An Enhancement of Eigenface Algorithm Applied for Identifying Spoofing Attacks in Facial Recognition

Ron Hale I. Casison[1], Chloe Gwyneth S. Upaga[2], Jamillah S. Guialil[3], Dan Michael A. Cortez[4]

[1]Computer Science Department, Pamantasan ng Lungsod ng Maynila, Gen. Luna, cor., Murralla St., Intramuros Manila, Philippines
[2]Computer Science Department, Pamantasan ng Lungsod ng Maynila, Gen. Luna, cor., Murralla St., Intramuros Manila, Philippines
[3]Computer Science Department, Pamantasan ng Lungsod ng Maynila, Gen. Luna, cor., Murralla St., Intramuros Manila, Philippines
[4]Computer Science Department, Pamantasan ng Lungsod ng Maynila, Gen. Luna, cor., Murralla St., Intramuros Manila, Philippines

Article Information

Received: 21-11-2024
Revised: 28-11-2024
Published: 05-12-2024

Keywords
Algorithm, Attack, Eigenface, Enhancement, Face Recognition

Correspondence Email:
cronhale01@gmail.com

Abstract

Facial recognition is a biometric authentication technology that identifies individuals using their facial features in images and videos. The rise of spoofing attacks poses significant risks, especially for facial recognition, as malicious actors are impersonating individuals by misusing their identities. The accuracy of facial recognition can be impacted by factors like face occlusions, image low-resolution, and the distance of the user's face from the camera, leading to potential misidentification. This research enhanced the Eigenface Algorithm applied to identify spoofing attacks in facial recognition. The algorithm extracts facial features and transforms them into eigenvectors for improved accuracy. Previous studies showed limitations in face detection at varying distances, prompting the incorporation of a distance-based scale in the enhanced algorithm, targeting a range of 30 cm to 60 cm from the camera. In this study, the researchers implemented OpenCV2 and stored the trained dataset in a YAML file. The dataset was generated by capturing multiple images with varying environments and distances, which were then preprocessed to resize and convert them to grayscale. Results showed a confidence level of 93.83% for the enhanced algorithm, a significant improvement from 57.38% with the existing one, and a faster average recognition time of 0.0141 seconds compared to 0.0216 seconds, demonstrating a 36.45% increase in confidence and a speed improvement of 0.0075 seconds. The distance-based scaling improves the efficiency of the Eigenface Algorithm by preventing recognition attempts at unsuitable distances, thus enhancing usability in practical applications.

1. Introduction

Biometric authentications are now commonly used for personal devices or in corporations for securing confidential or personal information, facial recognition is one of the types of biometrics. Most mobile applications use facial recognition as their authentication instead of the PIN or traditional security measures in devices; it's much faster and more secure. Facial recognition is more advanced and uses an algorithm that processes digital photos or videos to recognize human facial features to match images stored in a database. Different algorithms are used to establish accurate facial recognition and secure digital information, the Eigenface Algorithm is one of the algorithms introduced that can be used for facial recognition.

The Eigenface Algorithm recognizes and detects the variances of human facial features and structure in a collection of images and transforms the facial feature into a smaller set of features (eigenvector). However, once the system detects similar features it automatically accepts them. Hackers may use their victim's photo to access confidential information that they can use to scam or steal from the victim and their surroundings. Human facial features are dynamic and complex and change with time. Turk and Pentland presented 1991 a face recognition experiment in which they stored face images and developed a system that recognized faces in a dynamic environment. Their experiment showed that changing lighting caused a few errors and performance drops with size changes.

Although spoofing attacks may accompany facial recognition through varying facial distance to the camera, face occlusions, low image resolution, etc., a spoofing attack is a way of pretending to be someone to gain access to confidential files or systems. It is one of the cybercrimes that have arisen in today's generation. This study resolved the issue of facial distance. The algorithm fails to consider the facial distance from the camera reduces the usability causing unintended face recognition at varying distances. The failure to account for the facial distance from the camera diminishes the usability of facial recognition at varying distances. Although the algorithm calculates the distances between the query vector and all obtained weight vectors, it neglects to adjust for faces that are far from the camera. This oversight can result in misidentification or unintended access, as individuals may be recognized from considerable distances, ultimately leading to user frustration and confusion.

The researchers strategically implemented distance-based scaling during the testing phase, significantly enhancing the usability of facial recognition across varying distances. Researchers ensured a robust framework by leveraging OpenCV2 and archiving the trained dataset in a YAML file. This innovative distance-based approach not only streamlines the algorithm's efficiency but also effectively eliminates recognition attempts at inappropriate distances, making it a highly practical solution with real-world applications.

1.1 Literature Review

1.1.1. Spoofing Attacks in Facial Recognition

Spoofing attacks have become a significant vulnerability in the use of automated facial recognition systems. Spoofing attacks will be able to compromise the security and privacy aspects of the user. In line with this, (Firc et al., 2023), in their study "Deepfakes as a threat to a speaker and facial recognition: An overview of tools and attack vectors," highlights that deepfake images present a major threat to biometric systems, including facial recognition. This situation poses a threat to the security and integrity of the facial recognition system which can be easily fooled by crafted images. The article cited aspects of Eigenface as one of the determinators to support this claim. One of the aspects of this problem is the process of manipulation of facial images to create spoofed content. This process includes the different alterations of original face images such as morphing and

swapping. Therefore, this highlights the deficiency in the facial recognition system which lessens the security of the system to spoofed attacks.

1.1.2. Application of Eigenface Algorithm

Face recognition involves multiple sequential steps to ensure accurate identification of individuals. According to (Aliyu et al., 2020) in their study titled "A Comparative Study of Eigenface and Fisherface Algorithms Based on OpenCV and Sci-kit Libraries Implementation," the process begins by detecting a region of the provided image that contains the human face. Then, facial recognition will entail the extraction of facial features such as the eyes, lips, nose, etc; these features will serve as the feature vector. Finally, the system of face recognition will now undergo testing of faces provided from a database of known faces to look for a match. Overall, this systematic process provides the information that lays the path to effectively implement an algorithm for facial recognition.

Building on this, (Wirdiani et al., 2019) in their study "Real-Time Face Recognition with Eigenface Method" highlight the efficiency of the Eigenface algorithm, which utilizes eigenvectors to represent key characteristics of face images. The study described the algorithm as a method that will operate by constructing a set of eigenvectors from the process of training the dataset of different face images. These eigenvectors represent the principal components that are essential for capturing the features to distinguish one face from another set of faces. The efficiency of this method lies in the ability to reduce the complexity of facial recognition by dimensional data representation. Despite its capability, the eigenface method still can be affected by different factors such as the distance of the face from the camera. Based on the testing of the study, the distance of the face from the camera affects the ability of facial recognition to take clear images of the face of the subject. These factors serve as surrounding conditions that reduce the accuracy of facial recognition.

1.1.3. Drawbacks of Eigenface Algorithm

The article by (Teoh et al., 2021)**,** "Face Recognition and Identification Using Deep Learning Approach," points out that the distance between the face and the camera also affects facial recognition performance. Specifically, the Eigenface algorithm is not designed to account for varying distances of faces from the camera, limiting its adaptability in real-world scenarios. The algorithm is fixed to operate only with the representation of faces. This situation allows the inability to account for the changes caused by various distances from the camera. As a result of the article, facial recognition has failed to recognize faces in situations of too far or too close distance from the camera.

1.1.4. Broader Challenges in Applying the Eigenface Algorithm

A broader challenge regarding the distance from the camera critically affects the performance of facial recognition. The study undergoes a comparison of two different algorithms to determine various aspects of facial recognition including distance accuracy. However, for Eigenface, the study highlighted the need to evaluate the distance accuracy of the subject to facial recognition. Due to this finding, the performance of the Eigenface algorithm is affected when faces are positioned farther away from the camera. Therefore, the Eigenface algorithm cannot recognize faces at longer distances because of its inherent capabilities.

With this challenge caused by the distance between the face and the camera, (Bermejo et al., 2022), focus on estimating the subject-to-camera distance in facial images. Their research addresses perspective distortion, which alters facial attributes based on distance. By accurately estimating this distance, FacialSCDnet provides essential information for adjusting facial features effectively. The proposed scaling technique normalizes facial

data by scaling features according to the estimated distance, mitigating perspective distortion's impact. This approach aligns with the goals of the Eigenface algorithm, improving facial recognition accuracy by accounting for distance variations and ensuring more reliable results.

2. Research Methods

Principal Component Analysis (PCA) is a powerful machine learning algorithm that effectively reduces the dimensionality of datasets while retaining the essential information needed for accurate identification. One of the most notable applications of PCA is the Eigenface Algorithm, a highly regarded method in facial recognition. By leveraging PCA, the Eigenface Algorithm condenses complex facial images into key features, creating a face space that highlights the unique aspects of each individual's appearance.

Enhanced Eigenface Algorithm

a. Training Phase

1. **Obtaining face images:** Collect a set of face images denoted as I=[I1,I2,I3,...,Im]. Each image must be preprocessed to ensure they are centered and have the same dimensions (N,N).
2. **Representing images as vectors:** Each face image Ii is represented as a vector Γi, where Γ=[Γ1 ,Γ2,...,Γm] . The dimensions of each Γi should be (N×N,1).
3. **Computing the average face vector:** Compute the average face vector Ψ=$(1/m)$×i=1mΓi
4. **Subtracting the mean face:** Subtract the mean face vector from each vector; φ=[$_{\Gamma 1}$−Ψ,Γ2−Ψ,...,Γm −Ψ]. The dimensions of φ should be (N×N,m).
5. **Computing the covariance matrix:** Compute the covariance matrix C=$(1/m)$ × $\varphi\varphi t$, where φt denotes the transpose of φ. The dimensions of C should be (m,m).
6. **Computing the eigenvectors (eigenfaces):** Compute the eigenvectors (eigenfaces) U of C. The dimensions U should be (m,K), where K is the desired number of principal components.
7. **Finding the weight vector for each image:** Use the formula $\Gamma_{i = j=iKWij\times Uj}$, where Γ$i$ is the reconstructed face image, $_{Wij}$ the weights for the $_{jth}$ eigenface, and Uj the $_{jth}$ eigenvector (eigenface). The dimension of $_{Wi}$ should be (1,K).
8. **Form the Weight matrix:** Concatenate the weight vectors for all images to form the weight matrix WT=[W1,W2,...,Wm], where the dimensions $_{W}$ should be (K,m).

b. Testing Phase:

1. Subtract the average face vector Ψ from the query image vector I_query.
2. Compute the weights W_query for the query image.
3. Calculate the distances between W_query and all weight vectors W obtained during the training phase.
4. Add a scaling factor to the distances between the query image's weights and the training weights.
5. Sort the calculated distances in ascending order.

The researchers enhanced the Eigenface Algorithm by incorporating a distance-based scaling method used during the testing phase. This allows the system to interpret the distance between the camera and the subject's face, ensuring optimal recognition performance. By employing diverse datasets that reflect a range of image conditions and environments, the researchers can thoroughly assess the effectiveness of the proposed enhanced Eigenface algorithm. The process outlined demonstrates how the enhanced Eigenface Algorithm utilizes a distance-based scaling factor to accurately gauge the device's proximity to the user's face, paving the way for improved facial recognition capabilities for identifying spoofing attacks.

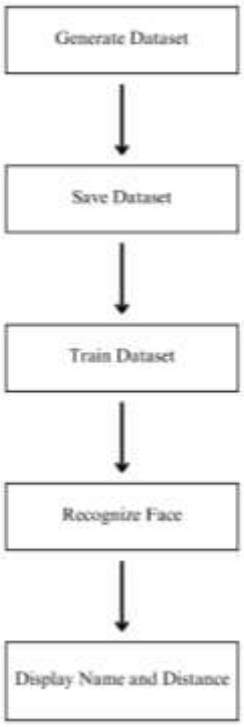

Fig. 1 System GUI

Figure 1 showcase the system GUI which the enhanced Eigenface Algorithm generates and saves the dataset for training. During this training process, the algorithm detects variances in human facial features and compares them to the user's stored dataset. When the Eigenface Algorithm identifies similar features, it automatically recognizes the user's face. Upon recognition, the system interprets the distance of the face from the device using distance-based scaling methods implemented by the researchers. Once this entire process is completed successfully, the system displays the user's name along with the facial distance to the camera.

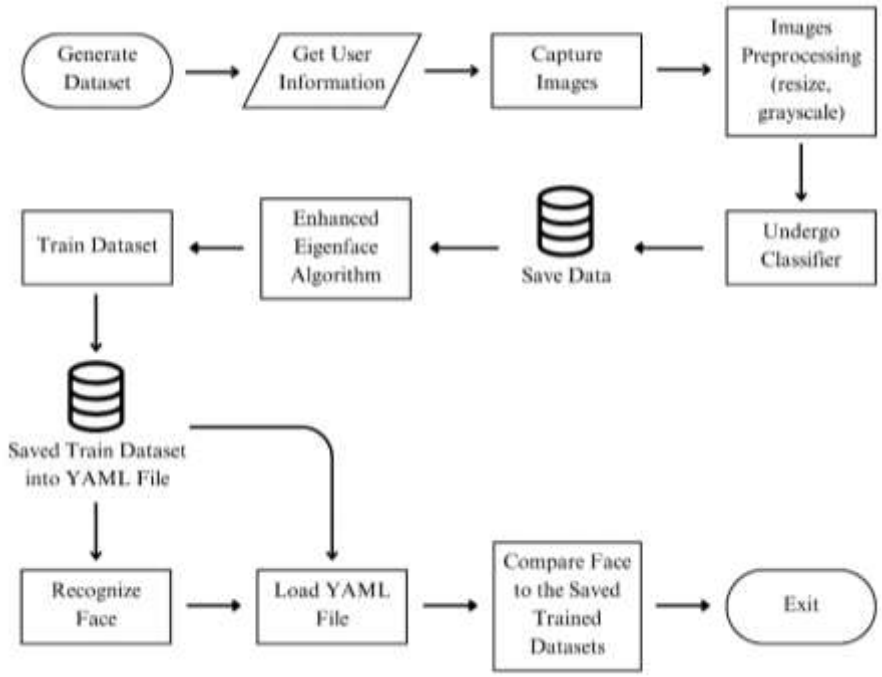

Fig. 2 Diagram of the System Process of the enhanced Eigenface Algorithm

In Figure 2, the diagram depicts the comprehensive process of the enhanced Eigenface Algorithm, which effectively interprets the distance of a user's face from the camera for precise facial recognition. The system initiates by generating a robust dataset and capturing essential user information, including their name. Following this, the system captures images of the user, which undergo thorough preprocessing—resizing and converting to grayscale—before being securely saved. Moreover, the enhanced Eigenface Algorithm incorporates a distance-based scale that accurately measures the proximity of a person's face to the camera. Researchers have determined an optimal distance range of 30 cm to 60 cm; any measurements outside this range are systematically disregarded by the system. The next phase involves training the dataset, with the resulting trained data meticulously stored in a YAML file. Once this training process is complete and the dataset is saved, the system confidently recognizes the user's face and effectively compares it to the stored trained datasets.

3. Result and Discussion

A distance-based scaling factor has been integrated into the existing eigenface algorithm to address its limitations, particularly its failure to consider the facial distance from the camera. This oversight significantly reduces the algorithm's usability, leading to unintended face recognition across varying distances. Tables 1, 2, and 3 present the results of the enhanced eigenface algorithm with the distance-based scaling factor, highlighting its effectiveness in terms of confidence level, recognition time, and the different distances at which it successfully detects a user's face.

Table 1. Results of Recognition Based on the Distance of the Face to Camera

Distance	Is Face Recognized?	
	Existing Eigenface Algorithm	**Enhanced Eigenface Algorithm**
20 cm	No	No
30 cm	Yes	Yes
40 cm	Yes	Yes
50 cm	Yes	Yes
60 cm	Yes	Yes
70 cm	Yes	No
80 cm	Yes	No
90 cm	Yes	No
100 cm	Yes	No
110 cm	No	No

Table 1 shows the result of the comparison of the existing and proposed Eigenface Algorithm concerning identifying faces at varying distances. The existing Eigenface Algorithm and the enhanced Eigenface Algorithm did not identify the face at a 20 cm distance as the minimum distance to detect the user's face at 30 cm. The researcher limits the enhanced Eigenface Algorithm to identify faces at a 60 cm distance to ensure the usability of facial recognition. With this result, the Eigenface Algorithm prevents face recognition attempts at inappropriate distances to avoid spoofing attacks.

Table 2. Comparison of Recognition Time Based on Distance

Distance	Recognition Time	
	Existing Eigenface Algorithm	**Enhanced Eigenface Algorithm**
20 cm	N/A	N/A
30 cm	0.0129 seconds	0.0100 seconds
40 cm	0.0157 seconds	0.0134 seconds
50 cm	0.0182 seconds	0.0155 seconds
60 cm	0.0188 seconds	0.0175 seconds
70 cm	0.0200 seconds	N/A
80 cm	0.0312 seconds	N/A
90 cm	0.0328 seconds	N/A
100 cm	0.0337 seconds	N/A
110 cm	N/A	N/A
Average Recognition Time:	0.0216 seconds	0.0141 seconds

Table 2 illustrates the performance results of both the existing and enhanced Eigenface Algorithm in terms of face recognition time. Analyzing Table 2 reveals that at a distance of 30 cm, the existing algorithm recognized a face in 0.0129 seconds, whereas the enhanced algorithm achieved recognition in 0.0100 seconds, resulting in a 0.0029-second advantage for the enhanced algorithm. Additionally, the existing algorithm recorded a face identification time of 0.0157 seconds, compared to the enhanced algorithm's 0.0134 seconds, reflecting a difference of 0.0023 seconds. At 50 cm, the enhanced algorithm recorded a time of 0.0155 seconds, while the existing algorithm took 0.0182 seconds, showing a difference of 0.0027 seconds. At 60 cm, the existing algorithm required 0.0188 seconds for face recognition, while the enhanced algorithm completed the process in 0.0175 seconds, indicating a 0.0013-second improvement. Overall, the average face recognition time for the enhanced Eigenface Algorithm was measured at 0.0141 seconds, in contrast to the existing algorithm's 0.0216 seconds, demonstrating that the enhanced algorithm was 0.0075 seconds faster on average.

Table 3. Comparison of Confidence Level Based on Distance

Distance	Confidence Level	
	Existing Eigenface Algorithm	**Enhanced Eigenface Algorithm**
20 cm	N/A	N/A
30 cm	78.75 %	93.65 %
40 cm	96.25 %	96.65 %
50 cm	87.08 %	94.43 %
60 cm	71.25 %	90.58 %
70 cm	55.21 %	N/A
80 cm	39.58 %	N/A
90 cm	23.75 %	N/A
100 cm	07.92 %	N/A
110 cm	N/A	N/A
Average Confidence Level:	57.38 %	93.83 %

Table 3 illustrates the confidence levels of both the existing and enhanced Eigenface Algorithms when identifying faces at varying distances. At a distance of 30 cm, the existing algorithm achieves a confidence level of 78.75%, whereas the enhanced algorithm significantly improves this to 93.65%, resulting in a notable increase of 14.9%. At 40 cm, the difference in confidence levels narrows to just 0.4%. At a distance of 50 cm, the enhanced algorithm exhibits a 7.35% increase over the existing one, surpassing the existing algorithm's confidence level of 87.08%. By 60 cm, the enhanced Eigenface algorithm achieves a confidence level of 90.58%, in contrast to the existing algorithm's 71.25%, clearly highlighting the advantages of the enhanced algorithm. It's important to note that the enhanced Eigenface algorithm restricts facial recognition to a maximum distance of 60 cm, so it did not compute confidence levels beyond this range. Overall, the research indicates that the enhanced Eigenface Algorithm achieved a confidence level of 93.83%, significantly higher than the existing algorithm's 57.38%. This represents an impressive increase of 36.45% in confidence levels with the enhanced approach.

4. Conclusions

Facial recognition technology is becoming essential for protecting digital information by recognizing human facial features and comparing them to stored images. However, threats such as spoofing attacks enable cybercriminals to impersonate others and gain access to confidential information. The existing Eigenface Algorithm had limitations regarding the distance of a face from the camera, which created vulnerabilities. Researchers improved the algorithm by introducing a distance-based scaling factor, focusing on distances between 30 cm and 60 cm. This enhancement resulted in a recognition confidence level of 93.83% and an improvement of 36.45%. Additionally, the enhanced algorithm recognized faces more quickly, averaging 0.0141 seconds compared to 0.0216 seconds with the existing version. Overall, this enhancement strengthens the algorithm against spoofing attacks by restricting the distances from which it can detect faces, ensuring the usability of the Eigenface Algorithm.

5. References

Aliyu, I., Bomo, M., & Maishanu, M. (2022). A Comparative Study of Eigenface and Fisherface Algorithms Based on OpenCV and Sci-kit Libraries Implementations. *International Journal of Information Engineering and Electronic Business*, *14*. https://doi.org/10.5815/ijieeb.2022.03.04

Andrejevic, M., & Selwyn, N. (2019). Facial recognition technology in schools: critical questions and concerns. *Learning, Media and Technology*, *45*(2), 115–128. https://doi.org/10.1080/17439884.2020.1686014

Bermejo, E., Fernández-Blanco, E., Valsecchi, A., Mesejo, P., Ibáñez, Ó., & Imaizumi, K. (2022b). FacialSCDnet: A deep learning approach for the estimation of subject-to-camera distance in facial photographs. *Expert Systems With Applications*, *210*, 118457. https://doi.org/10.1016/j.eswa.2022.118457

Çarıkçı, M., & Özen, F. (n.d.). A Face Recognition System Based on Eigenfaces Method. *Procedia Technology*, *1*, 118–123. https://doi.org/10.1016/j.protcy.2012.02.023

Firc, A., Malinka, K., & Hanáček, P. (2023). Deepfakes as a threat to a speaker and facial recognition: An overview of tools and attack vectors. *Heliyon*, *9*(4), e15090. https://doi.org/10.1016/j.heliyon.2023.e15090

Parkin, A., & Grinchuk, O. (2019). *Recognizing Multi-Modal face spoofing with face recognition networks*. https://openaccess.thecvf.com/content_CVPRW_2019/html/CFS/Parkin_Recognizing_Multi-Modal_Face_Spoofing_With_Face_Recognition_Networks_CVPR_2019_paper.html

Ramos, A. L. A., Buenafe, P. A., Cabrales, E. K. C., TeñIdo, J. D., & Portas, S. O. (2019, May 1). *Filipino based Facial Emotion Features Datasets using Haar-Cascade Classifier and Fisherfaces Linear Discriminant Analysis Algorithm*. innovatus-pub.github.io.

Teoh, K., Ismail, R. C., Naziri, S., Hussin, R., Isa, M., & Basir, M. (2021). Face Recognition and Identification using Deep Learning Approach. *Journal of Physics. Conference Series*, *1755*(1), 012006. https://doi.org/10.1088/1742-6596/1755/1/012006

Turk, M. (2006). EIGENFACES AND BEYOND. In *Elsevier eBooks* (pp. 55–86). https://doi.org/10.1016/b978-012088452-0/50003-0

Turk, M., & Pentland, A. (1991). Eigenfaces for recognition. *Journal of Cognitive Neuroscience*, *3*(1), 71–86. https://doi.org/10.1162/jocn.1991.3.1.71

Wahyuningsih, D., Kirana, C., Sulaiman, R., Hamidah, & Triwanto. (2019). Comparison of the performance of Eigenface and Fisherface algorithm in the face recognition process. *IEEE Xplore*. https://doi.org/10.1109/citsm47753.2019.8965345

Wirdiani, A., Lattifia, T., Supadma, I., Mahar, B., Taradhita, D., & Fahmi, A. (2019). Real-Time Face Recognition with Eigenface Method. *International Journal of Image, Graphics and Signal Processing*, *11*. https://doi.org/10.5815/ijigsp.2019.11.01