CONCORDIA INSTITUTE FOR INFORMATION SYSTEMS ENGINEERING (CIISE)

CONCORDIA UNIVERSITY

INSE 6150

SECURITY EVALUATION METHODOLOGIES

JEREMY CLARK

SECURITY EVALUATION OF FACIAL BIOMETRIC TECHNOLOGY: ASSESSING VULNERABILITIES, AND COUNTERMEASURES

REPORT BY

OKOYE ELVIS EMEKA

40274904

ABSTRACT

Authentication is a crucial element within the C.I.A (Confidentiality, Integrity, Authorization) triad, which plays a vital role in todays' security frameworks. It refers to the ability of a system to verify the validity of a user and confirm their authorization to access a system or resource. In the area of authentication, biometrics emerges as a pivotal player in modern security paradigms. Various forms of biometric authentication have been explored, encompassing fingerprints, hand vein patterns, voice, retina scans, and iris recognition. Notably, facial recognition technology has witnessed widespread adoption in diverse sectors, including authentication, surveillance, and access control. This paper presents a comparative analysis of facial biometric authentication, evaluating its reliability and efficiency within the context of contemporary security applications. The study also examines a range of facial biometric algorithms, including Eigenfaces, Fisher faces, and Convolutional Neural Network, and evaluates each algorithm using a dataset of conditions such as lighting, pose, facial expression, and false rate test. Furthermore, the research delves into the practical application of facial authentication and explores the vulnerability and potential threats faced by biometric system authentication.

INTRODUCTION

In an era dominated by digital advancements and heightened concerns regarding security and identity verification, the demand for robust security measures is escalating. Facial biometric authentication has emerged as a promising solution, ensuring secure access to critical data and information [1]. Its widespread integration into various facets of daily life, ranging from smartphone authentication [2] to surveillance systems, underscores the significance of biometrics in modern security.

Facial biometric authentication operates in two ways: the camera tracks key facial points, such as the eyes and nose, calculating distances between them; alternatively, the system analyzes distinct regions on the face, comparing contours and textures to create a unique topological map. Although facial recognition technology has existed for decades, recent years have witnessed its expanded adoption. Advances in artificial intelligence, deep learning, and systems capable of processing vast amounts of data have brought the technology closer to realizing its full potential, leading to increased accuracy and processing speed. Projections indicate that the global market for facial recognition is poised to reach $4.92 billion by 2027, with the technology making its presence felt in the retail, transportation, hospitality, and banking sectors.

The origins of facial recognition technology trace back to the 1960s. An early system developed by Woodrow Wilson Bledsoe classified photos by manually recording the coordinates of facial features such as the nose and mouth using an electronic stylus. This system could retrieve images closely resembling a given photograph from the database. In the 1990s, initiatives by the US Defense Advanced Research Project Agency and the National Institute of Standards and Technology led to the development of more sophisticated automatic face recognition technology. Early applications, such as the 2002 Super Bowl experiment, highlighted the technology's potential, but it flourished in the 2010s due to rapid advancements in artificial intelligence.

Facial recognition technology, while instrumental in safety and security, has sparked controversy. Law enforcement employs it for crime prevention, locating missing persons, and identifying suspects. Despite its increasing speed and accuracy, concerns over privacy have led some cities to consider banning facial

biometrics [3]. Researchers have pointed out that the technology can be circumvented, with anti-facial recognition glasses making wearers undetectable. Nevertheless, its prevalence in mobile devices, consumer products, educational settings, retail establishments, and automotive applications continues to rise [5]. From attendance tracking in college classrooms to theft prevention in retail, facial recognition technology finds diverse applications, reflecting its growing influence in various sectors [6]

EVALUATION OF FACIAL RECOGNITION ALGORITHMS

EIGENFACE

The fundamental concept underlying the eigenface method revolves around utilizing eigenfaces, as opposed to original images, for the purpose of comparison. Eigenfaces are essentially the eigenvectors derived from the covariance matrix of the dataset [8][9][10]. The rationale behind adopting the eigenfaces approach lies in its capacity to represent inputted data more efficiently. Each individual face is expressed as a linear combination of eigenfaces, contributing to a more streamlined representation of the data. Achieving this efficiency requires a dimension reduction technique, and in this context, Principal Component Analysis (PCA) is employed to extract the desired number of principal components from the multidimensional data [4][13].

PCA operates to eliminate redundant information, thereby reducing the dimensions of the data and accurately organizing the facial structure into orthogonal principal components, commonly referred to as eigenfaces [11].

The recognition process involves several steps:

Reading the images in the database.

I. Computing the mean for the images.
II. Determining the deviation of the inputted images in the database from the mean image.
III. Evaluating the centered image matrix based on the differences identified in the previous step.
IV. Identifying the eigenvectors of the covariance matrix, which represent the eigenfaces. The resulting image, in the end, resembles a ghost.

In the context of recognizing unknown faces, the process involves:

I. Feeding a test image into the program.
II. Computing its eigenface components through the initialized process.
III. Calculating the Euclidean distance between these components and those previously identified.

FISHERFACES

The Fisher face methodology shares similarities with Eigenfaces as it employs Principal Component Analysis (PCA) in its implementation [14][15]. However, a key distinction lies in the integration of Linear Discriminant Analysis (LDA). LDA, a linear discriminant classifier, aims to segregate two distinct classes from each other. In cases where there are two distinct classes, LDA seeks to maximize the separation between them while minimizing the separation among objects within similar classes[17]. Essentially, it distinguishes dissimilar objects while minimizing the distance between objects that share similarities.

The Fisher face initially applies PCA to diminish the dimensionality of image dimensions before subsequently employing LDA to discriminate between classes.

Implementation proceeds as follows:

I. Application of PCA to reduce dimensionality.
II. Application of Fisher LDA to distinguish between multiclass independent variables.
III. Construction of the centered matrix and calculation of the average face using the mean minus the image vector.
IV. Computation of the covariance matrix and determination of eigenvalues and eigenvectors.
V. Projection of all training images onto the subspace that maximizes class separation.

In the context of recognizing unknown faces, the process involves:

I. Selection of a test image from the database subspace.
II. Measurement of the distance between the new face and the templates of faces in the training set.
III. Differentiation of classes using the closest face in the training database.

Convolutional Neural Network (CNN)

At its fundamental level, neural networks undergo a training process where they ingest data, recognize patterns within that data, and subsequently predict outcomes for new sets of similar data [12]. The architecture of a neural network comprises layers of neurons, serving as the central processing units. In a CNN, there are two primary layers: the input layer, which receives input, and the output layer, responsible for predicting the final output [16]. Between these layers are the hidden layers, where the majority of computational tasks are executed.

The CNN operates by comparing multiple images to learn and adapt its model.

I. The initial step involves taking an image and extracting its pixel density.
II. Each pixel then becomes input for neurons in the first layer, and channels connect neurons between successive layers.
III. Each channel is associated with a numerical weight. The inputs are multiplied by their corresponding weights, and the sum is sent as input to the neurons in the hidden layer.
IV. These hidden neurons are linked to a numerical value known as bias, which is added to the input sum.
V. The result passes through an activation function, acting as a threshold, determining whether a neuron will activate.
VI. Activated neurons then transmits data to the next layer through channels, and this process, known as forward propagation, continues throughout the network.
VII. In the output layer, the neuron with the highest value activates, determining the output. These output values are probabilistic, introducing the possibility of errors. The network mitigates this by training on extensive data, adjusting its weights based on the comparison between predicted and actual outputs.
VIII. Back propagation follows, where the direction and magnitude of the error are fed back into the network, prompting adjustments to the weights.

The iterative cycle of forward propagation and back propagation continues with multiple inputs until the weights are refined sufficiently for the network to accurately predict images from a set of testing samples.

EVALUATION CITERIA

Varying Light Condition

Eigenfaces

Eigenfaces exhibit sensitivity to variations in illumination, which significantly influences their performance [9]. The impact of illumination variations on eigenfaces can lead to diminished effectiveness since they rely on the principal component analysis of the entire dataset.

Fisherfaces

Fisherfaces on the other hand demonstrates a better capacity to handle changing light conditions compared to eigenfaces. They are capable of distinguishing between individuals even in varying light environments by prioritizing discriminative traits during the training process.

Convolutional Neural Networks (CNNs)

Convolutional Neural Networks (CNNs) exhibit a high degree of adaptability to navigate different lighting situations. Their proficiency comes from their ability to capture hierarchical characteristics, allowing them to acquire reliable representations even in the presence of variations in lighting conditions [16].

Pose

Eigenfaces

Eigenfaces encounter challenges when faced with fluctuations in posture. Significant deviations from the poses observed during training may result in misclassifications, as eigenfaces are not inherently equipped to handle changes in posture.

Fisherfaces

Fisherfaces exhibit a greater tolerance for drastic pose changes compared to eigenfaces, though they are still not entirely immune to such variations. Despite their relatively enhanced resilience, significant deviations from the training positions can lead to a decline in their performance [17].

Convolutional Neural Networks (CNNs)

In the subject of pose variations, Convolutional Neural Networks (CNNs) surpass both eigenfaces and Fisherfaces in resilience. The convolutional layers of CNNs are well-suited for recognizing faces in a diverse range of positions due to their capacity to autonomously learn hierarchical characteristics that remain invariant to translation and rotation.

Facial Expressions

Eigenfaces

Eigenfaces, subject to their limitations with posture changes, lack inherent adaptability to alterations in facial expression [4]. They may overlook subtle differences in facial characteristics induced by diverse expressions.

Fisherfaces

While Fisherfaces may not excel in managing variations in facial expressions as effectively as eigenfaces, their primary strength lies in their capacity to capture identity-related distinguishing features.

Convolutional Neural Networks (CNNs)

Convolutional Neural Networks (CNNs) excel in interpreting variations in facial expressions [12]. Due to their capacity in identifying faces across a spectrum of emotional states is attributed to their ability to learn hierarchical characteristics, enabling them to capture both low- and high-level data associated with facial emotions.

False Match Rate (FMR) and False Non-Match Rate (FNMR).

Eigenfaces

Eigenfaces, a facial identification system based on Principal Component Analysis (PCA), is known for its user-friendly nature and effectiveness. However, in real-world scenarios, it may encounter challenges adapting to variations in lighting, posture, and facial expressions. These challenges can lead to elevated False Match Rates (FMR) and False Non-Match Rates (FNMR) [1] [7]. In practical applications, Eigenfaces might not exhibit the same level of accuracy as more intricate techniques, especially in challenging conditions.

Fisherfaces

Leveraging class-specific information through linear discriminant analysis (LDA), Fisherfaces surpass Eigenfaces in performance. In contrast to Eigenfaces, Fisherfaces generally exhibit greater resilience to variations in lighting and facial positions. While Fisherfaces can prove valuable, challenges may arise in complex environments, potentially leading to false positives or non-positives. The efficacy of Fisherfaces is intricately linked to the quality of the training data and its ability to capture relevant facial features.

Convolutional Neural Networks (CNNs)

Convolutional Neural Networks (CNNs) have demonstrated exceptional performance across various computer vision tasks, notably excelling in facial recognition. CNNs strength lies in their ability to learn hierarchical features, enabling them to detect complex patterns and variations in facial appearances. When subjected to extensive and diverse datasets during training, deep learning techniques such as CNNs have the potential to yield reduced False Match Rates (FMR) and False Non-Match Rates (FNMR). CNNs excel in handling challenging scenarios, showcasing adaptability to diverse facial expressions, positions, and lighting conditions. However, the efficacy of CNNs may be influenced by factors such as the availability and quality of training data, as well as the specific architecture and parameters utilized. Despite these potential limitations, their robust performance makes them a powerful tool in the field of facial recognition.

Category	*Varying light Conditions*	*Pose*	*Facial Expressions*	*False match rate and non-false match rate*
Eigenfaces	○	○	◎	○
Fisherfaces	◎	○	○	◎
Convolutional Neural Network	●	●	●	●

Table 1. A comparison of Facial Biometrics Algorithm. A full dot indicating the algorithm meets all requirements, half dot indicating the algorithm partially meets the requirement and a no dot indicating the algorithm doesn't do a good job when it comes to meeting the necessary requirement of a facial biometric system.

LIMITATIONS AND CHALLENGES WITH FACIAL BIOMETRICS

Stored Data:

Biometric Authentication stands out as one of the most secure means of authentication, as it relies on unique physical characteristics inherent to individuals. The distinctiveness of facial features, even among identical twins, reinforces the security of this authentication method. Notable differences in facial structures, such as the relative position of the eyes to the ears or the distance from the nose to the chin, contribute to the individuality of each person's face.

However, the inherent strength of biometric data becomes a potential vulnerability in the event of data theft. Unlike passwords, which can be changed swiftly and easily if compromised, facial biometric data is immutable – altering one's face is not a viable option. Consider the scenario of a phishing attack attempting to gain access to a Twitter account. In most cases involving password resets, a victim receives notifications and can promptly change their password and associated information. But, if facial biometrics was used to secure the victim's Gmail account, the victim would face a unique challenge. Unlike passwords, biometric data cannot be altered hastily, leaving the individual at the mercy of the attacker. This scenario underscores the potential risks associated with biometric data theft and the challenges in securing such data.

Spoofing Attacks:

Spoofing attacks pose a significant challenge to the efficacy of biometric authentication, exploiting the simplicity and user-friendly nature of the technology. Researchers have explored various methods to deceive or spoof facial biometrics, with one prevalent tactic involving presenting an image of the victim to the system. The objective is to trick the system into recognizing the displayed image as the authentic person.

More sophisticated spoofing attacks have emerged, including the use of deep fake faces and the highly advanced technique of employing 3D prints of the victim's face. A notable instance of such a spoofing attack occurred in China, involving a criminal duo who manipulated the government agency tax system. This complex scheme utilized facial recognition software, and the attackers employed deep fakes—computer-generated videos of individuals. To enhance the illusion, artificial intelligence was employed to

simulate natural head movements, such as nodding or turning, fooling the system's liveness detection feature. Despite efforts to implement liveness detectors in facial recognition systems, there are methods to circumvent them. A security researcher once demonstrated this by creating a printout of someone's face, cutting out the eyes, and placing the printout in front of their face. This maneuver allowed the individual's real eyes to peer through the holes, effectively tricking the liveness detection feature of the camera or facial recognition system.

Aging, Growth, Lighting, and Pose:

Facial biometrics encounter significant challenges due to factors such as aging, growth, lighting, and pose. The effect of aging raises questions about the system's ability to adapt to changes in a person's facial features over time. As individuals age, certain facial structures may change, and elements like hair loss can further alter one's appearance. The challenge lies in the system's ability to effectively recognize and accommodate these changes for accurate identification.

Likewise, variations in lighting conditions and poses present substantial difficulties. Imagine a situation where a person is in a dimly lit environment, and the system is tasked with recognizing their face under these challenging lighting conditions. Or consider changes in facial expression, such as transitioning from a smiling expression (as stored in the database) to a neutral or frowning expression during authentication, which add further complexities. The question then arises: How does the system navigate these pose and lighting variations to ensure accurate and informed identification? These are the challenges that facial biometric systems must overcome to ensure reliable and accurate performance.

Ethical Disadvantage:

Facial biometrics has faced sustained scrutiny due to significant ethical concerns, particularly related to privacy issues. The unsettling idea of a technology having the capability to single out individuals in a crowd, track their movements, and make subjective judgments about their character has been a focal point of criticism. The increasing attention on facial recognition technology underscores its potential drawbacks, as people are naturally apprehensive about a technology that could compromise their safety, autonomy, or even their fundamental liberties.

Of particular concern is the ethical subject related to the technology's performance across different racial groups. For instance, there have been apprehensions about facial biometrics exhibiting a 0.18% false positive rate for representing a white person, while concurrently having a significantly higher 14% chance of failing to recognize an individual of a different race [3]. These disparities raise additional ethical considerations, further intensifying the debate surrounding the widespread use of facial biometrics.

SOLUTIONS TO SOME CHALLENGES FACED BY BIOMETRICS

Stored Data Solution:

Addressing the concern of stolen facial data, a potential solution lies in the tokenization of biometric data. It is crucial to recognize that in facial biometrics, the actual image of the person is not stored on the server.

Instead, a facial print data, known as a token, is retained after undergoing calculations for accurate user identification. Therefore, if an individual's facial fingerprint is compromised on a server, what is taken is not a photograph but rather a tokenized mathematical data representing the facial features.

However, this alone doesn't completely solve the issue. Your face is still what was tokenized, so if that's stolen, they still have your facial data that cannot be changed. A potential solution to this is to append a random or nonce value to the facial data. This way, if your facial data is stolen, it's not your actual facial data that's stolen, but a scrambled data. This allows your facial data to be changed with ease. Now, all you have to do is re-input or re-enter your face into the application, and a new facial biometric data appended with the nonce or random data will be your new facial biometric data for that application.

Spoofing Attacks Solution:

A technology known as liveness tech is widely employed by various services globally to ascertain the authenticity of a person on the other end of a phone or computer screen. Liveness technology utilizes an infrared (IR) blaster to project approximately 30 thousand invisible dots onto a person's face, effectively constructing a 3D face map. This map is then scrutinized for specific properties such as noise texture and glare, capitalizing on the distinctive way human skin reflects light, which differs from materials like silicone masks or phone screens. While the human eye may not discern these nuances, a neural network is adept at detecting them.

Upon uploading the image into the system, it undergoes an in-depth processing to facilitate the detection of forgeries. For instance, if an individual moves their head in front of the camera, it impacts the image seen by the camera, as the person approaches the lens, the proportions of their face may not change uniformly; for instance, their nose might appear larger. Liveness technology is meticulously crafted to adapt and engage with such variations. When a person turns their head, the system performs multiple checks, making it virtually challenging for someone to circumvent the technology using a static image. This adaptability is the key strength of liveness technology, making it highly effective in verifying the presence of a real human being on the other side of the camera.

Aging/growth/lighting and pose Solution

Facial recognition technology has made significant advancements in recent years, and has made some of those advancement in aging and growth, and it has done this with a 3D recognition system known as DeepFace. This system takes a 2D photograph of an individual and transforms it into a three-dimensional model of the face. This innovative approach enables the comparison of images captured from different angles or poses, effectively addressing the challenge of pose variation. Aging is also mitigated as a concern, given that the face recognition system has undergone refinement. It now constructs facial representations from areas featuring rigid tissues and bones, such as the curves of the eye socket or the chin of the nose—areas that remain relatively consistent as an individual ages.

The remarkable accuracy of DeepFace is primarily attributed to a computational teaching technique called deep learning. This methodology employs algorithms to iteratively refine its understanding, learning from both correct and incorrect face matches. Each successful or unsuccessful comparison contributes to the system's memory, creating a roadmap of connections. Through repeated iterations, the network of connections on this map expands, enhancing the system's accuracy in face recognition. The underlying

concept is for the computer to develop a network of connections similar to the functioning of neurons, ultimately optimizing its efficiency.

CONCLUSION

In the ever-evolving landscape of security technology, facial biometrics have emerged as a forefront solution, promising secure and efficient identity verification. The study evaluated various algorithms used in facial recognition, including Eigenfaces, Fisherfaces, and Convolutional Neural Networks (CNNs). These algorithms form the backbone of modern facial recognition systems, each contributing unique strengths to address various facets of facial feature recognition and analysis. Eigenfaces and Fisherfaces, while effective, demonstrated certain limitations in handling variations in lighting, pose, and facial expressions. On the other hand, CNNs showed remarkable resilience to these challenges due to their ability to learn hierarchical features.

However, the deployment of facial biometric technology is not without its challenges. Privacy concerns, potential biases, facial data theft and the need for robust security measures have been key areas of focus. To address these issues, solutions such as tokenizing and encrypting facial data stored in centralized servers serve as crucial safeguards, ensuring that sensitive information remains protected from unauthorized access. Advancements in deep learning, particularly the advent of deep face technology, demonstrate the industry's commitment to overcoming persistent challenges such as aging and face changes. These innovations contribute to the adaptability of facial recognition systems, enhancing their performance across diverse scenarios and environments.

Overall, while facial biometric technology presents certain challenges, ongoing research and technological advancements continue to enhance its effectiveness and reliability in security applications. As the field continues to evolve, it is anticipated that these technologies will become even more robust and secure, paving the way for broader adoption in various sectors.

REFERENCES

[1] R. D. Inioluwa and G. Fried, "About Face: A Survey of Facial Recognition Evaluation".

[2] M. . G. Galterio, S. A. Shavit and T. Hayajneh, "A Review of Facial Biometrics Security for Smart Devices," 2018.

[3] L. Pang, "Research on the Privacy Security of Face Recognition Technology," 2022.

[4] W. ZHAO, R. CHELLAPPA, P. J. PHILLIP and A. ROSENFELD, "Face Recognition: A Literature Survey," 2003.

[5] K. Modi and L. Devaraj, "Advancements in Biometric Technology with Artificial Intelligence," 2022.

[6] S. S. Harakannanavar, C. R. Prashanth and K. B. Raja, "Comprehensive Study of Biometric Authentication Systems, Challenges and Future Trends," 2019.

[7] . P. Sanmoy and S. Acharya, "A Comparative Study on Facial Recognition Algorithms".

[8] M. N. A. Rahman, A. R. Armanadurni , H. Afzaal, Seyal and N. Kamarudin, "Facial Recognition Using Eigenfaces Approach," 2014.

[9] C. Kline, "Eigenface for face detection," 2017.

[10] S. Ravi and S. Nayeem, "A Study on Face Recognition Technique based on Eigenface," 2013.

[11] M. A. Takalkar and M. Gaikwad, "Face Recognition Using Eigenfaces," 2011.

[12] M. Kumar, "Face Recognition Using Eigen Faces and Artificial Neural Network," 2010.

[13] T. Heseltine and J. Austin, "Evaluation of Image Pre-Processing Techniques for Eigenface Based Face Recognition," 2002.

[14] P. N. Belhumeur, J. P. Hespanha and D. Kriegman, "Eigenfaces vs. Fisherfaces: Recognition Using Class Specific Linear Projection," 1997.

[15] V. Y. Lata, C. Kiran, R. M. R. Hanmanth and A. Govardhan, "Facial recognition using eigenfaces by PCA," 2009.

[16] S. Yaacob, H. Desa, P. Saad and a. y. shakaff, "Face Recognition using Eigenfaces and Neural Networks," 2006.

[17] M. Anggo and La Arapu, "Face Recognition Using Fisherface Method," 2018.