LAUTECH Journal of Engineering and Technology 19 (1) 2025: 128-141

10.36108/laujet/5202.91.0121

Comparative Analysis of Score Level Fusion Techniques in Multi-Biometric System

[1] Akintunde O. A., [2]Adetunji A. B., [3]Fenwa O. D., [4*]Oguntoye J. P., [5]Olayiwola D. S., and [6]Adeleke A. J.

[1,2] Department of Computer Sciences, Ladoke Akintola University of Technology Ogbomoso, Nigeria.
[3]Department of Cyber Security, Ladoke Akintola University of Technology Ogbomoso, Nigeria.
[4,5,6] Department of Computer Engineering, Ladoke Akintola University of Technology Ogbomoso, Nigeria.

[1] olayemiakintunde1@gmail.com ,[2] abadetunji@lautech.edu.ng , [3]odfenwa@lautech.edu.ng
[4]jpoguntoye@lautech.edu.ng, [5]olayiwola_dare@yahoo.com, [6]ayomidejoshua72@gmail.com

Article Info

Article history:

Received: Jan. 08, 2025
Revised: Feb. 11, 2025
Accepted: Feb. 12, 2025

Keywords:

Face Recognition,
Fingerprint Recognition,
Multimodal biometrics,
Principal Component Analysis,
Score Level Fusion,
Security and Access Control

Corresponding Author:
jpoguntoye@lautech.edu.ng ; +2348035282237

ABSTRACT

Multimodal biometric systems have garnered significant interest from researchers owing to their applicability in security and access control. Despite the development of numerous score-level fusion techniques for multimodal biometrics, most of them have concentrated solely on enhancing fusion accuracy, neglecting the potential advantages of various score-level techniques. This research investigates the comparative performance of four different score-level fusion approaches for multimodal recognition of combined face and fingerprint biometrics: Product rule, Weighted Sum rule, Simple Sum rule, and Max rule methods. Five hundred and seventy (570) sample images from 190 students of Ladoke Akintola University of Technology (LAUTECH), Ogbomoso, used in this study were acquired using a CMITech camera for faces and digital personnel for fingerprints, respectively. The images consist of three (3) samples of each biometric trait. Three hundred and forty-two (342) images of these traits were used for training while two hundred and twenty-eight (228) images were used for testing. The acquired images were pre-processed using histogram equalization, features extraction was done using Principal Component Analysis. Euclidian distance and Manhattan distance were used for generating the matching score of face and fingerprint feature, respectively while Min-max was used to normalize each score. The fused score of each technique was used for identification. The results obtained was evaluated using False Acceptance Rate (FAR), False Rejection Rate (FRR), Recognition Accuracy (RA) and Recognition Time (RT). Experimental results revealed that the Weighted Sum Rule outperformed other techniques, achieving a FAR of 1.75%, FRR of 5.85%, RA of 95.18%, and RT of 56.12 seconds. Comparatively, the Product Rule, Simple Sum Rule, and Max Rule demonstrated lower performance metrics. This study underscores the efficacy of the Weighted Sum Rule as a superior score-level fusion technique for developing advanced multimodal biometric systems, particularly in applications requiring high security and reliability.

INTRODUCTION

Biometric systems have become increasingly important in the technologically advanced world, addressing security concerns such as ATM PIN theft. These systems use unique physical or behavioural characteristics of an individual for authentication (Aarohi *et.al.*, 2015; Adedeji *et al.*, 2021). However, uni-biometric systems, which rely on a single biometric trait, often fall short in representing subjects and preventing spoofs. To overcome these limitations, multi-biometric systems have been developed (Liang *et al.*, 2016;

Adedeji *et al.,* 2021). These systems integrate multiple biometric modalities, such as face, fingerprint, and iris recognition, to enhance security and accuracy. Multi-biometric systems offer several advantages, including improved subject representation and discrimination, enhanced spoof prevention, increased accuracy and reliability, and the ability to address issues like intra-class variability, interclass similarity, and sensitivity to noise (Mondal and Kaur, 2016; Haider *et al.*, 2020).

Information fusion in multi-biometric systems can occur at four stages: sensor, feature, score, and decision. The score fusion stage is generally preferred by researchers as it provides an appropriate trade-off between ease of implementation and information preservation (Kolivand *et al.*, 2023; Okediran and Oguntoye, 2023). Various techniques have been employed for score-level fusion, broadly categorized into rule-based fusion (e.g., sum rule, product rule, weighted sum rule) and classification-based fusion (e.g., Support Vector Machine, Bayesian classifier, neural networks) (Ross and Jain, 2003; Aarohi, *et. al.*, 2015; Ola *et al.,* 2020). By effectively combining the discriminative power of multiple biometric traits, multi-biometric systems based on score fusion can overcome the limitations of individual traits and lead to better overall performance in biometric authentication (Liang *et al.*, 2016; Yang *et al.*, 2023).

A significant amount of score-level fusion techniques have been proposed in recent studies. Most of these studies achieved a very promising performance but focused majorly on increasing the fusion accuracy (Ross and Jain, 2003, Aguilar *et al.*, 2003). Also, the reported performances from different attempts are not directly comparable, because the databases used for evaluations are different in size and quality, and these have a direct impact on performance. Therefore, it is difficult for one to choose the best fusion method (Bolle, *et al.*, 2008, Xue and Titterington, 2008). This research intends to combine face and fingerprint biometrics at the score fusion level and carry out a comparative analysis on four fusion techniques (i.e. Product rule, Weighted Sum Rule, Simple Sum rule and Max rule) concerning both fusion accuracy and computational requirement (processing time) using the same database. The comparison of these fusion techniques will provide comprehensive guidance for selecting an appropriate strategy for a particular application. This study seeks to provide empirical evidence to identify the most effective score fusion technique, evaluating its performance against alternative methods.

LITERATURE REVIEW

Biometrics is the science of establishing the identity of a person based on 'Who you are,' which refers to physiological characteristics such as fingerprints, iris, or face, and 'What you produce,' which refers to behavioural patterns like voice or signature (Adetunji *et al.,* 2015). These characteristics, known as biometric modalities, have been extensively used in security systems for automatic recognition (Poh and Bengio, 2006). Similarly, Omidiora *et al.* (2008) described biometric techniques as identifying people by "who they are" and not by "what they have" or "what they know."

The choice of a biometric trait for any application depends on several factors beyond matching performance and accuracy (Adetunji *et al.,* 2018). According to Jain *et al.* (2004), biometric traits should satisfy universality, distinctiveness, permanence, and collectability requirements. Additionally, practical applications should consider performance, acceptability, and circumvention to ensure biometric systems are efficient and secure (Abolade *et al,* 2022; Atanda *et al.,* 2023; Sijuade *et al.,* 2024). Unimodal biometric systems, which rely

on a single biometric trait, are the simplest method for biometric recognition. However, they face several limitations, including noisy data, intra-class variations, non-universality, and vulnerability to spoof attacks (Ross and Jain, 2003; Olayiwola *et al.*, 2023). As a result, researchers have advocated for multimodal biometric systems, which combine multiple biometric traits to improve recognition accuracy, security, and robustness (Jain *et al.*, 2006; Sanjekar and Patil, 2013).

Multimodal biometric systems fuse data from different sources at various levels, including feature extraction, matching scores, and decision levels (Jain *et al.*, 2005). However, score-level fusion has been identified as the most appropriate and effective method for multimodal systems, as it balances the richness of information with ease of implementation (Indovina *et al.*, 2003). The scores from different modalities must first be normalized using techniques such as Min-Max or Z-Score normalization to bring them into a common domain (Jain *et al.*, 2005; Snelick *et al.*, 2005).

Several score-level fusion techniques, such as Sum Rule, Product Rule, Min Rule, and Max Rule, have been explored to combine the matching scores effectively. The Sum Rule computes a fused score by adding the scores from all modalities, while the Product Rule multiplies the scores. These methods are simple and computationally efficient but vary in performance depending on the biometric traits involved (Snelick *et al.*, 2003; Shakhnarovich and Darrell, 2002). Other approaches include the Weighted Sum Rule, which assigns weights to different traits based on their importance, and machine learning techniques like Support Vector Machines (SVMs) and Multi-Layer Perceptrons (MLPs) for more sophisticated score fusion (Jain and Ross, 2002; Czyz *et al.*, 2003). Empirical studies (Ribaric *et al.*, 2003; Peng *et al.*, 2020) have shown that multimodal systems using score-level fusion significantly improve recognition performance compared to unimodal systems. For instance, Rani and Shanmugalakshmi (2015) demonstrated that a multimodal system combining palmprint and finger knuckle print with score-level fusion yielded higher accuracy and lower error rates than unimodal systems. Similarly, Silva *et al.* (2018) reported state-of-the-art results using Particle Swarm Optimization for feature fusion in the iris and periocular recognition tasks. Other applicable optimization techniques are discussed in Ola *et al.* (2017) and Ola *et al.* (2019).

Given the effectiveness of score-level fusion, this research aims to conduct a comparative analysis of four selected fusion techniques. Product Rule, Weighted Sum Rule, Simple Sum Rule, and Max Rule for both fusion accuracy and recognition time.

METHODOLOGY

This study involves the comparative analysis of score-level fusion techniques in face and fingerprint-based multi-biometric systems. The stages involved include face and fingerprint datasets acquisition, preprocessing, feature extraction using Principal Component Analysis (PCA), generating matching scores using Euclidian distance and Manhattan distance, normalization of scores using Min-max, fusing normalized scores using various techniques, and identifying subjects as genuine users or impostors using the fused score. The fused score was used for identification. Figure 1 illustrates the Scheme of this study.

Multi-Biometric Data Acquisition

This phase involves the acquisition of facial and fingerprint datasets. Facial data were collected from LAUTECH students using a CMITech camera, while fingerprint data were obtained using a Digital Persona scanner. The face and the fingerprint of each subject were stored correspondingly. Three face and fingerprint samples were collected from

190 students, resulting in 570 images per trait. Of these, 342 were used for training and 228 for testing per trait.

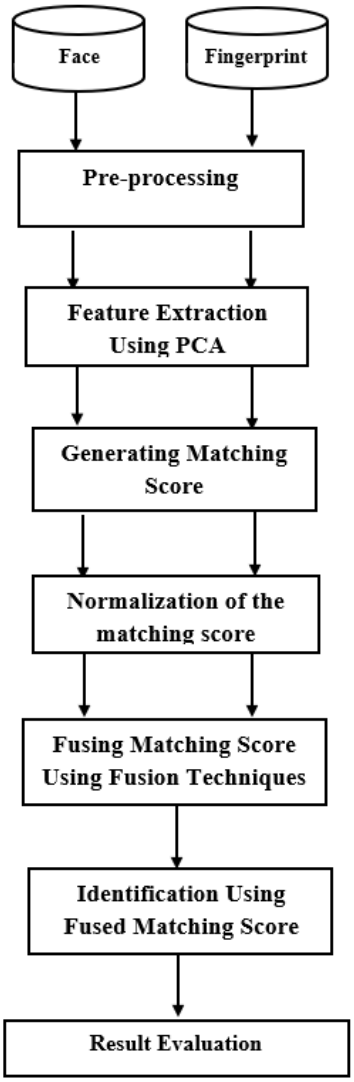

Figure 1: The Scheme of the Study

Pre-processing phase

Pre-processing involves actions such as image brightness, contrast adjustment, image scaling, filtering, cropping, and other operations that enhance images, carried out for both fingerprint and face datasets before feature extraction. For the fingerprint dataset, pre-processing included enhancement to suppress noise and enhance ridge-valley structures, detection of the region of interest to discard background data, binarizing to convert images to black and white, thinning to reduce ridge thickness to one pixel wide, and normalization using histogram equalization to standardize grayscale variations and enhance contrast. The face dataset underwent conversion of coloured images from three-dimensional form to grayscale and normalization, where the grayscale images were expressed as matrices in MATLAB and converted to vector images for processing, with histogram equalization applied to improve contrast and brightness for clearer facial features.

Feature Extraction

The features of the pre-processed face datasets and fingerprint datasets were extracted using Principal Component Analysis (PCA). A significant set of key parameters that best describe the face and fingerprint features were extracted using PCA, which retrieved relevant features by removing redundant and irrelevant features without losing useful information from the face and fingerprint dataset. For the fingerprint dataset, this stage is otherwise known as Minutiae Extraction, where the endings and bifurcations of the fingerprint images are known as the minutiae. Minutiae detection was conducted to accurately extract distinctive minutiae features, while the Principal Component Analysis (PCA) technique was employed for feature extraction. PCA utilized statistical methods to determine the optimal projection bases, effectively distinguishing between genuine minutiae regions and false minutiae regions. Similarly, for the face dataset, relevant information was extracted from the face such as the eyebrows, the eyelids, the nose, the cheeks, and the lips, with PCA employed to extract features and reduce the dimension sizes of images to form Eigenfaces. The PCA method uses the statistical distribution of input samples to find the best projection bases, and its advantages include the orthogonality of principal eigenvectors that represent the directions of maximum variation, speeding up the convergence of model training and

improving system performance. The Principal Component Analysis (PCA) technique was applied following Adetunji et al. (2018).

Matching Phase

In this study, the matching module compared the extracted feature set with stored templates using a classifier or matching algorithm to generate matching scores. In the decision module, these matching scores were utilized to either identify an enrolled user or verify a user's identity. The face and fingerprint features extracted using Principal Component Analysis (PCA) were input into the matching module, where their respective matching scores were computed and subsequently fused using the fusion techniques considered in the study.

The matching score for the face feature was computed using Euclidean distance, while Manhattan distance was applied to the fingerprint feature. The matches aligned the extracted features with their corresponding templates in the database and generated matching scores. For face recognition, the matching process between the test face feature template and the stored templates in the system database was performed using the Euclidean distance, mathematically expressed as:

$$S_{face}(x,y) = \sqrt{\sum_{i=1}^{n}(y_i - x_i)^2} \quad (1)$$

For fingerprint recognition, the matching process between the test fingerprint feature template and the stored templates was executed using the Manhattan distance, defined as:

$$S_{fprint}(x,y) = \sum_{i=1}^{n}|x_i - y_i| \quad (2)$$

Following the matching phase, various threshold points were determined, and based on the score values, multiple performance evaluation metrics were computed to assess the effectiveness of the biometric system.

Score Normalization

The normalization of the face and fingerprint matching score represented as S_{face} and S_{fprint} was achieved using Min-max. This rule retained the distribution, was sensitive to outliers, and mapped the scores into a common range. Normalization was essential to ensure consistency among the match scores generated by different matches, as they might not be homogeneous. The scores were scaled to the interval [0,1] while preserving the original distribution of matching scores, thereby maintaining the relative ranking of matches. The normalization is given by:

$$S'_{face} = \frac{S_{face} - \min(S_{face})}{\max(S_{face}) - \min(S_{face})} \quad (3)$$

$$S'_{fprint} = \frac{S_{fprint} - \min(S_{fprint})}{\max(S_{fprint}) - \min(S_{fprint})} \quad (4)$$

where S_{face} and S_{fprint} are the matching scores obtained from face and fingerprint modalities, respectively. $\min(S_{face})$ and $\max(S_{face})$ are the minimum and maximum scores for face traits and $\min(S_{fprint})$ and $\max(S_{fprint})$ are the corresponding values obtained from the fingerprint trait.

Score Level Fusion Techniques

The study investigated the performance of the following score-level fusion techniques:

Simple Sum Rule

The sum rule combines the normalized face (S'_{face}) and fingerprint (S'_{fprint}) scores corresponding to a particular individual by applying the sum rule on the scores for fusion. The sum rule is very simple and computationally efficient. It gives both face and fingerprint biometric traits to be fused equal importance. The mathematical representation for the sum rule that was used is given in Equation 5.

$$S_{fus} = F(S'_{face}, S'_{fprint}) = S'_{face} + S'_{fprint} \quad (5)$$

Where S_{fus} is the fused score, S'_{face} and S'_{fprint} are the normalised scores of face and fingerprint models respectively.

Product Rule

The product rule combines the normalized face (S'_{face}) and fingerprint (S'_{fprint}) scores corresponding to a particular individual by applying the product rule on the scores for fusion. The product rule is very simple and computationally efficient. The mathematical representation for the product rule is given in equation 6.

$$S_{fus} = F(S'_{face}, S'_{fprint}) = S'_{face} * S'_{fprint} \quad (6)$$

Where, S_{fus} is the fused score,S'_{face} and S'_{fprint} are the normalised scores of face and fingerprint models, respectively.

Weighted Sum Rule

Weighted Sum Rule computes the combined score as a weighted sum of both normalized faces (S'_{face}) and fingerprint (S'_{fprint}) scores. The weighted sum rule was employed to evaluate the best performance under linear combination. Firstly, each normalized score was multiplied by the corresponding weight of its modality. Secondly, the multiplication results were added together to produce the fused score. The weights per trait were computed based on the accuracy of each score. If a_1 was the accuracy of the face score and $a_2$was the accuracy of the fingerprint score, then the weights were calculated as:

$$W_{face} = \frac{a_1}{a_1 + a_2} \quad (7)$$

$$W_{fprint} = \frac{a_2}{a_1 + a_2} \quad (8)$$

with the constraint $W_{face} + W_{fprint} = 1$, and the fusion score is computed in equation 9.

$$S_{fus} = W_{face} * S'_{face} + W_{fprint} * S'_{fprint} \quad (9)$$

Where W_{face} and W_{fprint} are weights of face and fingerprint traits, respectively.

Max Rule:

The max rule combines both normalized faces (S'_{face}) and fingerprint (S'_{fprint}) scores corresponding to a particular individual by selecting maximum of the scores that come for fusion. Max rule is very simple and computationally efficient. This rule also forces the score of only one biometric to be used for fusion. Mathematical representation for the max rule is given in equation 10.

$$S_{fus} = \max(S'_{face}, S'_{fprint}) \quad (10)$$

Where, S_{fus} is the fused score,S'_{face} and S'_{fprint} are the normalised scores of face and fingerprint models respectively. The procedure is depicted in Algorithm 1.

Decision Module

The fused matching score from each of the fusion techniques was used to identify a user as either genuine or impostor. The fused score S_{fus} was compared to a pre-specified threshold (th). If $S_{fus} > th$, then the user is identified to be genuine otherwise an impostor. The decision function defined in Equation (11) verifies the identity.

$$Decision(S_{fus}) = \begin{cases} Accept\ (Genuine), & if\ \ S_{fus} > th \\ Reject(Impostor), & otherwise \end{cases} \quad (11)$$

Implementation for training and testing

There were two phases in the implementation of the score fusion techniques in this study. These included the learning (training) phase and the testing phase. The performance of each technique was evaluated using the aforementioned performance metrics and compared. In the learning (training) phase, the training dataset underwent a pre-processing stage after which PCA was used for dimension reduction and extraction of face and finger features.

Algorithm 1: Fusion of Face and Fingerprint Traits at Score Level.

for each fusion per User do
for each User **do**
if face **then**
$S_{face} \leftarrow Euclidian\ Distance$**{Face Score Generation}**
Else
$S_{fprint} \leftarrow Manhattan\ distance$**{Fingerprint Score Generation}**
end if
end for
for each score **do**
if S_{face} **then**
$S'_{face} \leftarrow Normalization\ (S_{face})$
Else
$S'_{fprint} \leftarrow Normalization\ (S_{fprint})$
end if
end for
$S_{fus} \leftarrow F(S'_{face}, S'_{fprint})$ **{fuse score based on selected techniques}**
If $S_{fus} > threshold$ **then**
Identify the user as Genuine
Else
Identify the user as Impostor
end if
end for

The trained dataset was stored in the face and fingerprint gallery. During the testing phase, the input dataset underwent the pre-processing stage after which PCA was used for dimension reduction and extraction of face and fingerprint features. Euclidian distance and Manhattan distance were used to perform similarity measurements for face and fingerprint features in the gallery, respectively. The matching score for the face and fingerprint trait was normalized using the min-max rule.

The normalized matching scores were fused using any of the fusion techniques (i.e. Product rule, Weighted Sum Rule, Simple Sum rule and Max rule). Figure 2 depicts the stepwise procedure of the training and testing phases. Moreover, Figure 3 depicts the developed Graphical User Interface (GUI). The interactive GUI application was developed with a real-time database consisting of both face and fingerprint datasets. MATLAB R2018a was used for implementation on a computer system with high specifications.

Performance Evaluation

The performance of the investigated score-level fusion techniques in a multi-biometric system was evaluated by calculating the False Acceptance Rate (FAR), Equal Error Rate (EER), False Rejection Rate (FRR), and Genuine Acceptance Rate (GAR)

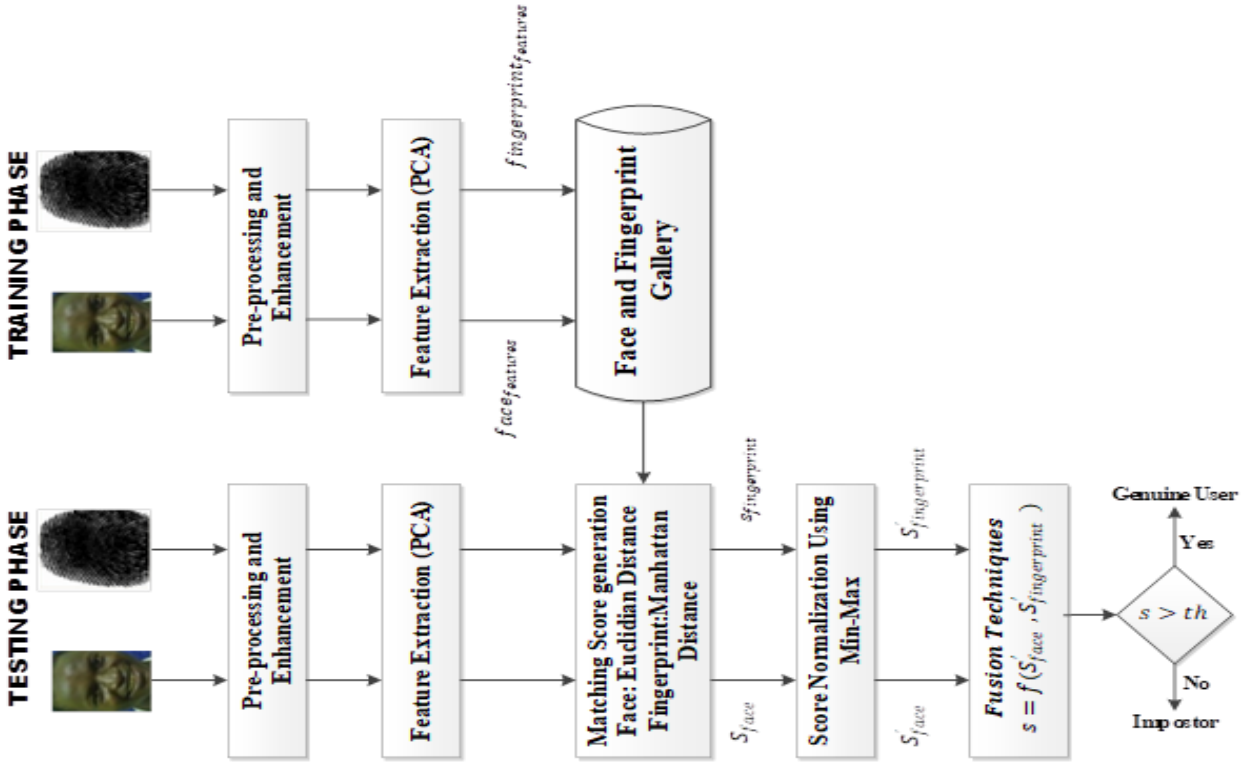

Figure 2: The process flow for the training and testing phase

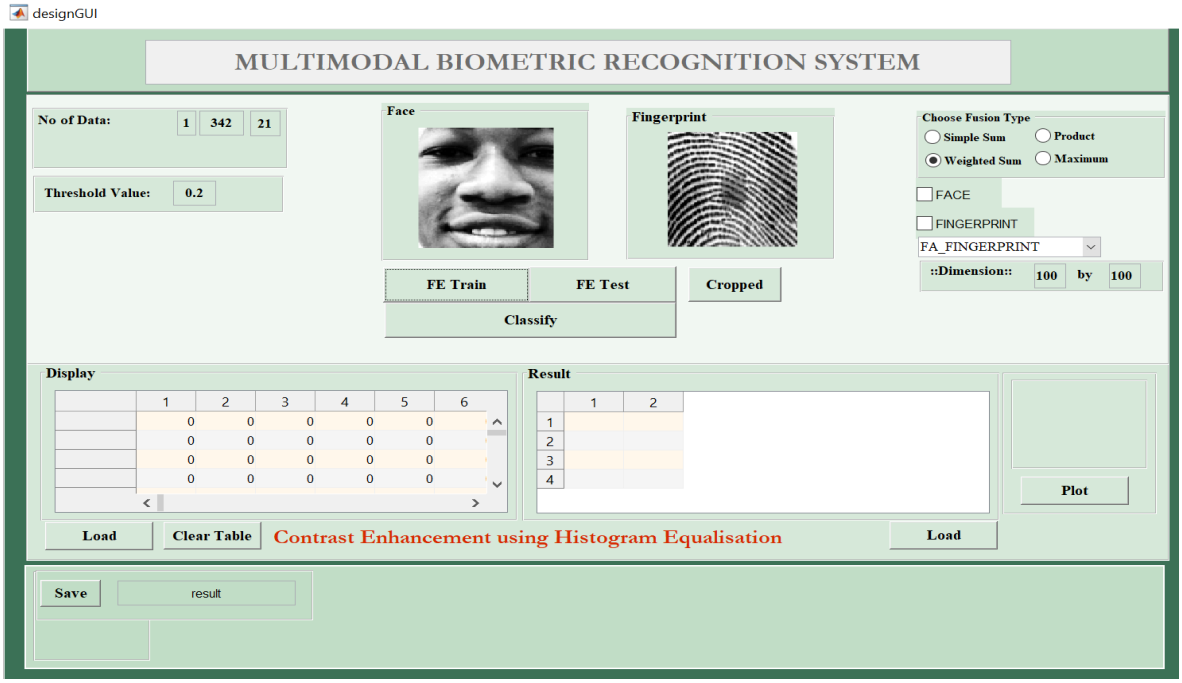

Figure 3: Graphical User Interface (GUI) showing training phase sample of Face and Fingerprint

at various thresholds. These metrics were computed by generating all possible genuine and impostor matching scores and then setting a threshold for deciding whether to accept or reject a match. EER was calculated at the operating point corresponding to the threshold (η) where FAR(η) = FRR(η). GAR represents the overall accuracy of the biometric system. In the verification phase, four decisions are

possible in response to a claimed identity: accept a client, accept an impostor, reject a client, or reject an impostor. The system may produce two types of errors: False Acceptance (FA), when an impostor is accepted, and False Rejection (FR), when a client is rejected. The performance of the system can be measured in terms of these two different errors as follows:

$$\text{FAR} = \frac{\text{Number of false acceptances}}{\text{Number of imposor accesses}} \times 100 \quad (10)$$

$$\text{FRR} = \frac{\text{Number of false rejections}}{\text{Number of client accesses}} \times 100 \quad (11)$$

$$\text{GAR} = \frac{\text{Number of Correct Acceptance}}{\text{Number of Identification Attempts}} \times 100 \quad (12)$$

$$\text{ERR} = \frac{\text{FAR}(\eta) + \text{FRR}(\eta)}{2} \times 100 \quad (13)$$

RESULT AND DISCUSSION

The Weighted Sum Rule (WSR), Simple Sum Rule (SR), Product Rule (PR) and Maximum Rule (MR) models were experimented with by implementing face and fingerprint recognition using 128 by 128-pixel resolution. The system was tested and evaluated using the following performance metrics: FAR, FRR, accuracy and computation time. All performance metrics were analysed using a square dimension pixel resolution stated earlier at 0.8 threshold value. Total face and Fingerprint collected = 3 samples per 190 individuals (3×190) = 570

TRAINING: 2 samples × 171 individuals

=342 (60% of total dataset)

TESTING: 1 sample × 171 individuals + 3 × 19

= 171 + 57 = 228 (40% of total dataset)

In biometric recognition, the 60:40 training-to-testing split ensures model generalization. Using 342 training samples improves feature learning, while 228 test samples validate performance, to ensure robust identity verification.

The dataset used contained 570 Fingerprint images and 570 face images, 342 of the Fingerprint images and 342 of the face images were used in training the model while 228 of the Fingerprint images and 228 of the face images were used to test the model. The training was carried out using WSR, SR, MR and PR with fused Fingerprint and face. **Table 1** depicts the performance of the score-level techniques. The performance was presented based on performance metrics using the confusion matrix (TP, FN, FP and TN). **Table 1** details the performance of four score-level fusion techniques; Weighted Sum Rule, Simple Sum Rule, Maximum Rule, and Product Rule; on access control classification tasks involving genuine users and impostors.

For the **Weighted Sum Rule**, the technique correctly classified 161 genuine users while 10 genuine samples were misclassified as impostors. Only 1 impostor was incorrectly accepted as genuine, while 56 were correctly classified as impostors. Also, for the **Simple Sum Rule**, 158 genuine users were correctly classified, with 13 genuine samples misclassified as impostors. Additionally, 2 impostors were incorrectly accepted as genuine, and 55 were correctly classified as impostors. Moreover, for the **Maximum Rule**, the technique successfully classified 154 genuine users but misclassified 17 genuine samples as impostors.

Five impostors were incorrectly accepted as genuine, while 52 were accurately classified as impostors.

Table 1: Performance of Score level techniques

Score-level fusion techniques	TP	FN	FP	TN	FAR (%)	FRR (%)	Accuracy (%)	Time (Seconds)
Weighted Sum Rule	161	10	1	56	1.75	5.85	95.18	56.12
Sum Rule	158	13	2	55	3.51	7.60	93.42	62.10
Maximum rule	154	17	5	52	8.77	9.94	90.35	67.35
Product rule	156	15	4	53	7.02	8.77	91.67	72.99

Similarly, for the **Product Rule**, 156 genuine users were correctly classified, with 15 genuine samples misclassified as impostors. Four (4) impostors were incorrectly accepted as genuine, while 53 were correctly classified as impostors. The results highlight the **Weighted Sum Rule** as the most effective fusion technique for access control classification, achieving the highest true positive rate (161) and the lowest false positive (1) and false negatives (10). This demonstrates its superior ability to accurately classify genuine users and impostors. The **Simple Sum Rule** also performs well but has slightly higher misclassification rates. The **Maximum Rule** and **Product Rule** exhibit lower accuracy, with higher false positives and negatives. These findings underscore the importance of selecting optimal fusion techniques to enhance system reliability, minimize security risks, and improve user experience in access control applications. The **Weighted Sum Rule** technique demonstrated the best performance among the evaluated score-level fusion techniques, achieving a low False Acceptance Rate (FAR) of 1.75% and a False Rejection Rate (FRR) of 5.85%, coupled with an overall accuracy of 95.18%. It also exhibited a relatively fast processing time of 56.12 seconds, indicating its efficiency and reliability for access control systems. In comparison, the **Sum Rule** showed moderate performance, with a FAR of 3.51%, an FRR of 7.60%, and an accuracy of 93.42%, taking 62.10 seconds for processing. The **Maximum Rule** exhibited a higher FAR (8.77%) and FRR (9.94%), resulting in a lower accuracy of 90.35%, with a processing time of 67.35 seconds. The **Product Rule** achieved a FAR of 7.02%, an FRR of 8.77%, and an accuracy of 91.67%, with the longest processing time of 72.99 seconds. These results imply that the Weighted Sum Rule is the most effective technique for accurate and efficient classification in access control systems. Its superior accuracy and minimal error rates enhance system reliability, while its fast-processing time ensures a seamless user experience. In contrast, techniques like the Maximum and Product Rules, with higher error rates and slower processing, may pose risks such as increased security vulnerabilities and user inconvenience.

Therefore, the Weighted Sum Rule emerges as the most preferable technique among the evaluated methods, offering superior accuracy, minimal error rates, and faster processing times. Its adoption can significantly enhance the overall reliability, security, and operational efficiency of access control systems compared to alternative techniques. Empirical studies corroborate the effectiveness of low FAR and FRR rates in enhancing system security and user experience. According to Jain *et al.* (2006), a low FAR is critical in preventing unauthorized access, while a low FRR ensures

minimal inconvenience to legitimate users. The Weighted Sum Rule's low FAR and FRR signify its robustness in accurately classifying access requests, aligning with previous findings that highlight the importance of fusion techniques in biometric systems (Ross *et al.,* 2003). The Simple Sum Rule, though moderately effective, and the Maximum and Product Rules, with higher error rates, reinforce the need for optimized techniques to minimize security risks and improve system reliability (Oguntoye *et al.,* 2023). The FAR and FRR metrics are critical in evaluating the trade-off between security and usability in biometric systems. A high FAR poses significant security risks, such as unauthorized access, while a high FRR leads to user frustration and inefficiency (Jain *et al.,* 2004). The Weighted Sum Rule's optimal balance between these metrics demonstrates its suitability for achieving both security and user satisfaction, aligning with established best practices in biometric security design according to ISO/IEC 19792 standard (McAteer *et al.,* 2019). From a theoretical standpoint, the study supports the efficacy of score-level fusion methods, particularly the Weighted Sum Rule, as proposed in multi-biometric systems (Ross and Jain, 2004). The findings validate the integration of multiple biometric scores to enhance decision-making accuracy, offering a basis for further exploration of advanced fusion algorithms, such as machine learning-based adaptive fusion (Tiwari *et al.,* 2024). Practically, the Weighted Sum Rule's low FAR and FRR enhance system reliability, making it suitable for applications requiring high-security standards, such as financial transactions, healthcare access (Ogundepo *et al.,* 2022), and border control (Uludag *et al.,* 2004). Its faster processing time ensures scalability for real-time applications, addressing practical challenges like user impatience and operational delays in access control systems (Sumalatha *et al.,* 2024).

Therefore, this study addressed the challenge of determining the most effective score-level fusion technique for biometric access control by comparing the Weighted Sum Rule, Simple Sum Rule, Maximum Rule, and Product Rule using a consistent database. The results provide a definitive benchmark for selecting score-level fusion techniques, overcoming the limitations of prior studies where inconsistent evaluation methods hindered direct comparisons. This research provides a unified evaluation of performance and computational efficiency, confirming the Weighted Sum Rule as the most effective fusion technique. It also offers practical guidelines for implementing fusion methods in biometric systems, ensuring they are tailored to specific application requirements.

CONCLUSION AND RECOMMENDATIONS

This study conducted a comprehensive comparative analysis of four score-level fusion techniques for biometric access control using the same database. The findings highlight the Weighted Sum Rule as the most effective method, combining superior accuracy, minimal error rates, and computational efficiency. This research advances the understanding of fusion techniques by providing standardized performance metrics and addressing the gaps identified in previous studies. The results reinforce the importance of selecting fusion techniques that balance security, accuracy, and operational feasibility, ensuring reliable performance in real-world applications.

Organizations implementing biometric systems should prioritize the Weighted Sum Rule due to its superior accuracy and efficiency. For environments requiring moderate accuracy, alternative methods like the Simple Sum Rule can be customized based on specific security and processing needs. Future research should explore hybrid approaches, integrating machine learning with fusion

techniques, to enhance adaptability across diverse datasets. Additionally, scalability testing on larger datasets is essential to validate the generalizability of findings. Establishing industry standards for unified evaluation frameworks will ensure the comparability of biometric fusion techniques in research and practice.

REFERENCES

Aarohi V., Chirag P. and Mita P. (2015). Review on Fusion Algorithms for Multimodal Authentication System. International Journal of Engineering Development and Research. 3(2):911-917.

Abolade, J. O., Konditi, D. B., Mpele, P. M., Orimogunje, A. M., and Oguntoye, J. P. (2022). Miniaturized Dual-Band Antenna for GSM1800, WLAN, and Sub-6 GHz 5G Portable Mobile Devices. Journal of Electrical and Computer Engineering, 2022(1), 5455915.

Adedeji, O. T., Alade, O. M., Oguntoye J. P., Awodoye, O. O. (2021). Comparative Analysis of Feature Selection Techniques for Fingerprint Recognition Based on Artificial Bee Colony and Teaching Learning Based Optimization. LAUTECH Journal of Computing and Informatics. 2(1): pp 25-34.

Adedeji, O. T., Alo, O. O., Akerele, T. I., Oguntoye, J. P., Makinde, B. O., Jooda J.O. (2021). Comparative Analysis of Feature Level Fusion Bimodal Biometrics for Access Control. International Journal of Progressive Sciences and Technologies, 28(2): pp 484-492.

Adetunji A. B., Oguntoye J. P., Fenwa O. D. and Omidiora E. O. (2018): Reducing the Computational Cost of SVM in Face Recognition Application Using Hybrid Cultural Algorithm. IOSR Journal of Computer Engineering (IOSR-JCE). 20 (2): pp. 36-45.

Adetunji A. B., Oguntoye J. P., Fenwa O. D. and Omidiora E. O. (2015): Facial Expression Recognition Based on Cultural Particle Swamp Optimization and Support Vector Machine. LAUTECH Journal of Engineering and Technology. 10(1): pp. 94-102.

Aguilar J. F., Garcia J. O. and Rodriguez J. G. (2003). Fusion Strategies in Multimodal Biometric Verification. International Conference of Multimedia and Expo (ICME '03), 3: 5-8.

Atanda, O. G., Ismaila, W., Afolabi, A. O., Awodoye, O. A., Falohun, A. S., and Oguntoye, J. P. (2023). Statistical Analysis of a Deep Learning Based Trimodal Biometric System Using Paired Sampling T-Test. In 2023 International Conference on Science, Engineering and Business for Sustainable Development Goals (SEB-SDG) (Vol. 1, pp. 1-10).

Bolle R., Pankanti S. and Ratha N. (2008). Evaluation Techniques for Biometrics-based Authentication Systems (FRR). 15th International Conference on Pattern Recognition (ICPR '00). 2: 2831- 2837.

Czyz J., Bengio S., Marcel C. and Vandendorpe L. (2003). Scalability analysis of audio-visual person identity verification, Audio- and Video-based Biometric Person Authentication, 752–760.

Haider, S. A., Rehman, Y., and Ali, S. U. (2020). Enhanced multimodal biometric recognition based upon intrinsic hand biometrics. Electronics, 9(11), 1916.

Indovina M., Uludag U., Snelick R., Mink A. and Jain A.K. (2003). Multimodal Biometric Authentication Methods: A COTS Approach, Proceeding Multi-Modal User Authentication (MMUA), 99-106.

Jain A., Nandakumara K. and Ross A. (2005). Score normalization in multimodal biometric Systems. In Pattern Recognition, 38 (12): 2270-2285.

Jain, A. K., and Ross, A. (2002). Learning user-specific parameters in a multibiometric system. In Proceedings. International Conference on Image Processing . 1, pp. I-I). IEEE.

Jain, A. K., Ross, A., and Pankanti, S. (2006). Biometrics: a tool for information security. IEEE transactions on information forensics and security, 1(2), 125-143.

Jain, A. K., Ross, A., and Prabhakar, S. (2004). An introduction to biometric recognition. IEEE Transactions on circuits and systems for video technology, 14(1), 4-20.

Kolivand, H., Asadianfam, S., Akintoye, K. A., and Rahim, M. S. (2023). Finger vein recognition techniques: a comprehensive review. Multimedia Tools and Applications, 1-35.

Liang Y., Dinga X, Liua C. and Xue J. (2016). Combining multiple biometric traits with an order-preserving score fusion algorithm. Neurocomputing, 171:252-261.

McAteer, I., Ibrahim, A., Zheng, G., Yang, W., and Valli, C. (2019). Integration of biometrics and steganography: a comprehensive review. Technologies, 7(2), 34.

Mondal A. and Kaur A. (2016). Comparative Study of Feature Level and Decision Level Fusion in Multimodal Biometric Recognition of Face, Ear and Iris. International Journal of Computer Science and Mobile Computing, 5(5): 822-842.

Ogundepo O. Y., Omeiza I. O. A. and Oguntoye J. P. (2022). Optimized Textural Features for Mass Classification in Digital Mammography Using a Weighted Average Gravitational Search Algorithm. International Journal of Electrical and Computer Engineering (IJECE). 12 (5): pp 1-12.

Oguntoye, J. P., Awodoye, O. O., Oladunjoye, J. A., Faluyi, B. I., Ajagbe, S. A., and Omidiora, E. O. (2023). Predicting COVID-19 From Chest X-Ray Images using Optimized Convolution Neural Network. LAUTECH Journal of Engineering and Technology, 17(2), 28-39.

Okediran, O. O., and Oguntoye, J. P. (2023). Analysis of critical success factors for information security management performance. LAUTECH Journal of Engineering and Technology, 17(1), 175-186.

Ola B. O, Awodoye O. O. and Oguntoye J. P. (2019). A Comparative Study of Particle Swarm Optimization and Gravitational Search Algorithm in Poultry House Temperature Control System. World Journal of Engineering Research and Technology. 5(6): pp. 272-289.

Ola B. O, Oguntoye J. P. and Awodoye O. O. (2017). Performance Evaluation of Particle Swarm Optimization on Poultry House Temperature Control System. IOSR Journal of Computer Engineering (IOSR-JCE). 19(5): pp. 69–76.

Ola B. O, Oguntoye J. P., Awodoye O. O. and Oyewole M. O. (2020). Development of a Plant Disease Classification System using an Improved Counter Propagation Neural Network. International Journal of Computer Applications (0975 – 8887). 175(20): pp 19-26.

Olayiwola, D. S., Olayiwola, A. A., Oguntoye, J. P., Awodoye, O. O., Ganiyu, R. A., and Omidiora, E. O. (2023). Development of a Fingerprint Verification and Identification System Using a Gravitational Search Algorithm-Optimized Deep Convolutional Neural Network. Adeleke University Journal of Engineering and Technology, 6(2), 296-307.

Omidiora, E. O., Fakolujo, O. A., Ayeni, R. O. and Adeyanju, I. A. (2008). Optimised fisher discriminant analysis for recongnition of faces having black features. Journal of Engineering and Applied Sciences, 3 (7): 524-531.

Peng, J., Wu, J., and Chen, Y. (2020). A Score Level Fusion Method on Fingerprint and Finger Vein. In E3S Web of Conferences.185:1-6.

Poh, N., and Bengio, S. (2006). Database, protocols and tools for evaluating score-level fusion algorithms in biometric authentication. Pattern Recognition, 39(2), 223-233.

Rani E. P. and Shanmugalakshmi R. (2015). Score level fusion of multiple features for efficient personal recognition. ARPN Journal of Engineering and Applied Sciences 10(14): 5865- 5874.

Ribaric S., Ribaric D. and Pavesic N. (2003). A Multimodal Biometric User identification System for Network-based Applications, IEE Proceedings on Vision, Image and Signal Processing, 150: 409-416.

Ross A. and Jain A. (2003). Information fusion in biometrics. Pattern Recognition Letters, Elsevier, 24(13): 2115-2125.

Ross, A., and Jain, A. K. (2004). Multimodal biometrics: An overview. In 2004 12th European signal processing conference. pp. 1221-1224.

Sanjekar P. S. and Patil J. B. (2013). An overview of multimodal biometrics. Signal and image processing: An International journal (SIPIJ) 4(1): 1-8.

Shakhnarovich G. and Darrell T. (2002). On probabilistic combination of face and gait cues for identification. Proceedings of the 5th IEEE International Conference on Automatic Face and Gesture Recognition, 2002.

Sijuade, A., Ogunyote, J., Okediran, O., Omidiora, E., and Olabiyisi, S. (2024). Unified Theory of Acceptance and Use of Technology in Evaluating Voters' Intention Towards the Adoption of Electronic Forensic Election Audit System. FUOYE Journal of Engineering and Technology. 9 (1): 76-83.

Silva, P. H., Luz, E., Zanlorensi, L. A., Menotti, D., and Moreira, G. (2018). Multimodal feature level fusion based on particle swarm optimization with deep transfer learning. In 2018 IEEE Congress on Evolutionary Computation (CEC). 1-8.

Snelick R., Indovina M., Yen J., and Mink A. (2003). Multimodal Biometrics: Issues in Design and Testing. Proceedings of the Fifth International Conference on Multimodal Interfaces: 68-72.

Snelick R., Uludag U., Mink A., Indovina M. and Jain A.K. (2005). Large Scale Evaluation of Multimodal Biometric Authentication Using State-of-the-Art Systems, IEEE Transactions on Pattern Analysis and Machine Intelligence, 27: 450-455.

Sumalatha, U., Prakasha, K. K., Prabhu, S., and Nayak, V. C. (2024). A Comprehensive Review of Unimodal and Multimodal Fingerprint Biometric Authentication Systems: Fusion, Attacks, and Template Protection. IEEE Access.

Tiwari, S., Raja, R., Wadawadagi, R. S., Naithani, K., Raja, H., and Ingle, D. (2024). Emerging Biometric Modalities and Integration Challenges. In Online Identity-An Essential Guide. IntechOpen.

Uludag, U., Pankanti, S., Prabhakar, S., and Jain, A. K. (2004). Biometric cryptosystems: issues and challenges. Proceedings of the IEEE, 92(6), 948-960.

Xue J. and Titterington D (2008). Comments on @ On Discriminative vs. Generative Classifiers: A Comparison of Logistic Regression and Naive Bayes. Neural Processing Letters, 28(3):169-187.

Yang, W., Wang, S., Cui, H., Tang, Z., and Li, Y. (2023). A Review of Homomorphic Encryption for Privacy-Preserving Biometrics. Sensor, 23 (7), 3566.