EAI Endorsed Transactions
on Intelligent Systems and Machine Learning Applications Research Article EAI.EU

Timing for securing the biometric template transformation based on supervised learning using Double Random Phase Encoding Method

Mahmoud Nasr[1,2]and Pascal Muam Mah*[3,4]

[1]Department of Biocybernetics and Biomedical Engineering AGH University of Science and Technology, Poland.
[2]Faculty of Engineering and Technology, Future University in Egypt, Cairo, Egypt.
[3]Department of Information and Communication Technology, AGH University of Science and Technology
[4]Faculty of Computer Science, OPIT-Open Institute of Technology, Malta

Abstract

Background: Among optical encryption techniques, Double Random Phase Encoding (DRPE) is one of the most widely used. Individual identities and the recognition process remain essential to ensuring proper data access security. **Aim:** The study aims to optimize an approach that ensures the significant performance effectiveness of cancelable biometric methods for different templates and the associated time taken to transform biometric data. **Problem:** This study focuses mainly on the effectiveness of cancelable biometric methods that measure the probability that an authorized effort may be mistakenly rejected as unauthorized. In addition, when compromised, several nonrenewability safety challenges arise, and insufficient matching performance templates are required to build a security protection method. **Method and material:** The study uses supervised learning for the Double Random Phase Encoding Method (DRPE), a 4F optical encryption system, and 20 randomly chosen images from the ORL database of faces. **Results:** The result based on supervised learning for the Double Random Phase Encoding Method revealed false favorable rates for both fingerprint and face templates. **Conclusion:** The study concluded that the effectiveness of the cancelable biometric performance in this study has a false positive rate probability that an authorized effort may not be mistakenly rejected as an unauthorized one.

Received on 02 February 2025; accepted on 05 June 2025; published on 18 June 2025

Keywords: Biometric security, supervised learning, Double Random Phase Encoding, Biometric templates

Copyright © 2025 M. *Nasr*, licensed to EAI. This is an open access article distributed under the terms of the Creative Commons Attribution license (http://creativecommons.org/licenses/by/4.0/), which permits unlimited use, distribution and reproduction in any medium so long as the original work is properly cited.

doi:10.4108/eetismla.8773

1. Introduction

The scope of applicable biometric systems is rapidly expanding due to advances in technology. Biometric identification is widely being used in verifying several internets of things (IoTs) applications [19]. As system amalgamate to remote-based, there is need for biometric application especially as the cloud-based computing on the rise. There is need for performance-based authentication to ensure accuracy in personal access. Cloud based computing requires high level security which can be achieved only with a proper biometric system. Cancelable biometric systems are one of the data identify systems that is promising to uphold better security standards [9]. The growing era of process automation in areas like digital banking, online shopping, online studies, online trading, online entertainment required high level security due a lot of association with automated process and human data. Much of management of human resources have shifted to digital services which shows that more of human data is available in the online system. Without proper data security measures, humans are vulnerable to data bridge, cyberpunk, bullying and theft [36]. Recent advance developments in machine learning are also another era that promises better understandable algorithms that allow users to train and learn from daily circumstances. Machine learning as a computational

*Corresponding author. Email: pascal.muammah@faculty.opit.com system that allows users to train computers to learn from the input data and teaches users with output data. Learning from datasets has gained so much popularity in recent years that a lot has changed to just perceived imputation of data to computer predictions. Humans, Institutions, establishments, and organizations are now heavily dependent on this system to facilitate decision making based on their accuracy and reliability. The metamorphosis within the paradigmatic machine learning has amalgamated to a new system called deep learning. Deep learning which is a subset of machine learning uses training frames of machine learning to understand associated data to predict outputs. With the much transformation in the world today, from a single, multiverse and blended traditional computing approach to a cloud-based computing, there is a need to ensure proper security [6]. Modern machine learning techniques have been developed to ensure information security. Due to human nature complexity, there have been a lot of challenges to properly safeguard human details. With many associated challenges associated with understanding human data and preserving human mistrust with accuracy and reality, threats have remained predominant. Mah et al., [?] have developed an AI-driven system for facial-age detection that is integrated with IoT to enhance the security of data on social media. Their innovative approach guarantees that users, particularly minors, are provided with age-appropriate content access, thereby protecting them through the enforcement of visibility rules and the advancement of content regulation via intelligent automation and secure data management.

Cancelable biometric templates have emerged as one of the advancements in technology to secure human data [28]. Even though this security system promises to enhance and safeguard human data from being stolen, there have been weaknesses within the system itself. The cancelable biometric templates are quite inflexible to be stored across different systems. This study introduces a transformable approach that aims to ensure proper data security and limited privacy bridge. Neural network is one of the few aspects of deep learning that facilitates the process of information retrieval. For instance, Siddhad et al., [23] uses convolutional auto encoders to a cancelable biometric template to enhance a classical machine learning paradigm to a novel deep learning architecture. The authors use this as a great tool for extraction of features from an image by compressing the image to a lower dimension using latent vector space. To achieve this the authors, use palm vein, wrist vein and palm tree image combined with different datasets like CASIA, CIEPUT and PolyU. The world is shifting to a cloud-based system which requires higher level security. The cancelable biometrics templates are a novel approach that will transform machine learning to deep learning architecture for proper security.

2. Literature Review

This section provides definitions of key terms, discusses the importance of cancelable biometric templates, outlines the types of cancelable biometric templates, highlights the pillars of biometric cancelable templates, and addresses the challenges associated with cancelable biometric templates.

2.1. Definition of key terms

Cancelable biometric templates: This is a form of biometric technology that has the most recognized options that consist of fingerprint mapping, facial recognition, and retina scans [33], [30]. Rathgeb & Uhl, [15], said is biometric transform that is designed in a way that it should be difficult computationally to regain the original biometric data.

Machine learning: This is a computer science field and a branch of artificial intelligence focused on the use of information and the set of rules and regulations (algorithms) that imitates humans learning aspects by improving its accuracy [1],[27],[13].

Deep learning: This is a computer science field and branch of machine learning with a set of rules and regulations (algorithms) that uses pattern layers to transmit higher-level extracted features from the raw input to predict its outcome [25]. Mahdavinejad et al., [8] said deep learning is an algorithms explaining how different techniques are applied to the data to extract higher level features.

Cloud computing: This is the art of delivering computing services via the internet using servers, storage, networking, databases-software, analytics, and intelligence [26],[21]. Kim, [32], said cloud computing is compelling paradigm for servicing computing needs for both enterprises and end customers

2.2. Deep Learning and cancelable biometric templates

Abdellatef et al., [34], propose a multi-biometric cancelable method of face recognition that (CNNs) extract deep features from different facial frame using multiple convolutional neural networks (CNN). According to the authors fingerprints defined the physiological features of an individual which makes it possible for deep neural networks to easily generate features unique to a user based on deep learning systems. Deep learning especially neural networks has the capability of authenticating human features and can predict a danger is one is observed or identified. Also, Talreja et al., [17], said cancelable biometric template can secure achieve a multibiometric template by using a selection of a different set of reliable and discriminative features for each user. According to the test results, with the application of deep learning for cancelable biometrics, it was possible to generate a multibiometric template by using a selection of a different set of data for every user. Abd El-Rahiem et al., [2], proposed a deep image transfer style and a fusion process system to the biometric authentication. The study aims at transferring fingerprints, finger vein and face images by way of cascading human biometric data. Sandhya et al., [29], proposed a multi-instance cancelable iris system that uses a convolutional neural network trained input dataset. Their approach extract and stores the feature as a cancelable template using convolutional neural network to trained using triplet loss for feature extraction.

2.3. Cloud Computing and cancelable biometric templates

As the world technology shift from traditional computing, storing and management of information system to the cloud-based systems, the study carefully examines the new changes that come along with users' security. The following paragraphs present instances and work based on Cloud Computing and cancelable biometric templates for instance, Zhu et al., [38],[7], presents a voiceprint protection approach of homomorphic encryption and authentication system where training allows queries execution by matching users biometric data without decrypting the data enhance security of biometrics. Voice biometric is becoming very essential for used especial as it is very convenient. The digital era require trust in this section and highly encrypted to avoid penetration into personal server by malicious users with the help of computer aided voice systems. Soyjaudah et al., [29], proposed a data hiding method that uses embed demographic data in the biometric image to construct a cancelable biometric system. They explained that this approach is one of the methods that can be applied to preserved users' data without exposing their content especial where the data can be expose to cyber threats. From the application and logical presentation, it is likely that te approach can solved the management problem that currently exist with biometric authentication. Eldesouky et al., [10], said cancelable biometric can be constructed by regularly and repeatedly generating a distorted features of biometric to secure and enable data sensitive of users. When regular distortion approach is applied, features of biometric distortion parameters obtain a modified, and new cancelable templates which capable of implementing in the cloud-based computing. To El-Rahiem et al., [9], they said their aim is to exploit by invigorating the criminal efforts aimed at violating the integrity of biometric cancelable. They used multi-biometric cancellable scheme to exploit the functionality of deep learning models to limit the multi-exposure of fingerprints, finger veins, and iris biometrics with the help of Inspection V3 pre-trained model.

2.4. Characteristics of Cancelable Biometric Templates

For any biometric system or method of authentication to be approved, it should contain the following characteristics below. The following characteristics were carefully examined to see that they respond to the needs of users and that of practitioners constantly working to improve the security challenges associated with biometric systems.

Reliability: The characteristics changes in biometric templates has led to a lot of improvement and thus the reliability of the biometric system thanks to the elicitation protocol fusion. To Wang et al., [35], there is need for trust in any reliability in the biometric cancelable templates because it gives hope for practitioners to keep on and fetch for better ways to improve the existing system. Reliability at the level of application, usage and recommendation is very important for a continuous improvement. Lahmidi et al., [18], said the reliability of the cancelable biometric protection system mainly depends on the choice of the mechanism transformation and the approach of the stored templates. They mean that reliability consist of time of classification, extraction time set to build the structure and time set to scatter the new generated set.

Convenience: The cancelable biometrics templates are good because they offer a convenient approach of authenticating an individual's identity. Kim et al., [16], further said that the privacy challenges and security issues associated with biometric templates come from the management level and at the templates themselves. This goes to say that biometric templates are easy to use but difficult to management. This study therefore suggests a method to properly managed biometric templates. Ganjewar et al., [12], said biometric system of checking has become the most convenient way for authenticity as almost all avenues now preferred to use it. They further said in areas like government institutions, malls, private and public gendering now sees biometric checking to be the most responsible and convenient means of personal identification.

Faster authentication: Sudhakar & Gavrilova, [33], proposed a biometric system on cloud-based system that uses ubiquity as an authentication service. Their result shows that highly intensive computational power for biometric authentication ensures a quick response times and high authentication accuracy. Another fast authentication was proposed [13]. They argue that if a system is built that will permit a one-time vector code to be generated during biometric transformation, this will go a long way to improve security, authentication and most importantly improve time of biometric identification.

Scalability: Biometrics-based system of authentication offer a different usability advantage over traditional password method of authentication in that they provide scalability in its entirety [27]. Also, Singh et al., [31], proposed an approach that allows users to authenticate themselves by proposing a cancelable biometric authentication approach that uses CNN, a light weighted deep learning approach and KNN. Their method aims to revocability biometric templates that is projected onto a random subspace called user-specific key.

Verifiability: Abidin et al., [3], proposed a security and privacy biometric authentication based on remote efficient mechanism that verify users details by outsourced computation protocols encrypted messaging.
.

2.5. Basic Pillars of Biometric Templates for Cloud Computing

The following pillars are required for biometric cancelable templates to fulfill the requirements for a smooth cloud computing system. Piccolotto & Maller, [23], they study users' perception to accepting biometric data usages. The process of every system requires mutual trust. There is need for cancelable biometric to fulfil certain requirements and process of transformation. Andrade & von Solms, [4], identified 5 pillars of information security system architecture as per regulation and requirements of ISO 7498/2 documentary. These 5 pillars are made up of Identification/Authentication, Confidentiality, Authorization, Integrity, and Non-Repudiation. For cancelable biometric templates to run effectively with cloud computing, they require a road map for transparency. The following pillars determines a clean sheet information of users to cloud-based systems.

Sensors: Sensors are the most common subcomponents that detect and measure biometric information and digitize it to the desired software.

Templates: Templates are a set of signal processing rules and regulations (algorithms) and techniques that help create biometric templates of a user. Templates can be compared to stored information that matches the existing user profiles.

Decision: In biometric systems, rules and a decision process exist that utilize matching event results. The decision is the third most important pillar of biometric systems.

Governance: For every biometric template to be able to guarantee trust and confidence uniquely, it is required to have a level of identified management system. There exist many forms of biometric systems for personal security and authentication, but there also exist a few management approaches to personal data. The process of personal data is crucial for every biometric template system that we identified in this study.

2.6. Forms of cancelable biometric templates best identified for Cloud Computing

The following paragraphs detail some common types of biometric systems. The difference lies in their distinct uses and applications. The types of biometric systems are explained, along with their importance and the applications where they are required. The following paragraphs provide examples of biometric types commonly used in cloud-based systems.

Fingerprint Recognition. This is a biometric type that exhibits distinctiveness and stability in fingerprints, with continuous and most widely used anatomized features of a system that recognizes a person's identity [20]. Fingerprint recognition is an optical or thermal sensor that collects data digitally and stores it. They are the most popular biometric authentication method and have been in widespread use for more than a century. Fingerprints have about 30 to 40 minutiae points, and no more than two people have eight points in common.

Facial Recognition. This is a biometric system that utilizes computer programs for face recognition, as demonstrated in face recognition experiments [5]. Facial recognition is a system of identification that uses statistical patterns. Facial recognition helps measure the different points on an individual's face with the objective of extracting information and matching it with pre-existing templates that are linked to the extracted person, who uses it to verify their identity.

Iris Recognition. This is a system of recognition that uses special sensors to identify an iris and maps its segments into vectors that include spatial orientation data. Iris recognition information is converted to unique codes and compared with other stored codes. According to Raghava [24], he used iris recognition authentication in a cloud computing-based environment to evaluate its performance as a biometric technique. After their experiment, they concluded that the iris identification method is one of the strongest authentication methods. Yi et al.[37] use cloud-based iris recognition to examine the relationship between cloud computing, storage, and cloud recognition. Ultimately, they concluded that iris recognition is a vital biometric technology.

Voice recognition. This is another form of identification that uses the human voice to recognize the unique biological characteristics of an individual. Voice recognition differs from passwords and tokens in that it requires physical input, as opposed to digital input. According to Ramírez De La Pinta et al.[25], the Rovio robot allows the use of object detection and voice recognition as cloud-based system services for home-based authentication. They concluded that Rovio robots are inexpensive home automation technology based on cloud servers.

Vein Recognition: Vein Recognition is also known as vascular technology. Vein recognition is a biometric identification technique that uses blood vessels to analyze visible patterns on the surface of a user's fingers. According to Jhong et al., [14] proposed a CNN-based palm vein authentication method on a cloud computing platform and their proposed system achieved an effective non-contact palm vein.

2.7. Importance of cancelable biometric templates for Cloud computing

- Highly fraud-resistant.
- Maintains standards of accuracy.
- Uphold originality standards: Little or no room for faking identity.
- Convenience users with experience.
- Verification of originality.

2.8. Challenges associated with cancelable biometric templates for cloud computing

High power computing. To run biometric systems for cloud computing, high-power computing is needed. The automation system, as required by most software for biometric systems, requires a substantial power supply. The reason is due to the nature of most of its processes and the automation process and procedure.

Costly. The cost of running a biometric system is not only time-consuming but also very costly. Cancelable biometric systems are quite costly because they handle highly sensitive software systems and delicate data sets. The process of running a biometric system itself is costly and requires a substantial amount of energy, as well as large amounts of data, which significantly increases its price.

Fragile in storage. More often than not, human-related data are the most complicated and challenging to manage. The biometric system process is quite complicated, as it involves handling personal information that requires privacy, encryption, and transformation. The process from data collection to coding and transformation is very complicated and fragile.

Higher knowledge requirements. The management of biometric systems requires specialists with advanced knowledge of human systems, computer processes, and automation. The field of biometric systems requires experience in mathematics to run a successful automation.

3. Applied Method

This section is based on the following subtopics. Application used: Material Application and Data Analysis.

3.1. Application Used

Double Random Phase Encoding (DRPE) was used in the study. DRPE is widely used because it allows for the easy setup of an optical setup using lenses or software to accomplish it. The optical setup needed for the DRPE algorithm is shown in Fig. 1.

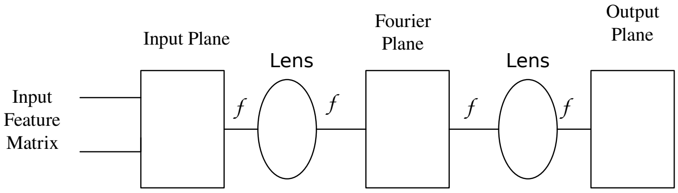

Figure 1. the DRPE encryption setup.

Figure 1 illustrates the 4f optical encryption system, a well-known version of the system. It simply requires two lenses and two random phase masks, and is expandable for four focal lengths. Traditional DRPE encryption involves setting an input image at the input plane, which is one focal length away from the input lens, and obtaining the Fourier transform on the other side of the lens at the same distance. To enhance security, two random phase masks are applied: one at the input plane and the other at the Fourier plane. In the second 2f part of the setup, the second lens is used to perform an inverse Fourier transform (Refregier and Javidi, [28]. Therefore, it is certain that the encrypted image obtained is in the spatial domain in this situation. The DRPE is highly resistant to assaults Frauel et al., [11]; Peng et al., [22].

3.2. Material Application

We used 20 randomly chosen images from the ORL collection to test the proposed cancelable face recognition system. We ran the suggested algorithm using images collected from the ORL database of faces, which was produced between 1992 and 1994 at the laboratories of Cambridge University, to test and assess the effectiveness of the proposed cancelable face recognition technique. This database comprises 10 unique images of 40 distinct subjects, captured under various lighting conditions and emotional states.

3.3. Datasets Analyze

The following figures represent all the data sets used in this experiment to validate the study's results. The

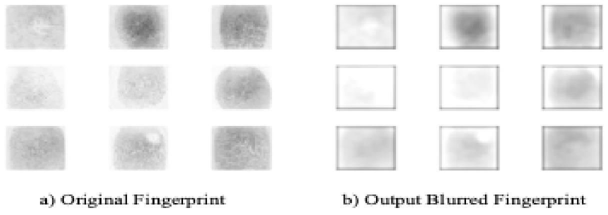

Figure 2. Samples of Fingerprints results.

datasets have been explained at each stage, along with their contributions to the study's novelty.

Figure 2 represents the data sets used for fingerprint analysis, which are used to determine the time required to train the cancelable biometric template. Figure 2a represents the original dataset, while Figure 2b represents the training dataset. From the two datasets, 2a and 2b, we can see that information is visible in 2a but not in 2b.

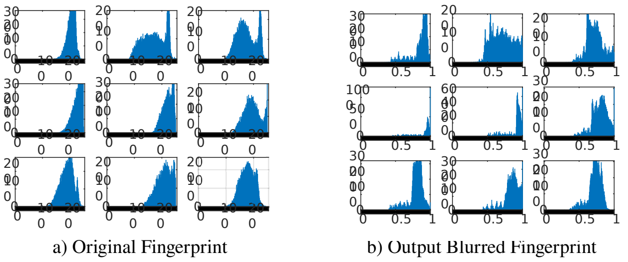

Figure 3. Histograms of original Fingerprints and Output results

Figure 3 represents the histograms of the fingerprint images used as datasets for this study. Figures 3a and 3b, which reveal perceptible variations in histograms of the Fingerprint that have been blurred, enabling the detection of biometric images based on histograms.

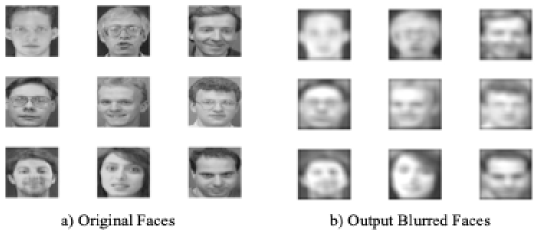

Figure 4. Samples of cancelable face templates generated

Figure 4 represents the face data sets used to analyze the time taken to train the cancelable biometric template. Figure 4a represents the original dataset, while Figure 4b represents the training dataset. From the two datasets, 4a and 4b, we can see that information is visible in 4a, which is before training, but not visible in 4 b after the training dataset.

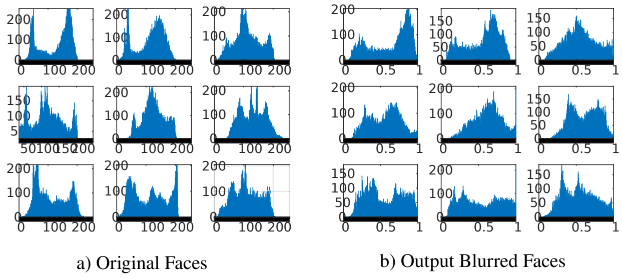

Figure 5. Histograms of original Faces and Output results

Figure 5 represents the histograms of the face images used as data sets for this study. Figures 5a and 5b reveal perceptible variations in the histograms of the blurred faces, enabling the detection of biometric images based on histograms.

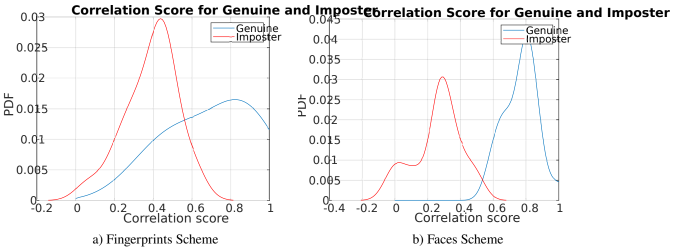

Figure 6. Genuine and impostor distributions for the Fingerprints and the Faces recognition scheme

Figure 6 represents the genuine and impostor distributions for both Fingerprint and face biometric schemes trained for this study using the supervised learning method of the double random phase encoding.

On the cross-correlation graph of the fingerprints, we can see that the intersection between the probability density function distributions is overlapped, indicating that the system cannot differentiate between genuine and imposter fingerprints properly, which leads to incorrect decisions.

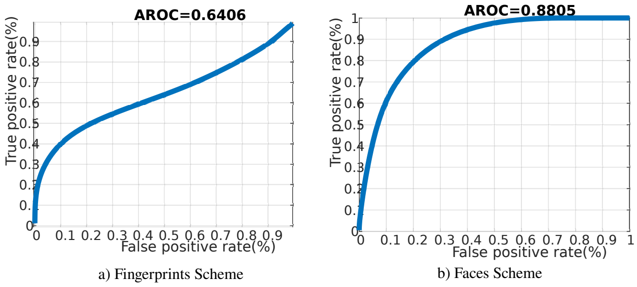

Figure 7. ROC curves for the Fingerprints and the Faces recognition scheme

Figure 7 illustrates the estimated ROC curves for the numerical evaluation of fingerprints and faces, based on the cancellation technique employed. The method indicates that both the fingerprint and face images have a false positive rate. The probability of mismatched identification is low, as shown in the results.

4. Results

In the study, the timing for the securing of the biometric template was examined using the double random phase encoding method (DRPE), and the following statistics were obtained.

4.1. Faces Dataset

The enrollment stage time is: 0.105718 seconds.

The authentication stage time is: 0.423996 seconds.

4.2. Fingerprints Dataset

The enrollment stage time is: 0.128358 seconds.

The authentication stage time is: 0.424651 seconds.

Table 1 explains the results obtained after training the fingerprint and face datasets. The study classified the training process into two levels. Level 1 represents the enrollment stage time, while Level 2 represents the authentication stage time.

The results of this study indicate that face images perform better than fingerprints. The face datasets obtained during training: 0.105718 seconds for the enrollment stage and 0.423996 seconds for the authentication stage. On the other hand, the fingerprint obtained 0.128358 seconds during the enrollment stage time frame and 0.424651 seconds during the authentication stage time frame. From the two categories used in this study, face datasets performed better than fingerprints.

Table 2 compares the two methods numerically while taking the AROC and EER into account. There is little doubt that the suggested cancelable face recognition system performs better than the one based on cancelable fingerprint recognition.

The measurement of metric parameters to determine the distance between the codes generated for new subjects and those kept in the database is a critical component of the performance assessment of a cancelable biometric identification system. The correlation coefficient between the codes of fresh subjects and those stored in the database is used for performance evaluation, as the codes generated in the proposed cancelable facial recognition system are real-valued.

5. Discussion of the Performance

From these images, the cancelable templates are retrieved using two separate comparison situations. The histograms of the fingerprint images from Figure 2 are presented in Figure 3, which reveals hardly perceptible variations in the histograms of the faces that have been blurred. This enables the detection of biometric images based on histograms. On the other hand, Fig. 4 displays the cancelable face templates created using the suggested method. The suggested approach is successful in concealing the specifics of the images. Furthermore, the histograms shown in Figure 5 demonstrate near-uniformity over a specific bandwidth, a desirable quality for high levels of security. The genuine and impostor distributions for both schemes have been computed, as shown in Fig. 6. The ROC curves have also been estimated, as shown in Fig. 7, for the numerical assessment of fingerprints and faces based on the cancelable technique utilized.

Based on the chosen assessment measure, the genuine and impostor distributions are calculated for the two proposed cancelable biometric systems. The False Positive Rate (FPR), False Negative Rate (FNR), and Equal Error Rate (EER) rates are used to calculate the performance effectiveness of the suggested cancelable biometric methods. The FPR measures the likelihood that an authorized effort may be mistakenly rejected as unauthorized. The FNR is the likelihood that an unauthorized effort would be mistakenly accepted as being allowed. The intersection of the real and fake distributions is where the Equal Error Rate (EER) is calculated. The incorrect reject and incorrect accept errors are equivalent at the point where these distributions converge. The security of the system is more effective the lower the EER value. The True Positive Rate (TPR) and the False Positive Rate (FPR) are parametrically related by the ROC curve, where T is a parameter that varies the discriminating threshold. This study will use the ROC curve to assess the effectiveness of biometric technologies. The AROC will be utilized as an indicator of system efficiency. Higher AROC values indicate improved performance.

6. Conclusion

The study concluded that the system, software, application, and biometric category templates determine the effectiveness of cancelable biometric performance, with a false positive rate that ensures that an authorized effort is not mistakenly rejected as unauthorized. The study observed that timing, in this case, matters significantly when training a biometric template. The study observed that the enrollment stage time and the authentication stage time are crucial in determining the likelihood of better performance.

Timing reveals the level at which intruders can gain access to biometric secure datasets and how likely it is to make adjustments to secure biometric templates. When the enrollment stage and authentication stage times are too long, it is detrimental to such a system, especially in a compromised situation.

Table 1. Biometric Security Timing Comparison

Biometrics Security Time	Level 1 Param/sec	Level 2 Param/sec	Comparative Scale
Faces Dataset	0.105718	0.423996	Excellent
Fingerprints Dataset	0.128358	0.424651	Good

Table 2. Numerical Comparison

Biometric Templates Category	Level 1 Parameter per seconds	Level 2 Parameter per seconds	Comparative View Scale
Faces Dataset	0.105718	0.423996	Excellent
Biometric Metrics	ROC	EER	Comparative View Scale
Faces Dataset	0.8805	0.0049	Excellent (Recommended)
Fingerprints Dataset	0.6406	0.0130	Fair (Not Recommended)

Abbreviations

DRPE: Double Random Phase Encoding
ORL Database: Olivetti Research Laboratory Database
CNN: Convolutional Neural Network
IoTs: Internet of Things
KNN: K-Nearest Neighbors
4F System: Four-Focal-Length Optical System
ROC Curves: Receiver Operating Characteristic Curves
AROC: Area Under the Receiver Operating Characteristic Curve
EER: Equal Error Rate
FAR: False Acceptance Rate
FRR: False Rejection Rate

Conflict of Interest

We declare that there no conflict of interest associated with this findings

Funding

No funding available

Ethics Approval

Not Applicable

Availability of data and materials

Datasets used in this study was obtained from https://www.cl.cam.ac.uk/research/dtg/attarchive/facedatabase.html. All analysis and classifications are available as part of this manuscript. No other information is available elsewhere.

Acknowledgment

This study was support, edited and formatted by a team of researchers from Inventive Creativity Foundation. https://inventivecreativity.org/

Author Contribution

Conceptualization, Mahmoud Nasr & Pascal Muam Mah.; methodology, Mahmoud Nasr & Pascal Muam Mah,; validation, Mahmoud Nasr & Pascal Muam Mah., formal analysis, Mahmoud Nasr & Pascal Muam Mah.; investigation, Mahmoud Nasr & Pascal Muam Mah.; resources, Mahmoud Nasr & Pascal Muam Mah.; data curation, Mahmoud Nasr & Pascal Muam Mah; writing-original Mahmoud Nasr & Pascal Muam Mah,; preparation, Mahmoud Nasr & Pascal Muam Mah.; writing-review and editing, Mahmoud Nasr & Pascal Muam Mah.; visualization, Mahmoud Nasr & Pascal Muam Mah.; supervision, X.X.; project administration, Pascal Muam Mah and Pascal Muam Mah.; funding acquisition, Pascal Muam Mah. All authors have read and agreed to the published version of the manuscript."

References

[1] Basma Abd El-Rahiem, Fathi E Abd El Samie, and Mohamed Amin. Efficient cancellable multi-biometric recognition system based on deep learning and bio-hashing. *Applied Intelligence*, 53(2):1792–1806, 2023.

[2] Essam Abdellatef, Nabil A Ismail, Salah Eldin SE Abd Elrahman, Khalid N Ismail, Mohamed Rihan, and Fathi E Abd El-Samie. Cancelable multi-biometric recognition system based on deep learning. *The Visual Computer*, 36:1097–1109, 2020.

[3] Aysajan Abidin, Abdelrahaman Aly, Enrique Argones Rúa, and Aikaterini Mitrokotsa. Efficient verifiable computation of xor for biometric authentication. In *Cryptology and Network Security: 15th International Conference, CANS 2016, Milan, Italy, November 14-16, 2016, Proceedings 15*, pages 284–298. Springer, 2016.

[4] Christopher Andrade and Sebastian H von Solms. Investigating and comparing multimodal biometric techniques. In *Policies and Research in Identity Management: First IFIP WG11. 6 Working Conference on Policies and Research in Identity Management (IDMAN'07), RSM Erasmus University, Rotterdam, The Netherlands, October 11-12, 2007*, pages 79–90. Springer, 2008.

[5] Robert J Baron. Mechanisms of human facial recognition. *International Journal of Man-Machine Studies*, 15(2):137–178, 1981.

[6] Jiazhen Cai, Xuan Chu, Kun Xu, Hongbo Li, and Jing Wei. Machine learning-driven new material discovery. *Nanoscale Advances*, 2(8):3115–3130, 2020.

[7] ZX Chu, Q Ma, YX Lin, XL Tang, YQ Zhou, SW Zhu, J Fan, and BJ Cheng. Genome-wide identification, classification, and analysis of two-component signal system genes in maize. *Genet Mol Res*, 10(4):3316–3330, 2011.

[8] Richard Clodfelter. Biometric technology in retailing: Will consumers accept fingerprint authentication? *Journal of Retailing and Consumer Services*, 17(3):181–188, 2010.

[9] Basma Abd El-Rahiem, Mohamed Amin, Ahmed Sedik, Fathi E Abd El Samie, and Abdullah M Iliyasu. An efficient multi-biometric cancellable biometric scheme based on deep fusion and deep dream. *Journal of Ambient Intelligence and Humanized Computing*, pages 1–13, 2022.

[10] Samer Eldesouky, Walid El-Shafai, Hossam El din H Ahmed, and Fathi E Abd El-Samie. Cancelable electrocardiogram biometric system based on chaotic encryption using three-dimensional logistic map for biometric-based cloud services. *Security and Privacy*, 5(2):e198, 2022.

[11] Yann Frauel, Albertina Castro, Thomas J Naughton, and Bahram Javidi. Resistance of the double random phase encryption against various attacks. *Optics Express*, 15(16):10253–10265, 2007.

[12] Pramod D Ganjewar, Sanjeev J Wagh, and Aarti L Gilbile. Privacy threat reduction using modified multi-line code generation algorithm (mmlcga) for cancelable biometric technique (cbt). In *International Conference on Intelligent Cyber Physical Systems and Internet of Things*, pages 275–289. Springer, 2022.

[13] D Harikrishnan, N Sunil Kumar, Shelbi Joseph, and Kishor Krishnan Nair. Towards a fast and secure fingerprint authentication system based on a novel encoding scheme. *International Journal of Electrical Engineering & Education*, 61(1):100–112, 2024.

[14] Sin-Ye Jhong, Po-Yen Tseng, Natnuntnita Siriphockpirom, Chih-Hsien Hsia, Ming-Shih Huang, Kai-Lung Hua, and Yung-Yao Chen. An automated biometric identification system using cnn-based palm vein recognition. In *2020 international conference on advanced robotics and intelligent systems (ARIS)*, pages 1–6. IEEE, 2020.

[15] Harkeerat Kaur and Pritee Khanna. Biometric template protection using cancelable biometrics and visual cryptography techniques. *Multimedia Tools and Applications*, 75:16333–16361, 2016.

[16] Jihyeon Kim, Yoon Gyo Jung, and Andrew Beng Jin Teoh. Multimodal biometric template protection based on a cancelable softmaxout fusion network. *Applied Sciences*, 12(4):2023, 2022.

[17] Won Kim. Cloud computing: Today and tomorrow. *J. Object Technol.*, 8(1):65–72, 2009.

[18] Ayoub Lahmidi, Chouaib Moujahdi, Khalid Minaoui, and Mohammed Rziza. On the methodology of fingerprint template protection schemes conception: meditations on the reliability. *EURASIP Journal on Information Security*, 2022(1):3, 2022.

[19] Mohammad Saeid Mahdavinejad, Mohammadreza Rezvan, Mohammadamin Barekatain, Peyman Adibi, Payam Barnaghi, and Amit P Sheth. Machine learning for internet of things data analysis: A survey. *Digital Communications and Networks*, 4(3):161–175, 2018.

[20] Davide Maltoni, Dario Maio, Anil K Jain, Salil Prabhakar, et al. *Handbook of fingerprint recognition*, volume 2. Springer, 2009.

[21] Kennedy Okokpujie, Etinosa Noma-Osaghae, Samuel John, and Rhema Oputa. Development of a facial recognition system with email identification message relay mechanism. In *2017 international conference on computing networking and informatics (ICCNI)*, pages 1–6. IEEE, 2017.

[22] Xiang Peng, Peng Zhang, Hengzheng Wei, and Bin Yu. Known-plaintext attack on optical encryption based on double random phase keys. *optics letters*, 31(8):1044–1046, 2006.

[23] Pablo Piccolotto and Patricio Maller. Biometrics from the user point of view: Deriving design principles from user perceptions and concerns about biometric systems. *Intel Technology Journal*, 18(4), 2014.

[24] NS Raghava et al. Iris recognition on hadoop: A biometrics system implementation on cloud computing. In *2011 IEEE International Conference on Cloud Computing and Intelligence Systems*, pages 482–485. IEEE, 2011.

[25] Javier Ramirez De La Pinta, José María Maestre Torreblanca, Isabel Jurado, and Sergio Reyes De Cozar. Off the shelf cloud robotics for the smart home: Empowering a wireless robot through cloud computing. *Sensors*, 17(3):525, 2017.

[26] Nalini K Ratha, Sharat Chikkerur, Jonathan H Connell, and Ruud M Bolle. Generating cancelable fingerprint templates. *IEEE Transactions on pattern analysis and machine intelligence*, 29(4):561–572, 2007.

[27] Christian Rathgeb and Andreas Uhl. A survey on biometric cryptosystems and cancelable biometrics. *EURASIP journal on information security*, 2011:1–25, 2011.

[28] Philippe Refregier and Bahram Javidi. Optical image encryption based on input plane and fourier plane random encoding. *Optics letters*, 20(7):767–769, 1995.

[29] Mulagala Sandhya, Mahesh Kumar Morampudi, Indragante Pruthweraaj, and Pranay Sai Garepally. Multi-instance cancelable iris authentication system using triplet loss for deep learning models. *The Visual Computer*, 39(4):1571–1581, 2023.

[30] Avantika Singh, Gaurav Jaswal, and Aditya Nigam. Cancelable biometrics for template protection: future directives with deep learning. In *AI and Deep Learning in Biometric Security*, pages 23–49. CRC Press, 2021.

[31] Avantika Singh, Chirag Vashist, Pratyush Gaurav, and Aditya Nigam. A generic framework for deep incremental cancelable template generation. *Neurocomputing*, 467:83–98, 2022.

[32] Krishnaraj Madhavjee Sunjiv Soyjaudah, Gianeswar Ramsawock, and Muhammad Yaasir Khodabacchus. Cloud computing authentication using cancellable biometrics. In *2013 Africon*, pages 1–4. IEEE, 2013.

[33] Tanuja Sudhakar and Marina Gavrilova. Cancelable biometrics using deep learning as a cloud service. *IEEE Access*, 8:112932–112943, 2020.

[34] Veeru Talreja, Matthew C Valenti, and Nasser M Nasrabadi. Multibiometric secure system based on deep learning. In *2017 IEEE Global conference on signal and information processing (globalSIP)*, pages 298–302. IEEE, 2017.

[35] Min Wang, Song Wang, and Jiankun Hu. Cancellable template design for privacy-preserving eeg biometric authentication systems. *IEEE Transactions on Information Forensics and Security*, 17:3350–3364, 2022.

[36] Sarah Webb et al. Deep learning for biology. *Nature*, 554(7693):555–557, 2018.

[37] Kaijun Yi, Qianzhong Deng, Baoguo Yuan, Xiuxia Qu, Junxiong Gao, and Tomas Fernandes. Iris recognition and data storage on cloud. In *2018 Asia-Pacific Magnetic Recording Conference (APMRC)*, pages 1–3. IEEE, 2018.

[38] Hua-Hong Zhu, Qian-Hua He, Hong Tang, and Wei-Hua Cao. Voiceprint-biometric template design and authentication based on cloud computing security. In *2011 International Conference on Cloud and Service Computing*, pages 302–308. IEEE, 2011.