LAUTECH Journal of Engineering and Technology 18 (3) 2024: 68-79

10.36108/laujet/4202.81.0380

Enhanced multimodal biometric access control system using chicken swarm optimization and self-organizing feature maps: a study on ear and iris recognition

[1]Jeremiah Y.S., [2*]Adedeji O. T. [1]Ajala F. A., and [3]Fenwa O. D.

[1]Computer Science Department, Faculty of Computing and Informatics, Ladoke Akintola University of Technology, Ogbomoso, Nigeria.
[2]Information Systems Department, Faculty of Computing and Informatics, Ladoke Akintola University of Technology, Ogbomoso, Nigeria.
[3]Cyber Security Science Department, Faculty of Computing and Informatics, Ladoke Akintola University of Technology, Ogbomoso, Nigeria.

Article Info

Article history:

Received: July 7, 2024
Revised: Sept 4, 2024
Accepted: Sept 12, 2024

Keywords:

Access Control, Multimodal Biometrics, Self-Organizing Feature Map, Chicken Swarm Optimization, Ear and Iris Recognition, Feature Level Fusion, Biometric Security, Machine Learning Algorithms.

Corresponding Author:
otadedeji@lautech.edu.ng

ABSTRACT

Access control systems are crucial for securing sensitive data and system components by allowing authorized access while blocking unauthorized entities. Traditional unimodal biometric systems, make use of a single physiological or behavioural trait, and have limitations such as susceptibility to spoofing and environmental constraints, leading to reduced reliability. This study explores an enhanced multimodal biometric access control system that combines ear and iris traits using an enhanced Self-Organizing Feature Map (SOFM) algorithm improved with Chicken Swarm Optimization (CSO). The system's performance is evaluated against traditional SOFM, with a focus on recognition accuracy and processing time. The data used to train the classifier for this study were collected from 190 individuals, encompassing a total of 2,280 images of iris, and ear traits. Preprocessing involved cropping, resizing, and grayscale conversion using histogram equalization. Feature extraction utilized Local Binary Patterns (LBP), followed by feature fusion at the feature level to create an integrated feature set. The enhanced SOFM algorithm was then applied for classification, with the CSO technique optimizing the learning rate and weight parameters for improved performance. At different thresholds, the CSO-SOFM classifier outperformed the standard SOFM classifier using Sensitivity, Specificity, Precision, Accuracy and Recognition time.

INTRODUCTION

Access control systems enable authorized users to access data or system components while preventing unauthorized individuals from gaining access, thereby safeguarding against illegal access, data modification, and confidentiality breaches (Kahie *et al.*, 2021; Atlam *et al.*, 2020). Biometric authentication, derived from "bios" (life) and "metric" (measuring), can be unimodal, bimodal, or multimodal, utilizing one, two, or multiple biometric modalities, respectively (Das *et al.*, 2018; Adedeji *et al.*, 2021a). It relies on physiological traits such as face, fingerprint, and iris, as well as behavioural traits like voice and gait, to identify individuals (Sabhanayagam *et al.*, 2018). Biometrics refers to the automated identification of individuals based on physical or behavioural characteristics such as face, fingerprints, voice, iris, gait, or signature (Singh *et al.*, 2019; Adetunji *et al.*, 2018). These biometric modalities are used in diverse applications, ranging from personal device access to border control (Jain *et al.*, 2016). Biometric systems, or Identity Verification (IV) systems, authenticate individuals by identifying and validating unique biometric traits (Bowyer and Burge, 2016). Since each person's biometric identifiers are unique and permanent, it becomes challenging for imposters to mimic registered individuals' biometric traits (Yang *et al.*, 2019). These systems, therefore, play a critical role in enhancing digital security and are in high demand in applications such as forensics, defence, surveillance, personal identification, and banking (Okediran and Oguntoye, 2023). Recently, soft biometric characteristics such as gender, weight, and age have been introduced to enhance recognition systems (Hassan *et al.*, 2021). The choice of biometric traits depends on their uniqueness and the intended application, with face, ear, and iris being commonly selected for their reliability and stability (Wang *et al.*, 2022; Zhou and Bhanu, 2009). These biometric technologies significantly enhance security and efficiency in access control systems' user validation processes. In earlier times, unimodal systems that relied on a single physiological or behavioural trait for biometric authentication were widely used for identity confirmation. However, they are now limited due to several shortcomings, including susceptibility to spoofing, low accuracy, lack of universality, and vulnerability to environmental factors (Adedeji *et al.*, 2021b). On the other hand, multimodal biometric systems, which integrate multiple or complementary biometric features obtained through different methods, offer enhanced security against spoofing attacks and demonstrate high reliability and robustness in dynamic environments (Atanda *et al.*, 2023). For example, while fingerprints are commonly used for identification, they can be compromised by issues such as scars, distortions, wounds, and residual oils, which may affect accuracy (Oloyede and Hancke, 2016). In this study, ear and iris traits were selected based on their distinctiveness and established performance. The ear is notable for its ease of capture, user-friendly nature, and suitability for contactless access control, a feature particularly valuable in maintaining hygiene in healthcare and during pandemic scenarios like COVID-19 (Oguntoye, *et al.*, 2023). Additionally, its stability throughout an individual's life and reliability under varying environmental conditions, such as lighting and background noise, further enhance its utility (Wang *et al.*, 2022; Zhou and Bhanu, 2009). The iris, with its lifetime stability, is recognized as one of the most accurate biometric traits. It can function as either a passive or active trait, depending on the proximity of the sensor to the individual.

A biometric system framework typically involves several operations: input of biometric characteristics, preprocessing, determining the region of interest, feature extraction, matching algorithms, and decision-making (Gomez-Barrero *et al.*, 2017). Preprocessing addresses variations in the input data, preparing it for feature extraction, where distinct patterns from the biometric trait are isolated (Ogundepo *et al.*, 2022). Matching algorithms then compare these extracted features against stored templates, and the decision-making phase authenticates or identifies the individual as a legitimate user or an imposter.

Biometric systems can be categorized based on various criteria (Sarmokaddam, 2017). For example, biometric traits can be classified as physiological (e.g., ear, fingerprints, face, iris, DNA) or behavioural (e.g., gait, voice, signature) (Adetunji *et al.*, 2018; Olayiwola *et al.*, 2023). Systems can also be unimodal, using a single biometric trait, or multimodal, using multiple traits for higher accuracy and security. Multi-sensor systems enhance accuracy by using multiple sensors to capture the same biometric trait, while Multi-Instance systems capture more than one instance of the same trait (e.g., multiple fingerprints). Additionally, Multi-Algorithm systems use multiple algorithms for feature extraction and fusion, further improving performance (Olayiwola *et al.*, 2024).

In multimodal biometric systems, fusion can occur at various stages, either before or after the matching phase. When fusion is carried out at the feature or sensor level, it occurs before the matching phase; in contrast, score and decision level fusion takes place after trait matching but before the final decision-making process. Sensor Level Fusion (Image Level Fusion) involves combining biometric modalities immediately after capture. Feature Level Fusion combines features from different biometric traits into a higher-dimensional feature vector containing rich raw data. Although this type of fusion can result in high dimensionality, effective preprocessing can mitigate this issue and improve recognition accuracy (Byahatti, 2017). Score Level Fusion combines scores generated by individual biometrics, while Decision Level Fusion merges decisions made by individual authentication systems to form the final decision (Nadheen and Poornima, 2013). Among these techniques, feature-level fusion is preferred because it uses raw biometric data, which contains rich information from raw images. This technique is expected to increase recognition accuracy, (Byahatti, 2017; Ola *et al.,* 2017). Therefore in this work, feature level fusion was chosen for its potential to enhance recognition accuracy by integrating information early in the processing stage.

Self-Organizing Feature Maps (SOFM) are machine learning algorithms that categorize input vectors based on their spatial arrangement, effectively learning the distribution and topology of the training data. This makes SOFMs highly effective for categorizing complex biometric data, as they map high-dimensional multimodal data onto a lower-dimensional map, extracting significant features and revealing underlying patterns (Wickramasinghe *et al.*, 2019; Ola *et al.,* 2020). The robustness of SOFMs is maintained through self-organization and continuous updates, with efficiency depending on well-tuned training parameters such as learning rate, neighbourhood function, input weights and weight update.

Several studies have explored multimodal biometric systems. For instance, Nadheen and Poornima (2013) in a paper titled Feature Level Fusion in Multimodal Biometric Authentication System examined the performance of ear and iris recognition individually and in combination using score level fusion. They extracted features using Principal Component Analysis (PCA) to reduce dimensionality while preserving information, demonstrating a 95% success rate with the multimodal approach. Similarly, Khursheed and Mir (2016) in a research titled Personal Verification Using Two Level Fusion Schemes Based on Ear and Iris Biometrics employed a two-level fusion scheme based on ear and iris biometrics, achieving a perfect recognition rate of 100% with zero False Acceptance Rate (FAR) and False Rejection Rate (FRR), the work could be computationally expensive since recognition time was not reported. Kaur *et al.(*2017) examined various security breach attacks in a paper titled **"**An Analysis of Security Breach Attacks and Errors in Biometric Systems". An analysis of error rates and security breaches was performed, but the focus was on analyzing breach attacks and errors such as False Acceptance Rate (FAR), False Rejection Rate (FRR), and Failure to Enroll (FTE) that occur during data capture. Ma *et al.* (2020) in the paper "An Overview of Multimodal Biometrics Using the Face and Ear", highlight the advantages of using ear biometrics alongside face recognition to address issues such as facial expression, pose variation, and occlusion, as ear structure is more stable and less affected by ageing. While combining face and ear improves accuracy and robustness in biometric systems, the study explored biometric quality-based adaptive fusion, offering a flexible approach to integrating face and ear recognition under varying conditions. However, the paper focused on degenerated images and the research was not tested with other biometric traits to ascertain its effectiveness. Sarangi *et al.* (2021) in a research paper titled **"**A feature-level fusion based improved multimodal biometric recognition system using ear and profile face**"**, proposed a system combining ear and profile face biometrics, using PCA and z-score normalization for feature extraction and k-nearest neighbour (KNN) for classification, demonstrating superior accuracy with multimodal data. The system made use of supervised learning algorithms which may experience overfitting when very large data is not used.

Shaban et al. (2023) in the paper titled "A Novel Fusion System Based on Iris and Ear Biometrics for E-exams" presented a system that uses ear and iris biometrics to identify students during electronic exams. The system applied Haralick texture for ear features and Tamura texture for iris features, and then fused them at the feature level, achieving 97% recognition accuracy. The study was particularly relevant during the COVID-19 pandemic and focused majorly on recognition accuracy without discussing the system's efficiency, specifically the recognition time. While the fusion of ear and iris traits at the feature level achieved 97% accuracy, there is no analysis of processing speed, which is crucial in real-time applications like electronic exams. This omission leaves room for further exploration in balancing accuracy with processing time.

This paper addresses the limitations of unimodal biometric systems—such as susceptibility to spoofing and environmental constraints—by introducing an advanced multimodal biometric system that combines ear and iris recognition. It improved the classification accuracy of ear-iris multimodal biometrics through an enhanced SOFM algorithm optimized with Chicken Swarm Optimization (CSO), thus addressing accuracy issues observed in previous multimodal systems like those studies by Nadheen and Poornima (2013) and Shaban et al. (2023). By refining the classification algorithm and optimizing parameters, this paper enhances recognition performance and evaluates the new CSO-SOFM classifier against traditional methods, demonstrating superior results in accuracy, sensitivity, specificity, and processing time.

RESEARCH METHOD

The study implemented a multimodal access control system integrating ear and iris biometrics using Chicken Swarm Optimization and Self-Organizing Feature Maps (CSO-SOFM) in MATLAB 2016a. The system development proceeded through five stages: data acquisition, preprocessing, feature extraction, fusion, and classification. Figure 1 illustrates the framework of the CSO-SOFM access control system, detailing its design and development stages.

Data Acquisition

This study captured high-quality iris, and outer ear images from 190 individuals at the LAUTECH Campus, ensuring uniform lighting conditions throughout the image acquisition process. Each biometric trait comprised six instances of each trait (6 instances*2 traits*190), resulting in a dataset of 2,280 images with a resolution of 100x100 pixels. Samples of acquired images are as shown in Figure 2

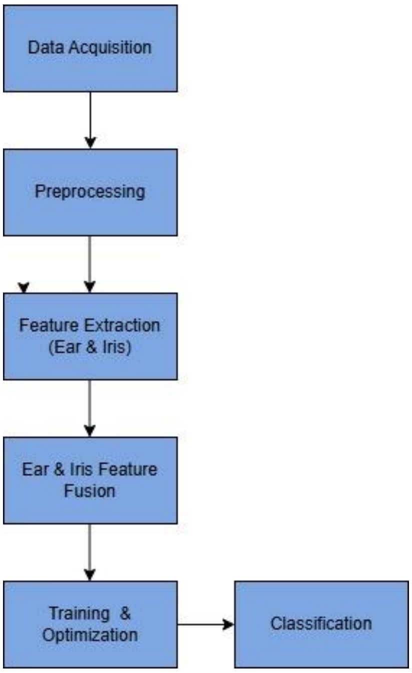

Figure 1. Framework of the CSO-SOFM access control system.

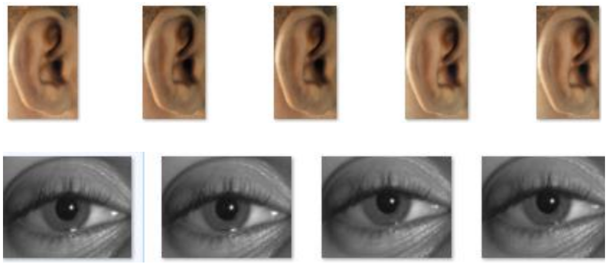

Figure 2. Samples from acquired ear and iris images

Data Preprocessing

After acquiring the local dataset, ear, and iris images underwent preprocessing steps including cropping, resizing, and conversion to grayscale using histogram equalization. Average vectors representing each biometric trait were extracted to enhance image clarity and reduce noise. Visual examples of the enhanced images using histogram equalization are depicted in Figure 3.

Normalization of Feature Vector

Feature vectors extracted from the dataset initially exhibited variations in range and distribution. To ensure uniformity, all traits were resized to 128x128 pixels.

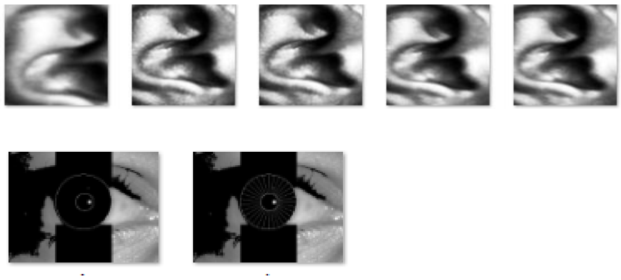

Figure 3. Samples of preprocessed images using histogram equalizer.

Subsequently, pixel values were normalized to a standard scale ([0, 1]) using the min-max normalization method. For a feature vector $X = \{x1, x2, x3,..., xn\}$, the normalized feature vector X' was computed using equation 1

$$X = \frac{xi - \min(X)}{\max(X) - \min(X)} \qquad (1)$$

Feature Extraction and Fusion

In this study, Local Binary Patterns (LBP) were employed for ear feature extraction, while the Log-Gabor filter was used for iris feature extraction. The LBP method determines the binary code of each central pixel by comparing it with its eight neighbouring pixels, as outlined in equations (2) and (3). These binary codes are then consolidated into a final representation for the central pixel using equation (4). To ensure robustness in feature extraction across the dataset, bilinear interpolation was incorporated to accurately compute the grey values of neighbouring pixels. The equations used for this process are as follows:

$$xL = gp - gc \qquad (2)$$

$$(xL) = \{01xx^{L}L^{\geq}\leq{}^{0}\ 0\} \qquad (3)$$

$$\text{LBP p(P, R)} = \Sigma\,(g(xL) * 2^{i}), \qquad (4)$$

for i = 0 to (P-1)

where $gpandgc$ refers to the grey value of neighbours and centre pixels, respectively; while 2^i indicates the binomial value. The two parameters P and R are referred to as the coordinates of the centre pixel. p refers to the total number of neighbours, while i refers to the current neighbour value. LBP(P, R) is the Local Binary Pattern value at the center pixel P with a radius of R. g(xL) is a function that returns 1 if the intensity of the neighbouring pixel xL is greater than or equal to the intensity of the center pixel P, and 0 otherwise.

For iris feature extraction, the Log-Gabor filter was used to extract the best features from the iris images. This process began with the setting of key parameters, including the center frequency p_0 and bandwidth σ. The normalized iris image was then converted to the frequency domain using the Fourier Transform. Next, the Log-Gabor filter transfer function, as specified in equation (5), was applied to the frequency domain representation of the iris image:

$$G(p) = \exp\left(-\frac{(log\ (p/p_0))^2}{2(log\ (\sigma/p_0))^2}\right) \quad (5)$$

Here, G(p) represents the transfer function of the Log-Gabor filter at frequency p, where p is the frequency variable, p_0 is the center frequency of the filter, and σ is the bandwidth parameter of the filter. Following this, the filtered image was converted back to the spatial domain using the Inverse Fourier Transform. Finally, phase information was extracted from the filtered image and encoded into a binary code known as the iris code. After the features had been extracted and normalized, Feature fusion was used to concatenate features extracted from the dataset to form a new, integrated feature set, facilitating the combination of incompatible feature vectors from multiple modalities. This process occurs at the feature level, merging the biometric information before matching through a weighted mean of the normalized feature vectors from each modality. The resulting fused vector is a single representation, achieved by assigning different weights to each feature and using the weighted average rule. The weighted average, also known as the weighted mean, calculates the combined value of multiple inputs to create a new pixel intensity or image for digital representation.

Classification using Enhanced SOFM (CSO-SOFM)

The SOFM is a simple artificial network that learns through an unsupervised method, similar to how human brains learn. It maps input vectors to specific output nodes without needing predefined input-target pairs, following a "winner takes all" strategy. This allows the automatic grouping of the dataset into the output layer nodes based on similarity. All neurons in the input layer are connected to those in the output layer, with the feature vector length determining the number of input neurons and the output classes determining the output layer size. During learning, input vectors are mapped to the output based on similarity, and the weight matrix W_{ij} connects input and output neurons.

Initially, the closest output neuron to the input vector is activated, termed the winner node. The weights of the winner node are adjusted to approximate the input vector closely, using the equation:

$$w_i(k) = w_{i,j}(k-1) + \alpha_r(x_i - w_{i,j}(k-1)) \quad (3)$$

Where: $w_i(k)$is the updated weight for the ith neuron at iteration k,$w_{i,j}(k-1)$ is the weight of the ith neuron at the previous iteration$(k-1)$, x_i is the input value for the ith neuron, and α_r is the learning rate usually chosen to be less than 1.

The SOFM was enhanced using the Chicken Swarm Optimization (CSO) technique instead of the standard weight update equation, making it more robust and improving performance. After learning, the weights are settled, (the weight reaches a state where they no longer change significantly) and used in the testing phase, where the input feature vectors are classified based on the dot product with the weight matrix. The CSO algorithm optimized the SOFM learning rate and weight parameters, transforming 3-D discrete maps into 2-D discrete maps for better accuracy.

The CSO-SOFM requires the training and classification stage. Training involves initializing neuron weights, sampling input vectors, finding the Best Matching Unit (BMU), and updating neuron weights. Training can be sequential, suitable for online learning, or batch, suitable for offline learning; (Kohonen, 2012; Bullinaria, 2004), sequential training was used.

The following steps were used for the CSO-SOFM training:

i. Input: This includes the following-

-training data X (the ear and iris data)

-SOFM parameters- the number of neurons, learning rate, number of iterations

-CSO parameters- coefficients for rooster, hen and chick

Vector Selection: An input vector is selected randomly from the dataset.

ii. SOFM and CSO Initialization:

-Initialize, normalize and establish SOFM and CSO network parameters-initialize a population of N chickens, positions of chicken, evaluate the fitness of the chicken and define other related parameters; set the SOFM learning rate, the neuron weights, the number of inputs and the number of iterations.

-Assign roles to each neuron (e.g., rooster, hen, and chick).

-Set CSO parameters: $\alpha, \beta, \gamma, \delta, \epsilon \zeta, \eta$.

iii. Determination of Winning Node: The winning node is also called the BMU, and it is determined by calculating the Euclidean distance between the connection weight and the randomly selected input. Find the best matching unit (BMU), c, with weights:

$$wBMU = arg\text{wi}min \parallel x - wi \parallel \quad (6)$$

where x is the Input Vector and $w_i$is the weight vector.

iv. Update weight using CSO: Instead of the continuous adjustment of the winning neuron and the connection weight of the neuron, the weight is updated using Chicken Swarm Optimization Algorithm in place of equation (6);

-For Roosters:

$$\mathrm{wi(t+1) = wi(t) + \alpha\big(wbest - wi(t)\big) + \beta \cdot N(0,1)} \quad (7)$$

where:

w best is the best weight vector found globally,α and β are coefficients, and N (0,1) is a normally distributed random number

-For Hens:

$$\mathrm{wi(t+1) = wi(t) + \gamma(wr(t) - wi(t)) + \delta(ws(t) - wi(t)) + \epsilon \cdot N(0,1)} \quad (8)$$

where:

wr(t)is the weight vector of a rooster, ws is the weight vector of another hen, γ, δ, and ϵ are coefficients, and N(0,1) is a normally distributed random number.

-For Chicks:

$$wi(t+1) = wi(t) + \zeta(wh(t) - wi(t)) + \eta \cdot N(0,1) \quad (9)$$

where:

wh(t) is the weight vector of the mother hen, ζ and η are coefficients, and N(0,1) is a normally distributed random number.

Update wbest based on the performance of the weight vectors with respect to the training data.

v. **Stopping Criteria:** The algorithm then checks if all the sample images have been considered and if the number of iterations has been met. If yes, it stops but if not completed, the image count is incremented, and the iterations are repeated until completion or a stopping criterion is met.

RESULTS AND DISCUSSION

This research developed an ear-iris-based access control system using the Chicken Swarm Optimization Self-Organizing feature map (CSO-SOFM) algorithm as a classifier. The system performance was validated using sensitivity (SEN), specificity (SPEC), precision (PREC), false positive rates, accuracy (ACC) all in percentage, and recognition time (Time) in seconds at varying thresholds. The results of the metrics were based on the confusion matrices' concepts which are: the True Positive (TP), True Negative (TN), False Positive (FP), and False Negative (FN) values achieved by the system against the actual outcomes.

The acquired 2,280 images were split into training (70%, 1,596 images) and testing (30%, 684 images) subsets to evaluate the performance of the developed system. The trained model was evaluated using the ear and iris traits. The results were evaluated using a threshold value, a decision boundary parameter that determines the behaviour of the classifiers as a range between 0 or 1. The thresholds between 0 and 1 were tested. Experimental results showed that the classifiers had constant values between 0-0.20, 0.21-0.35, 0.36-0.50, and between 0.51-0.99. Therefore, thresholds 0.20, 0.35, 0.50 and 0.80 were chosen.

The classification model's performance metrics across four threshold levels (0.20, 0.35, 0.50, and 0.80) show a consistent trade-off between sensitivity and specificity, with the highest accuracy of 94.44% achieved at a threshold of 0.80, where the model correctly identified 246 true positives and 77 true negatives, while minimizing false positives to 8 and false negatives to 11, all computed in approximately 97 seconds.

As seen in Table 1, True Positives slightly decreased from 249 to 246, while True Negatives increased from 70 to 77. The False Positive Rate showed significant improvement, dropping from 17.65% to 9.41%. Sensitivity remained relatively stable, decreasing marginally from 96.89% to 95.72%. Specificity improved considerably from 82.35% to 90.59%. Precision and Accuracy both showed steady improvements, with Precision increasing from 94.32% to 96.85% and Accuracy from 93.27% to 94.44%. Processing time slightly decreased from 97.88 to 96.86 seconds. Overall, the higher threshold of 0.80 demonstrated the best balance of performance metrics, with improved specificity and precision at a minimal cost to sensitivity, as the threshold increased.

Also, from Table 2, the performance of the CSO-SOFM classifier improved as the threshold increased from 0.20 to 0.80, with the best results achieved at a threshold of 0.80, where True Positives remained high at 251, False Positives decreased to 4, True Negatives increased to 81, False Positive Rate reduced to 4.71%, Sensitivity maintained at 97.67%, Specificity improved to 95.29%, Precision increased to 98.43%, Accuracy peaked at 97.08%, and the recognition time decreased to 86.83 seconds, demonstrating an

Table 1. Results of Standard SOFM

Threshold	TP	FN	FP	TN	FPR (%)	SEN (%)	SPEC (%)	PREC (%)	ACC (%)	Time (sec)
0.20	249	8	15	70	17.65	96.89	82.35	94.32	93.27	97.88
0.35	248	9	13	72	15.29	96.50	84.71	95.02	93.57	97.29
0.50	247	10	11	74	12.94	96.11	87.06	95.74	93.86	96.78
0.80	246	11	8	77	9.41	95.72	90.59	96.85	94.44	96.86

Table 2. Results of CSO-SOFM

Threshold	TP	FN	FP	TN	FPR (%)	SEN (%)	SPEC (%)	PREC (%)	ACC (%)	Time (sec)
0.20	253	4	12	73	14.12	98.44	85.88	95.47	95.32	87.85
0.35	252	5	9	76	10.59	98.05	89.41	96.55	95.91	87.07
0.50	251	6	6	79	7.06	97.67	92.94	97.67	96.49	87.03
0.80	251	6	4	81	4.71	97.67	95.29	98.43	97.08	86.83

optimal balance between classification accuracy and computational efficiency.

The results demonstrated a clear trade-off between sensitivity and specificity as the decision threshold varies. At lower thresholds (e.g., 0.20), the system achieves higher sensitivity but at the cost of higher false positive rates and lower specificity. Conversely, higher thresholds (e.g., 0.80) lead to improved specificity and precision, reducing the likelihood of false positives but slightly lowering sensitivity.

The optimal threshold value appears to be a balance between minimizing false positives and maintaining high sensitivity and accuracy. A threshold of 0.80 yields the best specificity (95.29%) and precision (98.43%) with a slight decrease in sensitivity (97.67%). This threshold also provides the highest accuracy (97.08%), indicating its effectiveness in maintaining a high level of security and performance in multimodal biometric systems.

The results demonstrated the superior performance of the Modified SOFM (CSO-SOFM) over the Standard SOFM across various threshold values. The Modified SOFM (CSO-SOFM) consistently achieves higher accuracy, precision, and specificity while maintaining lower false positive rates compared to the Standard SOFM.

This result agrees with Purohit and Ajmera (2020) who implemented a similar multimodal biometric system using Gray Wolf Optimization Algorithm (GWOA). However, the result of the Modified CSO-SOFM outperformed that of Purohit and Ajmera, (2020) in terms of sensitivity, specificity andaccuracy while the record of precision and processing time were not extensively reported. Purohit and Ajmera, reported sensitivity, specificity and accuracy all as 91.667% while this research using CSO-SOFM had sensitivity as 97.67%, specificity as 95.29%, precision as 98.43%, accuracy as 97.08% at 86.83 seconds.

Hence, this research demonstrates the effectiveness of the CSO algorithm in enhancing the classification performance when combined with SOFM.

CONCLUSION

The proposed multimodal biometric access control system, combining ear and iris traits and utilizing an enhanced CSO-SOFM algorithm, indicates that the Modified CSO-SOFM outperforms the Standard SOFM in all key performance metrics, particularly in terms of accuracy, sensitivity, specificity, false positive rate and recognition time. These improvements suggest that the Modified CSO-SOFM is a more reliable and efficient approach for enhancing access control systems with multimodal biometrics, and the efficient processing times also suggest better applicability for real-time systems. Future works will explore the integration of additional biometric traits and further optimization techniques to enhance system performance.

REFERENCES

Adedeji, O. T., Alade, O. M., Oguntoye J. P., Awodoye, O. O. (2021a). 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): 25-34.

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

Atanda, O. G., Ismaila, W., Afolabi, A. O., Awodoye, O. A., Falohun, A. S., & 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)*. 1: 1-10.

Atlam, H. F., Azad, M. A., Alassafi, M. O., Alshdadi, A. A., and Alenezi, A. (2020). Risk-based access control model: a systematic literature review. Future Internet, 12(6), 103.

Byahatti, P. (2017). *A Fusion Model for Multimodal Biometric System*. *5*(06), 1–5.

Das, A., Galdi, C., Han, H., Ramachandra, R., Dugelay, J. L., and Dantcheva, A. (2018, October). Recent advances in biometric technology for mobile devices. In 2018 IEEE 9th International Conference on biometrics theory, applications and systems (BTAS) (pp. 111). IEEE.

Fathima Nadheen, M., and Poornima, S. (2013). Feature Level Fusion in Multimodal Biometric Authentication System. *International Journal of Computer Applications*, *69*(18), 36–40. https://doi.org/10.5120/12074-8264

Gomez-Barrero, M., Galbally, J., Rathgeb, C., and Busch, C. (2017). General framework to evaluate unlinkability in biometric template protection systems. IEEE Transactions on Information Forensics and Security, 13(6), 1406-1420.

Hassan, B., Izquierdo, E., and Piatrik, T. (2021). Soft biometrics: a survey Benchmark analysis, open challenges and recommendations. Multimedia Tools and Applications.

Kahie, S. A., Nor, A. A., Hasan, A. H., Abdi, A. M., Hassan, L. M., and Mohamud, M. A. (2021, August). A Smart Access Control for Restricted Buildings Using Vehicle Number Plates Recognition System. In 2021 1st International Conference on Emerging Smart Technologies and Applications (eSmarTA). 1-5.

Kaur, G., Singh, S., and Kaur, N. (2017). Comparative Analysis Of Multimodal Biometric System. *An International Journal of Engineering Science, Special*, (2018), 129-137.

Khursheed, F., & Mir, A. H. (2016). Personal Verification Using Two Level Fusion Schemes Based on Ear and Iris Biometrics. *International Journal of Computing and Digital Systems*, *5*(06).

Ma, Y., Huang, Z., Wang, X., and Huang, K. (2020). An Overview of Multimodal Biometrics Using the Face and Ear. *Mathematical Problems in Engineering*, *2020*. https://doi.org/10.1155/2020/6802905.

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): 1-12.

Oguntoye, J. P., Awodoye, O. O., Oladunjoye, J. A., Faluyi, B. I., Ajagbe, S. A., & 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., & 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, 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): 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): 19-26.

Olayiwola, D. S., Olayiwola, A. A., Oguntoye, J. P., Awodoye, O. O., Ganiyu, R. A., & Omidiora, E. O. (2024). Development of A Palm-Vein Recognition System for Identification and Verification Systems using Enhanced Convolutional Neural Network. *FUOYE Journal of Engineering and Technology.* 9 (1): 62-69.

Olayiwola, D. S., Olayiwola, A. A., Oguntoye, J. P., Awodoye, O. O., Ganiyu, R. A., & 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.

Purohit, H., and Ajmera, P. K. (2020). Optimal feature level fusion for secured human authentication in a multimodal biometric system. *Machine Vision and Applications, 32*(1). https://doi.org/10.1007/s00138-020-01146-6.

Sabhanayagam, T., Venkatesan, V. P., and Senthamaraikannan, K. (2018). A comprehensive survey on various biometric systems. International Journal of Applied Engineering Research, 13(5), 2276-2297.

Sarangi, P. P., Nayak, D. R., Panda, M., and Majhi, B. (2021). A feature-level fusion based improved multimodal biometric recognition system using ear and profile face. *Journal of Ambient Intelligence and Humanized Computing*. https://doi.org/10.1007/s12652-021-02952-0

Shaban, S. A., Ahmed, H. M. M., & Elsheweikh, D. L. (2023). *A novel fusion system based on iris and ear biometrics for e-exams. Intelligent Automation & Soft Computing, 35*(3), 3295-3315. https://doi.org/10.32604/iasc.2023.030237

Strunk, W., Jr., and White, E. B. (1979). *The elements of style.* (3rd ed.). New York: Macmillan, (Chapter 4).

Van der Geer, J., Hanraads, J. A. J., and Lupton R. A. (2000). The art of writing a scientific article. *Journal of Scientific Communications*, 163, 51-59

Wang, Q., Hou, L., Hong, J. C., Yang, X., and Zhang, M. (2022). Impact of Face-Recognition-Based Access Control System on College Students' Sense of School Identity and Belonging During COVID-19 Pandemic. *Frontiers in Psychology, 13,* 808189. https://doi.org/10.3389/fpsyg.2022.808189

Wickramasinghe, C. S., Amarasinghe, K., and Manic, M. (2019). Deep self-organizing maps for unsupervised image classification. IEEE Transactions on Industrial Informatics, 15(11), 5837-5845.

Yang, P., Wang, D., Wei, Z., Du, X., and Li, T. (2019). An outlier detection approach based on an improved self-organizing feature map clustering algorithm. IEEE Access, 7, 115914115925.

Zhou, Q., and Bhanu, B. (2009). Ear Biometrics: A Survey. Journal of Pattern Recognition Research, 4(1), 80–97.