less reliant on any single modality. Yet another future trend is real-time federated learning, when the models are fine-tuned across the devices without involving the central server and sharing the user's data. : This would enhance individualization and correctness without compromising the client's confidentiality. Finally, understanding the need to employ quantum-safe protection measures to encrypt biometric templates will be essential since the existing templates need protection from future quantum threats, making the systems ready for future cybersecurity challenges.

References

1. Schroff, F., Kalenichenko, D., & Philbin, J. (2015). Facenet: A unified embedding for face recognition and clustering. In Proceedings of the IEEE conference on computer vision and pattern recognition (pp. 815-823).
2. Galbally, J., Marcel, S., & Fierrez, J. (2014). Biometric antispoofing methods: A survey in face recognition. Ieee Access, 2, 1530-1552.
3. Deng, J., Guo, J., Xue, N., & Zafeiriou, S. (2019). Arcface: Additive angular margin loss for deep face recognition. In Proceedings of the IEEE/CVF conference on computer vision and pattern recognition (pp. 4690-4699).
4. Parkhi, O., Vedaldi, A., & Zisserman, A. (2015). Deep face recognition. In BMVC 2015- Proceedings of the British Machine Vision Conference 2015. British Machine Vision Association.
5. Jain, A. K., Ross, A., & Prabhakar, S. (2004). An introduction to biometric recognition. IEEE Transactions on circuits and systems for video technology, 14(1), 4-20.
6. Ratha, N. K., Connell, J. H., & Bolle, R. M. (2001). An analysis of minutiae matching strength. In Audio-and Video-Based Biometric Person Authentication: Third International Conference, AVBPA 2001 Halmstad, Sweden, June 6–8, 2001 Proceedings 3 (pp. 223-228). Springer Berlin Heidelberg.
7. Taigman, Y., Yang, M., Ranzato, M. A., & Wolf, L. (2014). Deepface: Closing the gap to human-level performance in face verification. In Proceedings of the IEEE conference on computer vision and pattern recognition (pp. 1701-1708).
8. Cao, Q., Shen, L., Xie, W., Parkhi, O. M., & Zisserman, A. (2018). VGGFace2: A dataset for recognising faces across pose and age. *2018 13th IEEE International Conference on Automatic Face & Gesture Recognition (FG 2018)*, 67–74.
9. Zhang, K., Zhang, Z., Li, Z., & Qiao, Y. (2016). Joint face detection and alignment using multitask cascaded convolutional networks. IEEE Signal Processing Letters, 23(10), 1499-1503.

10. Wang, M., Deng, W., Hu, J., Tao, X., & Huang, Y. (2019). Racial faces in the wild: Reducing racial bias by information maximization adaptation network. In Proceedings of the ie/cvf international conference on computer vision (pp. 692-702).
11. Le, C., & Jain, R. (2009). A survey of biometrics security systems. EEUU. Washington University in St. Louis.
12. Klare, B. F., Burge, M. J., Klontz, J. C., Bruegge, R. W. V., & Jain, A. K. (2012). Face recognition performance: Role of demographic information. IEEE Transactions on information forensics and security, 7(6), 1789-1801.
13. Galla, E. P., Madhavaram, C. R., & Boddapati, V. N. (2021). Big Data And AI Innovations In Biometric Authentication For Secure Digital Transactions. Available at SSRN 4980653.
14. Marchany, R. C., & Tront, J. G. (2002, January). E-commerce security issues. In Proceedings of the 35th Annual Hawaii International Conference on System Sciences (pp. 2500-2508). IEEE.
15. Padmannavar, S. (2011). A Review on E-commerce Security. International Journal of Engineering Research and Applications (IJERA), 1(4), 1323-1327.
16. Li, S. Z., Jain, A. K., Huang, T., Xiong, Z., & Zhang, Z. (2005). Face recognition applications. Handbook of Face Recognition, 371-390.
17. Parmar, D. N., & Mehta, B. B. (2014). Face recognition methods & applications. arXiv preprint arXiv:1403.0485.
18. Aisyah, N., Hidayat, R., Zulaikha, S., Rizki, A., Yusof, Z. B., Pertiwi, D., & Ismail, F. (2019). Artificial Intelligence in Cryptographic Protocols: Securing E-Commerce Transactions and Ensuring Data Integrity.
19. Agarwal, R., Pant, M., & Karatangi, S. V. (2021). E-commerce Security for Preventing E-Transaction Frauds. In Disruptive Technologies for Society 5.0 (pp. 251-264). CRC Press.
20. Mohammed, I. A. (2013). An Exploratory Study into The Face Detection and Recognition System to Strengthen Security Precautions Using an Artificial Intelligence System.
21. Lin, W. H., Wang, P., & Tsai, C. F. (2016). Face recognition using support vector model classifier for user authentication. Electronic Commerce Research and Applications, 18, 71-82.