Computers, Materials & Continua

Tech Science Press

Doi:10.32604/cmc.2025.062440

ARTICLE

An Improved Chicken Swarm Optimization Techniques Based on Cultural Algorithm Operators for Biometric Access Control

Jonathan Ponmile Oguntoye[1], Sunday Adeola Ajagbe[2,3,*], Oluyinka Titilayo Adedeji[1], Olufemi Olayanju Awodoye[1], Abigail Bola Adetunji[1], Elijah Olusayo Omidiora[1] and Matthew Olusegun Adigun[2]

[1]Department of Computer Science and Engineering, Ladoke Akintola University of Technology, Ogbomoso, 210214, Nigeria
[2]Department of Computer Science, University of Zululand, Kwadlangezwa, 3886, South Africa
[3]Department of Computer Engineering, Abiola Ajimobi Technical University, Ibadan, 200255, Nigeria

*Corresponding Author: Sunday Adeola Ajagbe. Email: saajagbe@pgschool.lautech.edu.ng

Received: 18 December 2024; Accepted: 24 March 2025; Published: 30 July 2025

ABSTRACT: This study proposes a system for biometric access control utilising the improved Cultural Chicken Swarm Optimization (CCSO) technique. This approach mitigates the limitations of conventional Chicken Swarm Optimization (CSO), especially in dealing with larger dimensions due to diversity loss during solution space exploration. Our experimentation involved 600 sample images encompassing facial, iris, and fingerprint data, collected from 200 students at Ladoke Akintola University of Technology (LAUTECH), Ogbomoso. The results demonstrate the remarkable effectiveness of CCSO, yielding accuracy rates of 90.42%, 91.67%, and 91.25% within 54.77, 27.35, and 113.92 s for facial, fingerprint, and iris biometrics, respectively. These outcomes significantly outperform those achieved by the conventional CSO technique, which produced accuracy rates of 82.92%, 86.25%, and 84.58% at 92.57, 63.96, and 163.94 s for the same biometric modalities. The study's findings reveal that CCSO, through its integration of Cultural Algorithm (CA) Operators into CSO, not only enhances algorithm performance, exhibiting computational efficiency and superior accuracy, but also carries broader implications beyond biometric systems. This innovation offers practical benefits in terms of security enhancement, operational efficiency, and adaptability across diverse user populations, shaping more effective and resource-efficient access control systems with real-world applicability.

KEYWORDS: Access control; biometric technology; chicken swarm optimization; cultural algorithm; pattern recognition

1 Introduction

The administration of an access point, such as a door, turnstile, elevator, etc., to ensure that only authorized people are permitted admission, is referred to as access control [1]. Doors are the most typical access control applications, even though access control systems can be utilized for nearly any access point that incorporates an electronic lock mechanism. Access control systems can be based on what the user *has* (object-based), e.g., Keys, Fobs and ID Cards, what the user *knows* (information-based), e.g., Password, Pass-phrase, and PIN number, or who the user *is* (biometric-based): palm vein, fingerprint, iris, and face [2]. Biometric access control is among the most extensively utilized security systems available today due to the unique way it combines simplicity and security such as biometric authentication and facial animation [3]. Identity fraud is now considered among the most prevalent criminal acts since it is associated with dangerous security risks and a high cost. Given the imperative for exceptionally dependable security procedures in critical systems,

it has become necessary to implement rigorous measures. Several strategies, including the use of biometric techniques, have been used to prevent these problems [4,5].

The fingerprint trait is modern, safe, dependable, extremely accurate, and economical. Its matching procedure is quick and uses little memory space [6]. It may, however, cause problems due to absence, wounds, scars, dust, filth, twisting, and physical interaction with the system. It may also be applicable for driver identification, law enforcement, forensics, license, and access control [7]. Face recognition is a desirable biometric identifier due to its collectability and social acceptability. Facial recognition technology is well suited for surveillance applications since the face image may be taken from a distance without the user's participation [8]. Face biometrics need no physical contact, and template storage is simple, convenient, and has fewer complex statistics. Face biometric identification has a fast processing speed [9]. Nevertheless, facial attributes can change with time, age, and random events. The accuracy of a face recognition system can also be affected by lighting. Face recognition is also useful for access control verification, criminal identification, and surveillance [10]. Iris biometrics are more protective and have a higher degree of diversity, scalability, and accuracy with a small sample size. The processing speed is fast but expensive, and it requires no physical contact but user cooperation. The disease can also affect accuracy. Its utility extends to identification applications, access control, and national security [11].

Several techniques have been developed to facilitate the efficient recognition of biometric modalities. Intra-class variability, inter-class similarity, noisy input, mistake rate, high processing cost, and complexity remain obstacles for biometric recognition systems. As a result of their high dimensions, biometric image pixels are highly correlated. This results in redundant information and a computational burden for existing approaches in terms of processing speed and memory use [12,13]. These challenges can be solved with efficient optimization techniques [14].

The adoption of systematic methodologies, strategies, disciplines, and tactics to enhance a particular process within the confines of a project or initiative is known as an optimization technique in machine learning based work. It improves accuracy, reduces risk, minimizes mistakes, enhances effectiveness, and many more.

Several optimization techniques have been proposed to address pattern recognition challenges, as exemplified by the research conducted by [15,16] each exhibiting unique strengths and limitations. Notably, Chicken Swarm Optimization (CSO) is a technique inspired by the behaviors of the chicken swarm, where the intelligence of the chicken swarm is effectively utilized to obtain the optimal solution. The CSO replicates the hierarchical structure and food-seeking behavior observed in a swarm of chickens. Although the CSO method has performed well in tackling several issues, it also has several intrinsic flaws, including premature convergence and falling into local extrema. This study seeks to enhance the efficacy of CSO using cultural algorithm operators for biometric access control. The novel aspects of the Improved Cultural Chicken Swarm Optimization (CCSO) lie in its innovative integration of cultural algorithm operators with the standard CSO framework. This creates a hybrid approach that overcomes key limitations of CSO, such as premature convergence and suboptimal trapping in local optima [17]. In contrast to traditional CSO, which relies solely on swarm-based heuristics, CCSO integrates cultural components: belief space adjustments, and influence functions, to dynamically guide the optimization process.

These cultural operators enhance both the exploration phase, by maintaining population diversity, and the exploitation phase, by refining solution convergence. This dual enhancement enables CCSO to balance the trade-off between global and local search effectively. This will significantly enable the CCSO to outperform the basic CSO, Particle Swarm Optimization (PSO), and similar algorithms. The CCSO's ability to adaptively optimize multi-dimensional feature spaces in the biometric domain ensures higher accuracy and robustness in multimodal biometric systems. This is particularly critical for addressing challenges like

complex data distributions and high-dimensional feature selection, where the traditional algorithms often fall short [18]. Therefore, adapting the cultural evolution strategies, the application of CCSO is targeted to improve the convergence rate and ensure more reliable performance in real-world biometric applications, such as access control, where security and precision are paramount. Existing biometric access control systems struggle with high-dimensional data processing, inconsistent feature selection, and limited adaptability to diverse biometric traits. CCSO addresses these limitations through its cultural operators, enabling robust handling of complex data distributions and dynamic optimization of feature spaces, crucial for maintaining security standards in real-world applications.

The proposed technique has the following contributions:

(i) The study applied the cultural-based CSO technique based on cultural algorithm operators for biometric access control.
(ii) The significance of the cultural-based CSO technique is highlighted for biometric access control using face, fingerprint, and iris traits.
(iii) The study validates the cultural-based CSO against the CSO technique for biometric access control using face, fingerprint, and iris traits.
(iv) The performance evaluation of the proposed techniques was carried out using accuracy, precision, False Acceptance Rate (FAR), and False Rejection Rate (FRR), and the techniques were compared using state-of-the-art existing techniques.

The structure of this research is as follows: Section 2 provides a review of related work. Section 3 showcases the detailed research methodology utilized. Section 4 presents the results and ensuing discussion, while Section 5 outlines conclusions and future research avenues to achieve efficient biometric access control.

2 Literature Review

Previous studies have proven that it is possible to authenticate a person using several types of biometric modalities. It has been noted that biometrics' potential use in access control remains a hot topic of study. Rizk et al. [19] applied neural network classification for iris recognition using both PSO and gravitational search algorithm (GSA). Canny Edge Detection and Circular Hough Transforms identify iris borders. The Daugman rubber sheet model plays a crucial role in normalizing the extracted IRIS area, while the Haar wavelet transform is utilized to extract features from the normalized iris area. Principal component analysis then reduces the feature matrix, and to train a forward neural network with optimal weights and biases, PSO and GSA were employed. Remarkably, GSA has been found to outperform PSO for training the feed-forward neural network in an iris identification system. In another study, Adetunji et al. [12] explored the reduction of computational cost in face recognition applications through the use of a hybrid cultural algorithm. Specifically, the Cultural Algorithm optimizes SVM parameters to reduce computation. Testing shows that the proposed method boosts SVM efficiency and cuts compute and memory usage. Moreover, Adedeji et al. [15] performed a comparative analysis of feature selection techniques for fingerprint recognition using Artificial Bee Colony (ABC) and teaching learning-based optimization (TLBO). Their results demonstrate that TLBO outperforms the ABC technique as a feature selection technique in fingerprint recognition and leads to more discriminant features in fingerprint identification. Consequently, the study found that TLBO feature selection is better than ABC and would generate a more reliable and accurate fingerprint authentication system.

Furthermore, optimization techniques find applicability in a wide range of fields, spanning pattern recognition, machine learning, image analysis, and biometrics. Notably, Oguntoye et al. [16] employed an Optimized Convolution Neural Network (OCNN) to diagnose COVID-19 from chest X-ray images,

optimizing the network with PSO. This method eliminates iterative weight adjustments, markedly boosting computational speed and achieving an impressive accuracy rate of 99.20%. Recent advancements in feature selection have introduced new optimization methodologies aimed at dealing with the challenges associated with high-dimensional biometric datasets. Grey Wolf Optimizer, Whale Optimization Algorithm, Particle Swarm Optimization, Gravitational Search Algorithm [20], Firefly Algorithm, and Levy flight-based Chicken Swarm Optimization techniques [21] have been applied with the aim to improve classification accuracy, reduce dimensionality, and to avoid the problem of local optimum.

For this study, the proposed CCSO approach will be evaluated to examine its unique contributions to feature selection. Chicken Swarm Optimization (CSO) and its enhanced variants are becoming the state-of-the-art literature on feature selection due to their robust performance in dimensionality reduction as well as classification accuracy in various domains. Ahmed et al. [17] introduced a Chaotic CSO (CCSO), which uses chaotic maps to combat premature convergence and significantly improves classification accuracy. A study by Hafez et al. [22] showed that CSO was useful for choosing features at power plants. They found that swarm intelligence was better at choosing features than the more traditional PSO and GA methods. More recently, Wang et al. [23] combined Levy flight and inertial weight strategies with CSO to globally search and avoid local optima. In detail, Abolarinwa et al. [18] extended CSO for face recognition, and Verma et al. [21] introduced a two-stage hybrid scheme of multi-Philtre feature selection and Levy's flight-based CSO with unsurpassed feature reduction and forecasting precision. Self-adaptive CSO was applied to mango grading in a hybrid model by Kumari et al. [24] and the algorithm showed its adaptiveness and precision. However, limitations such as local optima challenges are shown in these studies as well as CSO's adaptability across tasks. The proposed Improved CCSO further advances this line of research by incorporating cultural algorithm operators, enabling enhanced exploration and exploitation. The CCSO is proposed to achieve superior classification performance and feature reduction compared to other optimization techniques like PSO, GA, and variants of CSO. This is to reinforce its relevance and efficacy in multimodal biometric systems.

It is evident from previous studies that biometric authentication has been a focal point of research in recent years. These studies have collectively demonstrated the continuous evolution and innovation in optimization techniques to enhance various biometric modalities, emphasizing their critical role in improving biometric system performance, including accuracy, computational efficiency, and feature selection. Moreover, they signify the broader applicability of optimization techniques in diverse fields, aligning with the exploration of an improved CSO technique in this study. The proposed CCSO technique, as discussed earlier, builds upon optimization principles, balancing exploration and exploitation, which can significantly contribute to the advancement of biometric access control systems.

3 Materials and Methods

The steps involved in the implementation of improved chicken swarm optimization techniques based on Cultural algorithm operators for biometric access control include the following:

1. Face, iris, and fingerprint datasets acquisition.
2. Preprocessing of the face, iris, and fingerprint datasets.
3. Feature Extraction of each dataset using the Haar Wavelet-Based Technique.
4. Feature selection using the Cultural Chicken Swarm Optimization technique.
5. Generating matching score from optimized feature using Mahalanobis distance.
6. Identification of the subject as a genuine user or impostor.

The scheme of the proposed biometric recognition system is presented in Fig. 1.

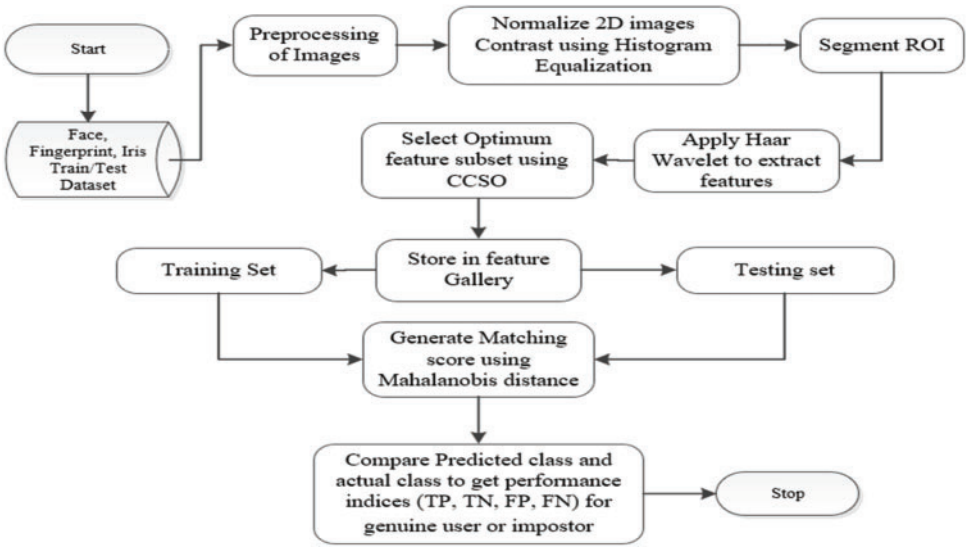

Figure 1: Block diagram of CSO techniques based on biometric access control

3.1 Acquisition of Biometric Traits

A total of 240 students at LAUTECH had their facial features, irises, and fingerprints scanned using a digital camera, an iris camera, and a fingerprint sensor. The subjects' fingerprints, irises, and facial images were stored. Three images were captured of each person's face from the front, with little variation in expression. Only 200 people were captured adequately. Therefore, 600 images of faces, irises, and fingerprints were used to train and evaluate the technique. Some of the acquired images are depicted in Fig. 2. Training and testing employed 360 and 240 trait images, respectively. Each component in the scheme is explained in detail in the sub-sections. Ethical approval was obtained from LAUTECH Ethics Review Committee in a letter dated 23 March 2023 for the collection and analysis of face, fingerprint, and iris biometrics. All data were anonymized, securely stored, and collected with informed consent, ensuring participant privacy and compliance with ethical standards.

Figure 2: Acquired images

3.2 Pre-Processing of Biometric Traits

Pre-processing encompasses acts including image brightness adjustment, scaling, filtering, cropping, segmentation, normalization, and additional operations that facilitate image enhancement. This section delineates the approach for pre-processing face, iris, and fingerprint datasets. The face dataset was pre-processed by image cropping and normalization. The normalization of the facial photos was executed by histogram equalization to enhance contrast by expanding the intensity range. This improved the luminance in the grayscale photos enabling a more distinct observation of the face characteristics in a vision guide work. By employing a sequence of preprocessing techniques, such as normalization, segmentation, orientation estimation, ridge filtering, binarization, and thinning, the fingerprint images were enhanced to improve their quality. The normalization process involved specifying a pre-determined mean and variance for the input fingerprint image. The Histogram equalization (HE) technique mapped the grey levels based on the probability distribution of the input grey levels. Histogram equalization flattened and stretched the dynamic range of the image's histogram. As a consequence of this, the image's contrast is improved, leading to an enhanced thumbprint image that can be utilized for feature extraction.

Segmentation, normalization, and enhancement were the operations performed on the iris images. Segmentation was conducted to eliminate extraneous information, specifically the pupil segment and the area beyond the iris. It assessed the iris perimeter. For boundary estimation, the iris images were initially processed using the Canny algorithm, which produces the edge map of the iris image in a similar manner to Keyless entry authentication system. Using Hough transforms, the detected edge map was leveraged to precisely locate the iris and pupil boundaries. Extracting the edge information of the eyelids was carried out using the horizontal segmentation operator and image binarization. The parabolic curves were used to model the eyelid boundaries based on the identified edge points. Daugman's rubber sheet model was then utilized to normalize the polar image of the iris, mapping it into the Cartesian frame as a rectangular strip. This homogenous model remaps each point within the iris region to a pair of polar coordinates (r, θ), where r ranges from 0 to 1 and θ ranges from 0 to 2π. The remapping process from (x, y) Cartesian coordinates to normalized polar coordinates is defined by Eqs. (1)–(3).

$$\mathrm{I}\left(x\left(r,\theta\right), y\left(r,\theta\right)\right) \rightarrow \mathrm{I}\left(r,\theta\right) \tag{1}$$

$$\mathrm{X}\left(r,\theta\right) = \left(1-r\right) x_i\left(\theta\right) + r \cdot x_0 + \cos\theta.\left(r_i + r \cdot \left(r_0 - r_i\right)\right) \tag{2}$$

$$\mathrm{Y}\left(r,\theta\right) = \left(1-r\right) y_i\left(\theta\right) + r \cdot y_0 + \sin\theta \cdot \left(r_i + r \cdot \left(r_0 - r_i\right)\right) \tag{3}$$

where $\mathrm{I}\left(x, y\right)$ represents iris region image, $\left(x, y\right)$ denotes the original Cartesian coordinates, $\left(r, \theta\right)$ represents the transformed polar coordinates obtained through normalization along the θ direction from the original Cartesian coordinates (x, y).

By mapping each point within the iris region to a pair of polar coordinates $\left(r, \theta\right)$ with the use of Daugman's rubber sheet model, inconsistencies in pupil dilation and size are taken into account to generate a normalized representation that has constant dimensions. When this is done, finally, histogram equalization will be used for image enhancement. Fig. 3 depicts the pre-processed images.

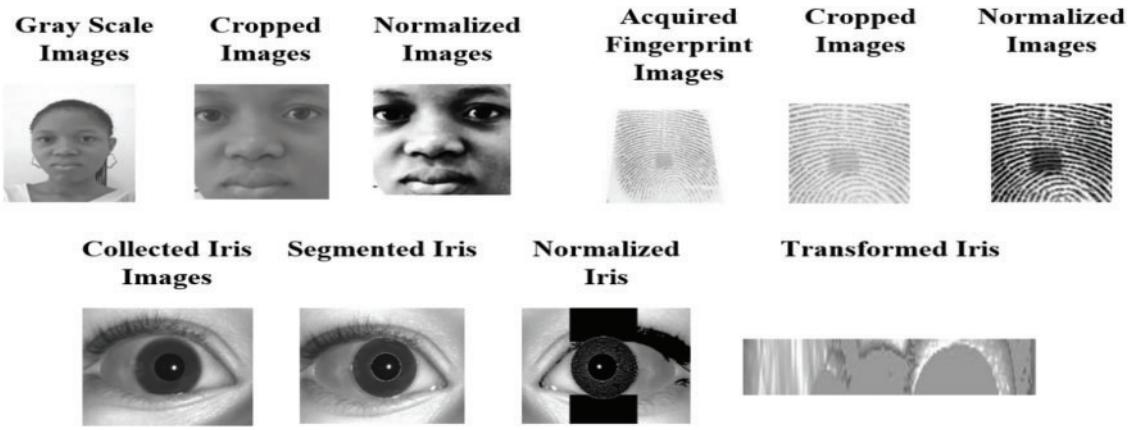

Figure 3: The pre-processed images

3.3 Feature Extraction Using Haar Wavelet-Based Technique

The Haar wavelet-based technique was applied to pre-processed face, iris, and fingerprint images to extract its features. The wavelet transform is a decomposition technique that produces many resolutions of an image, from the original's high-resolution version to lower-resolution approximations. In Fig. 4, the result of the multilevel 2-D wavelet decomposition can be observed, which is comprised of four sub-images. The detailed images for the horizontal, vertical, and diagonal orientations are represented by LH, HL, and HH, respectively, while the approximation image is represented by LL. Two-level decomposition was performed to reduce the image matrix size. The new image size on applying the technique was reduced to 1/4th the original. The maximum information of the image is contained in the approximation coefficient (LL), which is extracted until the final round of decomposition, following the same process as that used for the original image. The output of the Haar wavelet-based technique was converted to a feature vector to become input into the classification modules for all biometric systems considered in this study.

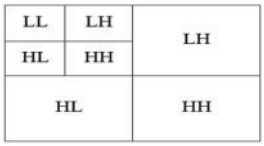

Figure 4: Haar wavelet decomposition

3.4 Cultural Chicken Swarm Optimization for Feature Selection

The Chicken Swarm Optimization technique is one of the most efficient intelligence optimization algorithms, as it solves complex optimization problems effectively. However, CSO typically suffers from poor convergence and accuracy when applied to problems with large dimensions due to the loss of diversity during solution space exploration. Introducing the cultural algorithm strategy involving the belief space, acceptance function, and influence function into the problem search space iteratively can increase the convergence and precision of the algorithm.

The cultural algorithm, through its operators, possesses a powerful global optimization ability, making it well-suited for high-dimensional data applications [25]. Integrating it with Chicken Swarm Optimization enhances the combined technique's exploration and exploitation capabilities [26]. This ensures robust feature

selection. This synergy effectively addresses challenges in multimodal biometric systems, such as diverse feature distributions and dimensionality, optimizing feature selection, and achieving superior classification accuracy for improved system performance. The integration of cultural algorithm operators with CSO enhances its optimization framework by utilizing its hierarchical structure. The belief space (Bs) is initialized as an empty set and dynamically updated using knowledge of optimal solutions derived from the hierarchical behaviors of roosters, hens, and chicks. The acceptance function evaluates and selects superior solutions influenced by roosters' leadership. The influence function guides hens and chicks to explore and exploit the search space more effectively. This framework ensures diversity preservation while optimizing feature selection for high-dimensional multimodal biometric systems, taking full advantage of CSO's hierarchical structure. The CCSO technique is described in detail.

Step 1: Initialization of the chicken swarm x_i and the related parameter $(N, Ir, G, R_N, H_N, C_N, M_N)$. Where N = total number of chickens, Ir = the maximum iterations, G = frequency of change of hierarchical order in the swarm, R_N = numbers of roosters, H_N = numbers of hens, C_N = numbers of chicks, and M_N = numbers of mothers, respectively.

Step 2: Creation of initial belief space: Belief space (B_s) was initially created as an empty set.

Step 3: Evaluate the fitness values of the chicken swarm x_i and initialize the personal best position p_{best} and the global best position g_{best}. Set $t = 1$.

Step 4: If t mod G is 1, sort the fitness values of the individuals within the chicken swarm, and establish the hierarchical structure of the chicken swarm; categorize the entire chicken swarm into multiple subgroups and clarify the link between the hens and the chicks.

Step 5: Update the positions of roosters, hens, and chicks and recalculate the fitness values, respectively: roosters, hens, and chicks update their positions according to (4)–(6), respectively.

$$x_{i,j}(t+1) = x_{i,j}(t) * \left(1 + Randn\left(0, \sigma^2\right)\right) \tag{4}$$

$$\sigma^2 = \begin{cases} 1 & if\ f_i < f_k \\ \exp\left(\dfrac{f_k - f_i}{|f_i| + \epsilon}\right) & otherwise, k \neq i \end{cases} \tag{5}$$

where $x_{i,j}(t+1)$ and $x_{i,j}(t)$ denote the new and old position of ith rooster in jth dimension, respectively; t refers to the iteration number; $Randn$ is the normal distribution with zero mean and σ^2 SD, f_i and f_k are the fitness value of rooster i and rooster k.

$$\begin{aligned} &x_{i,j}(t+1) = x_{i,j}(t) + s1 * Rand1 * \left(x_{r1,j}(t) - x_{i,j}(t)\right) + s2 * Rand2 * \left(x_{r2,j}(t) - x_{i,j}(t)\right) \\ &S1 = \exp\left(\frac{f_i - f_{r1}}{|f_i| + \epsilon}\right) \quad S2 = \exp\left(f_{r2} - f_i\right) \end{aligned} \tag{6}$$

where $x_{i,j}(t+1)$ and $x_{i,j}(t)$ denote the new and old position of ith hen in jth dimension, respectively; $r1$ should be the rooster of the same group, and $r2$ will be the randomly chosen rooster or hen from the entire chicken swarm such that $r1 \neq r2$; $Rand1$ and $Rand2$ will be a random number in the range $[0, 1]$.

$$x_{i,j}(t+1) = x_{i,j}(t) + FL * \left(x_{m,j}(t) - x_{i,j}(t)\right) \tag{7}$$

$x_{i,j}(t+1)$ and $x_{i,j}(t)$ denote the new and old position of ith chick in jth dimension, respectively; $x_{m,j}(t)$ is the position of the mother; FL refers to the random number in the range of $[0, 2]$.

Step 6: Apply the acceptance function and adjust the belief space B_s.

Eq. (8) determines the number of chickens that are used to adjust the belief space while Eq. (9) determines the interval of the belief space. The current best chicken was used to shape the belief space.

$$N_{accepted} = n\% \times N + \frac{n\%}{t} \times N \tag{8}$$

where $n\%$ is a parameter that is set by the user, N is the number of chickens, and t represents the th generation.

$$NB_s = \left[l_w, u_p\right] = \left\{x_i \middle| l_w \le p \le u_p, x \in 3i\right\} \tag{9}$$

where l_w is the lower bound on belief space (B_s) and u_p is the upper bound on belief space (B_s). l_w and u_p are determined using Eq. (10):

$$l_w = \begin{cases} x_i, & \text{if } x_i \le l_w \\ l_w, & \text{otherwise} \end{cases} \quad u_p = \begin{cases} x_{i,} & \text{if } x_i \ge u_p \\ u_p, & \text{otherwise} \end{cases} \tag{10}$$

Step 7: Adjust belief space using Eqs. (10) and (11).

Step 8: Apply the influence function to generate new chickens.

Based on the updated best chicken (x_i), l_w and u_p adjust the position of the chicken using an influence function (12) to change the direction of each chicken in solution space and to avoid being easily trapped at a local optimum.

$$x_i(t) = \begin{cases} x_i(t) + \left|\text{Rand}() \times \left(u_p - l_w\right)\right| & \text{if } x_i < l_w \\ x_i(t) - \left|\text{Rand}() \times \left(u_p - l_w\right)\right| & \text{if } x_i > u_p \end{cases} \tag{11}$$

Step 9: Update the individual's best fitness value (p_{best}) and the global best (g_{best}) solution: if the chicken's fitness value is better than the previous best one, the chicken's best fitness value or the global best solution will be updated using Eq. (12).

$$x_i(t) = \begin{cases} x_i(t-1), & f(x_i(t)) > f(x_i(t-1)), \\ x_i(t), & f(x_i(t)) \le f(x_i(t-1)). \end{cases} \tag{12}$$

Step 10: If the number of iteration times t is less than Ir, return to Step 4. Otherwise, terminate the algorithm and output the global best solution.

Step 11: Select the Optimal Parameter for the optimum solution

Select the best global position $x_i(t)$ of the Chicken.

The Selected best global position $x_i(t)$ of the chicken based on the feature subset mapped by $x_i(t)$ and model with the optimized parameter becomes the optimized features $F_i(t)$ as shown in Eq. (13).

$$F_i(t) = G_{Best}(x_i(t)) \tag{13}$$

3.5 Matching Phase

The matching module compares the optimized feature set with the stored templates using a matching algorithm to generate optimized matching scores. The matching score of the optimized feature was generated using Mahalanobis distance. The matching process involved comparing the extracted features with the pre-stored template in the database and generating matching scores as output. This is given in Eq. (14):

$$S_g(x, y)^2 = (x - y)' S^{-1} (x - y) \tag{14}$$

The vector with the minimum distance was selected as the most similar vector, where S represents the within-group covariance matrix.

3.6 Decision Module

The matching score of the optimized features was used to identify a user as either genuine or an impostor. The matching score S_c was compared to a pre-specified threshold (th). If $S_c > th$, then the user was identified to be genuine otherwise, be identified as an impostor. The decision function defined in Eq. (15) verified the identity of users.

$$Decision\ (S_c) = \begin{cases} Accept\ (Genuine), & if\ S_c > th \\ Reject\ (Impostor), & otherwise \end{cases} \tag{15}$$

3.7 Implementation

The research utilized MATLAB 9.4 (R2018a) on a Hewlett-Packard G56 system with an Intel® Core™ i5 Duo processor, Windows 10 Professional 64-bit OS, 2.7 GHz CPU, 6 GB RAM, and a 1 TB HDD. An interactive GUI application with real-time biometric datasets was designed using MATLAB's GUI toolbox. The simulation process for optimizing the biometric access control system with CCSO in MATLAB involved data collection (600 images), preprocessing, and dataset splitting (360 for training, 240 for testing). Parameters were initialized, and CCSO optimized the system, with performance evaluation conducted using various metrics, followed by parameter tuning and comparative analysis within the MATLAB environment.

3.8 Evaluation Measures

The performances of the investigated biometric systems were evaluated by calculating its FAR, FRR, sensitivity, precision and recognition accuracy. The evaluation based on performance metrics was achieved by employing confusion matrix. It contained True Positive (TP), False Positive (FP), False Negative (FN) and True Negative (TN). The performance of the system was measured as follows:

$$\text{FAR} = \frac{\text{FP}}{\text{FP} + \text{TN}} \tag{16}$$

$$\text{FRR} = \frac{\text{FN}}{\text{FN} + \text{TP}} \tag{17}$$

$$\text{Accuracy} = \frac{\text{TP} + \text{TN}}{\text{FP} + \text{FN} + \text{TP} + \text{TN}} \tag{18}$$

4 Results and Discussion

The analysis of the performance of the developed CCSO technique in comparison to the CSO technique is presented. The observations obtained from the techniques were thoroughly examined and discussed in detail in this section. The performance evaluation of the biometric techniques was carried out using face, fingerprint, and iris unimodal biometric data. The CSO technique is a parametric approach that heavily relies on its parameter settings. Specifically, the FL parameter in CSO plays a crucial role in determining its performance. To facilitate a fair comparison between the developed CCSO technique and the CSO technique, both approaches were evaluated using FL values of 0.4. This choice of FL was motivated by previous studies, including [27,28] which have shown that the range of FL $\in$ [0.4, 1] can produce satisfactory results for most optimization problems. Empirical evidence also supports the effectiveness of this FL value in practice. Table 1

presents the initial parameter settings for both the CSO and CCSO techniques. Initially, these parameters were configured to shape the performance of the proposed technique, impacting aspects such as solution quality, computational time, exploration, diversity, and leadership dynamics within the swarm [29].

Table 1: Initial parameters setting of CSO and CCSO technique

The maximum number of iterations	**100**
Number of populations	50
Interval Random number	0.04
Ratio of rooster	0.15
Ratio of hen	0.70
Ratio of hen with chick	0.50

The result is obtainable in Table 2 depicts the performance of the techniques based on face biometric traits at FL values of 0.2 and 0.4.

Table 2: Performance of techniques for face biometric

FL-Value	**Technique**	**FAR (%)**	**FRR (%)**	**Accuracy (%)**	**Time (s)**
0.2	CSO	43.33	10.56	81.25	93.43
	CCSO	33.33	6.67	86.67	64.61
0.4	CSO	31.67	12.22	82.92	92.57
	CCSO	16.67	7.22	90.42	62.13

Table 2 presents the evaluation results of the CSO and CCSO techniques for FAR, FRR, accuracy, and recognition time using face biometrics. Findings from the table indicate that the optimal level of performance was realized at an FL value of 0.4. The results show that at FL value 0.4, the CSO technique achieved a FAR of 31.67%, FRR of 12.22%, and accuracy of 82.92% at 92.57 s, while the CCSO technique achieved a FAR of 16.67%, FRR of 7.22%, and accuracy of 90.42% at 54.77 s. The results demonstrate that the CCSO technique outperformed the CSO technique in terms of FAR, FRR, recognition accuracy, and time, with an average recognition time of 0.228 s for the face biometric. The confusion matrices for the performance of CCSO and CSO techniques with face biometrics are depicted in Fig. 5a,b, respectively. These figures present actual classes as against the predicted classes.

The results in Fig. 5a reveal that the CCSO technique accurately identified 167 face datasets as genuine, but 13 datasets were wrongly identified as imposters. Interestingly, the technique also misclassified 10 imposter datasets as genuine but correctly identified 50 as imposters. Moving on to Fig. 5b, the CSO technique correctly classified 158 genuine face datasets but misclassified 35 as imposters. Moreover, the technique accurately identified 41 imposter datasets but wrongly classified 19 as genuine.

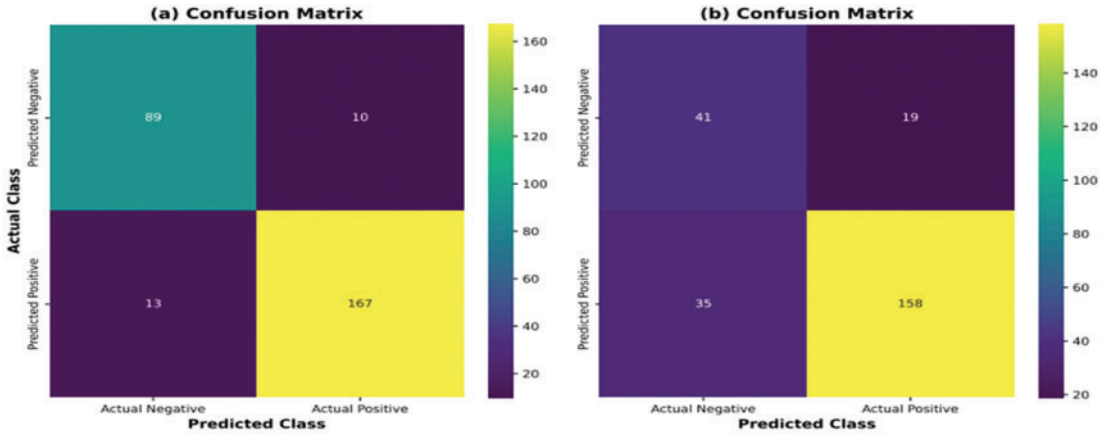

Figure 5: Performance of CCSO and CSO techniques with face

Table 3 illustrates the performance of the techniques using fingerprint biometric traits at FL values of 0.2 and 0.4. The results obtainable in Table 3 also revealed that at FL value 0.4 for the fingerprint biometric, the CSO technique achieved a FAR of 25.00%, FRR of 10.00%, and accuracy of 86.25% at 63.96 s, while the CCSO technique achieved a FAR of 23.33%, FRR of 3.33%, and accuracy of 91.67% at 27.35 s. The results demonstrate that the CCSO technique outperformed the CSO technique in terms of FAR, FRR, recognition accuracy, and time, with an average recognition time of 0.114 s for the fingerprint biometric. The confusion matrices for the performance of CCSO and CSO techniques with face biometrics are depicted in Fig. 6a,b, respectively.

Table 3: Performance of techniques for fingerprint biometric

FL-Value	Technique	FAR (%)	FRR (%)	Accuracy (%)	Time (s)
0.2	CSO	30.00	11.67	83.75	64.08
	CCSO	20.00	8.33	88.75	28.86
0.4	CSO	25.00	10.00	86.25	63.96
	CCSO	23.33	3.33	91.67	27.35

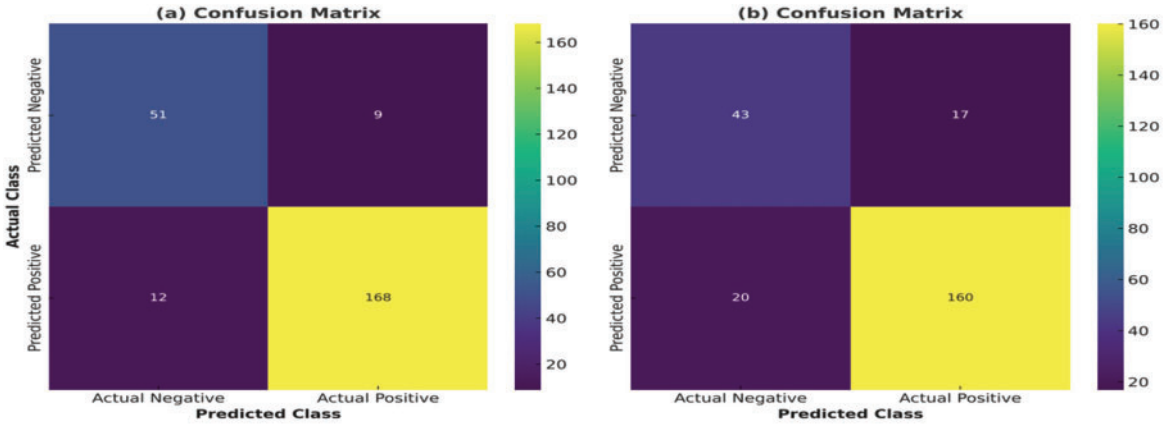

Figure 6: Performance of CCSO and CSO techniques with Fingerprint

According to the results shown in Fig. 6a, the CCSO technique accurately classified 174 face datasets as genuine, with only 6 misidentified as imposters. Notably, the method also correctly flagged 40 imposter datasets, while 14 were mistakenly categorized as genuine. In Fig. 6b, the CSO technique correctly identified 162 genuine datasets, but incorrectly classified 18 as imposters. Fig. 6a,b presents actual classes as against the predicted classes. Additionally, the CSO method accurately identified 45 imposter datasets, but erroneously classified 15 as genuine. Table 4 presents the results of the techniques' performance based on iris biometric traits at FL values of 0.2 and 0.4.

Table 4: Performance of techniques for iris biometric

FL-Value	Technique	FAR (%)	FRR (%)	Accuracy (%)	Time (s)
0.2	CSO	41.67	10.00	82.08	165.90
	CCSO	21.67	8.89	87.92	114.61
0.4	CSO	28.33	11.11	84.58	163.94
	CCSO	15.00	6.67	91.25	113.92

Table 3 illustrates that, at an FL value of 0.4, the CSO technique yielded a FAR of 28.33%, an FRR of 11.11%, and an accuracy of 84.58% in 163.94 s. In comparison, the CCSO method achieved better performance, with a FAR of 15.00%, FRR of 6.67%, and accuracy of 91.25% in only 113.92 s. The average recognition time for the iris biometric was 0.114 s, with the CCSO method surpassing the CSO technique in all aspects of performance, including recognition accuracy, FAR, FRR, and processing time. The outcomes are displayed in Fig. 7a revealed that the CCSO technique correctly identified 168 genuine face datasets and committed only 12 misidentifications. Impressively, the method accurately recognized 51 imposter datasets while only mistakenly classifying 9 as genuine. By contrast, Fig. 7b indicated that the CSO technique correctly classified 160 genuine datasets but erroneously flagged 20 as imposters. This presents actual classes as against the predicted classes. Moreover, the CSO method accurately identified 43 imposter datasets but wrongly classified 17 as genuine.

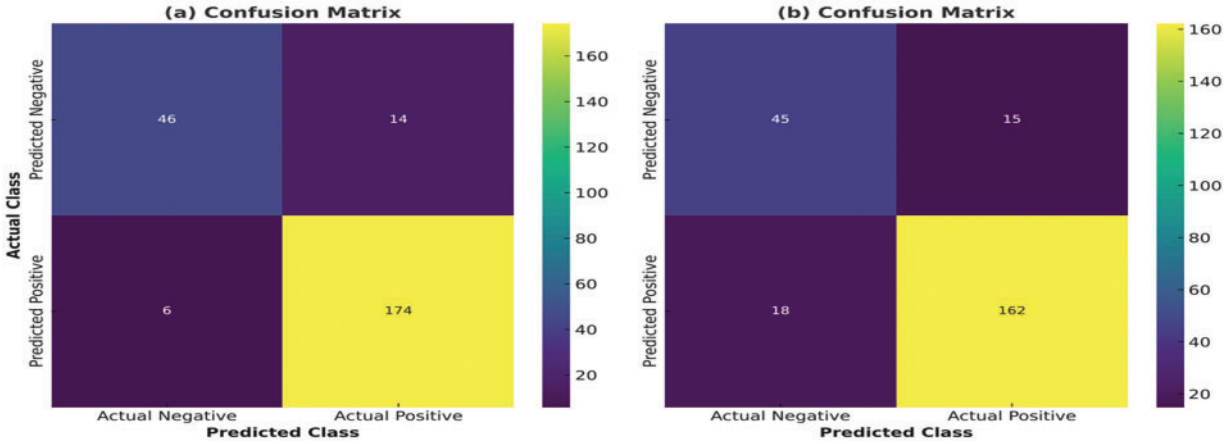

Figure 7: Performance of CCSO and CSO techniques with iris

In view of the performance with the unimodal biometrics, it was revealed that the CCSO technique achieved improved performance with less FAR, FRR, and recognition time and increased recognition

accuracy than the CSO technique. The CCSO technique demonstrated better accuracy in identifying genuine datasets compared to the CSO technique. However, both techniques had their limitations, with occasional misclassifications of genuine and imposter datasets. The choice between these techniques would depend on the specific requirements of the biometric access control system, balancing security and convenience factors. Further refinements and parameter adjustments might be necessary to improve the performance of these techniques in practice. In this study, the fingerprint biometric among others has the best performance while the face biometric has the least performance.

Face variation and the quality of some of the acquired facial images, such as blurriness, resolution, and noise, may account for the lowest performance of face biometrics when compared to other biometrics in this study. This is in line with the submission of [30,31]. Also, the iris biometric has the highest recognition time among others while the fingerprint biometric has the least recognition time. These findings can be attributed to the fact that iris recognition involves more complex processes which involves more computational resources and time. This is supported by [30,32]. The reduction in iris biometric performance may be attributed to the visible area of the iris region being affected by the eyelids and eyelashes [33]. Furthermore, the fingerprint biometric outperformed both face and iris biometric in time of accuracy and speed of recognition. Empirical evidence [34,35] suggested that fingerprint biometrics outperform both face and iris biometrics in terms of accuracy and speed of recognition, primarily due to the high degree of uniqueness, stability, and resolution of fingerprint patterns, and their robustness to various environmental and physiological factors.

The remarkable reduction in recognition time that the CCSO technique has achieved is primarily attributable to the ingenious incorporation of the cultural evolution strategy into the CSO technique. The computational complexity of CCSO arises from its hierarchical belief space and swarm-based optimization process. Its complexity is approximately O(N·T), where N is the population size and T is the number of iterations, consistent with other swarm intelligence algorithms [36]. This structure ensures efficiency and scalability for large datasets.

By skilfully improving the balance between the exploration and exploitation phases of the technique, this innovative approach has managed to accelerate the recognition process to unprecedented levels, as attested by [37]. The CCSO technique is exceptional because it artfully combines the fast convergence speed of the CSO technique [38] with the unmatched global optimizing ability that is enhanced by the introduction of cultural algorithm operators [25]. In an access control system, achieving a low FAR and FRR is crucial for maintaining high security while still providing a user-friendly experience. The introduction of the CCSO technique has demonstrated the potential to significantly reduce both FAR and FRR, resulting in an optimal Equal Error Rate (EER) that strikes the perfect balance between security and usability.

The effectiveness of the CCSO technique in reducing both FAR and FRR can be attributed to its powerful combination of exploration and exploitation capabilities, which allow it to optimize the search process in a dynamic and adaptive way. This not only improves the accuracy of the access control system but also enhances its overall efficiency, resulting in a more seamless and user-friendly experience for authorized users. The achievement of a suitable EER is paramount to ensuring that the access control system provides the highest degree of protection possible, while still maintaining a level of user-friendliness that does not hinder productivity. By leveraging the advanced optimization capabilities of the CCSO technique, organizations can ensure that their access control system strikes the perfect balance between security and usability, providing a robust and reliable security framework that is designed to meet the needs of today's fast-paced and ever-changing business environment.

Table 5 presents the result of inferential statistical analysis using paired sample *t*-tests between CCSO and CSO techniques based on accuracy, FAR, FRR, and computation time. The result revealed significant

differences across all metrics evaluated at a 95% confidence level ($p < 0.05$). The results show that CCSO significantly outperformed CSO in accuracy (mean difference = 5.98%, $t = 4.715$, $p = 0.005$), reduced FAR (−11.67%, $t = -3.378$, $p = 0.043$), FRR (−4.08%, $t = -4.029$, $p = 0.010$), and significantly less computation time (−38.73 s, $t = -9.721$, $p = 0.000$). The incorporation of cultural algorithm operators in the model of CSO is commensurate to the gain in accuracy and reduction of error rate and computation time achieved over CSO significantly. This validates the application of CCSO for feature optimization in biometric applications. The method was more computationally efficient and more accurate than CSO. This demonstrated that, when compared to other approaches, CCSO provides robust and scalable solutions to challenges associated with high-dimensional data effectively.

Table 5: *t*-test statistical comparison between CCSO and CSO techniques at 0.05 significance level

Techniques	Measures	Mean Difference	*t* Value	*p*-Value
CCSO vs. CSO	Accuracy	5.98	4.715	0.005
	FAR[a]	−11.67	−3.378	0.043
	FRR[b]	−4.08	−4.029	0.010
	C_Time[c]	−38.73	−9.721	0.000

Note: [a]: False Acceptance Rate; [b]: False Rejection Rate; [c]: Computation time.

The inclusion of cultural algorithm operators in the CSO technique has been substantiated by the demonstrably superior performance attained in this investigation. Analysis of the tables presented in this study unambiguously indicates that the CCSO technique consistently outperformed the CSO technique in terms of accuracy. The compelling results of this research offer compelling evidence that the incorporation of cultural algorithm operators in the CSO framework can greatly enhance its optimization capabilities. The systematic integration of cultural learning mechanisms with the CSO algorithm has engendered a dynamic synergy that optimizes the balance between exploration and exploitation, leading to improved optimization performance. The authors compared state-of-the-art reviews of the proposed method in similar studies. Table 6 depicts the comparison results of the developed technique with other state-of-the-art methods.

Table 6: Comparison with state-of-the-art methods

Ref	Method	Recognition performance
[19]	FFNNPSO	90.0%
[39]	HSA-ANN	94.0%
[15]	PCA-SVM	89.0%, 91.0%, and 87.0% for Face, Iris and Fingerprint.
[40]	PSO	93.0%
Proposed	**CCSO**	**90.42%, 91.67%, and 91.25% for Face, Fingerprint and Iris.**

Note: HSA-ANN attained the higher performance at 94.0%, while PSO demonstrated robust performance at 93.0%. PCA-SVM exhibited inconsistent performance across modalities, with the lowest score being 87.0% for Fingerprint. The proposed CCSO approach regularly surpasses PCA-SVM in all three modalities, demonstrating Face: 90.42% compared to 89.0%. Fingerprint: 91.67% compared to 87.0%, Iris: 91.25% compared to 91.0%.

The result presented in Table 5 reveals that the results achieved by the proposed CCSO are not only competitive but also well-matched with the accuracy levels achieved by established optimization techniques in previous studies. The implications of CCSO's competitive performance are significant. It underscores CCSO's potential to effectively enhance biometric access control systems, offering comparable accuracy to established techniques while potentially improving processing speed.

The CCSO technique directly addresses key research gaps in the need for scalable and efficient optimization methods for biometric systems [41]. Traditional swarm intelligence techniques like CSO are limited by slower convergence rates and higher computational costs, particularly in high-dimensional datasets. CCSO advances the state of the art by introducing cultural algorithm operators that enhance the optimization process through hierarchical belief spaces. These operators facilitate better exploration-exploitation balance, reducing false acceptance and rejection rates (FAR and FRR) while improving recognition accuracy and reducing computational time. The results demonstrate CCSO's effectiveness in optimizing unimodal biometric systems, with performance improvements over CSO across face, fingerprint, and iris biometrics. These advancements underscore CCSO's role in addressing scalability and efficiency gaps, positioning it as a superior alternative for real-time biometric system optimization. Cultural algorithm operators are central to optimizing CSO in the proposed CCSO framework. These operators are inspired by cultural evolution and utilize a hierarchical belief space to guide swarm behavior. In biometric applications, these components enable CCSO to adaptively refine feature selection and matching criteria. This adaptability improves the system's accuracy, reduces misclassification rates, and enhances computational efficiency. This suggests that CCSO can be a valuable addition to the toolkit of optimization methods for biometric systems, offering a promising avenue for enhancing security surveillance measures and operational efficiency in various domains.

5 Conclusions

The study shows that the CCSO technique is a promising optimization tool for the development of efficient and realistic biometric access control systems. The CCSO technique addresses the challenges of the CSO technique and offers superior accuracy and computational efficiency, making it an attractive option for biometric access control systems. The results achieved in this study emphasize the practical significance of CCSO in biometric recognition, offering not only improved accuracy but also faster processing times—a crucial factor in access control systems. The results suggest that CCSO could be instrumental in enhancing security surveillance measures across various domains where biometric access control systems are deployed. However, it is important to consider factors such as computational resources and scalability in implementing CCSO in larger-scale applications. Consequently, the adoption of the CCSO technique can significantly improve the security and efficiency of biometric access control systems, and its demonstrated effectiveness marks a promising advance in the evolution of optimization algorithms, inspiring further innovation in the field. The main contributions of this study are highlighted as follows:

- Integration of cultural algorithm operators into the CSO model for enhancing biometric access control.
- Emphasis on the importance of the cultural-based CSO technique for biometric access control, encompassing face, fingerprint, and iris traits.
- Validation of the cultural-based CSO against the conventional CSO technique for biometric access control, covering face, fingerprint, and iris traits.

These contributions address key research gaps by improving scalability and efficiency in high-dimensional biometric data through cultural algorithm integration. The study provides a unified framework for optimizing face, fingerprint, and iris traits while validating the cultural-based CSO's superior performance over the conventional model, showcasing enhanced accuracy, reduced error rates, and faster

processing for biometric access control systems. Future research should explore integrating CCSO with recent advancements in multi-modal learning to enhance biometric system performance, such as temporal biometric data fusion architectures inspired by TriChronoNet, hyper-relational interaction modeling for cross-modal feature correlation analysis, vision transformer approaches for multi-source biometric feature extraction, and mobile-optimized multimodal deep learning frameworks for real-time processing. Additionally, testing CCSO with larger datasets to evaluate scalability, enhancing security through multibiometric system optimization, and assessing operational efficiency across diverse deployment scenarios remain crucial research priorities.

Limitations and Future Works

The following are a few GSA's drawbacks for feature fusion in a multimodal biometric system:

Parameters sensitivity: Several GSA's parameters, including the gravitational constant, population size, and iterations, need to be fine-tuned. Finding the ideal collection of parameters might be difficult because the performance of GSA can be sensitive to them. Limited exploration: GSA may not adequately explore the search space, which can result in less-than-ideal solutions. This constraint can be particularly problematic in multimodal biometric systems if the feature spaces of the various modalities are intricately intertwined and complex. A future study can also examine CCSO's resilience to adversarial assaults, hardware acceleration to speed up processing, and algorithmic improvements to boost performance and convergence. New algorithms such as the Farmland fertility algorithm, Mountain Gazelle Optimize, African Vultures Optimization Algorithm, and Artificial Gorilla Troops Optimizer may also be considered in the future. Finally, evaluating user experience, energy efficiency, and prospective uses beyond access control, such as in healthcare or finance, may offer additional CCSO security and operational efficiency prospects.

Acknowledgement: The authors acknowledge the support received from the Computer Engineering Department, Ladoke Akintola University of Technology, Ogbomoso, Nigeria and the Computer Science Department, University of Zululand, South Africa on this project.

Funding Statement: The authors received no fund for the project, but the project is supported by Ladoke Akintola University of Technology, Ogbomoso, Nigeria and the University of Zululand, South Africa.

Author Contributions: The authors confirm contribution to the paper as follows: Conceptualization, methodology writing—original draft, and data curation: Jonathan Ponmile Oguntoye, Elijah Olusayo Omidiora; Project administration, methodology and validation, writing—original draft, data curation: Jonathan Ponmile Oguntoye, Sunday Adeola Ajagbe, Oluyinka Titilayo Adedeji, Abigail Bola Adetunji; Software, visualization, and methodology: Olufemi Olayanju Awodoye, Jonathan Ponmile Oguntoye, Oluyinka Titilayo Adedeji, Sunday Adeola Ajagbe; Project administration, resources, review, editing and supervision: Elijah Olusayo Omidiora, Matthew Olusegun Adigun. All authors reviewed the results and approved the final version of the manuscript.

Availability of Data and Materials: Not applicable.

Ethics Approval: Ethical approval was obtained from LAUTECH Ethics Review Committee in a letter dated 23 March, 2023 for the collection and analysis of face, fingerprint, and iris biometrics. This was approved with a reference number LAUERC/PG/2023/94. All data were anonymized, securely stored, and collected with informed consent, ensuring participant privacy and compliance with ethical standards.

Conflicts of Interest: The authors declare no conflicts of interest to report regarding the present study.

References

1. Nelson J. Access control and biometrics. Chapter 21—Access control and biometrics. In: Fennelly LJ, editor. Handbook of loss prevention and crime prevention. 6th ed. Oxford, UK: Butterworth-Heinemann; 2020. p. 239–49. doi:10.1016/b978-0-12-817273-5.00021-1.
2. Pan H, Tong S, Wei X, Teng B. Fatigue state recognition system for miners based on a multi-modal feature extraction and fusion framework. IEEE Trans Cogn Dev Syst. 2024;17(2):410–20. doi:10.1109/TCDS.2024.3461713.
3. Rajasekar V, Predić B, Saračević M, Elhoseny M, Karabasevic D, Stanujkic D, et al. Enhanced multimodal biometric recognition approach for smart cities based on an optimized fuzzy genetic algorithm. Sci Rep. 2022;12(1):622. doi:10.1038/s41598-021-04652-3.
4. Zokaee S, Faez K. Human identification based on ECG and palmprint. Int J Electr Comput Eng. 2012;2(2):261–6. doi:10.11591/ijece.v2i2.292.
5. El_Rahman SA. Multimodal biometric systems based on different fusion levels of ECG and fingerprint using different classifiers. Soft Comput. 2020;24(16):12599–632. doi:10.1007/s00500-020-04700-6.
6. Sabhanayagam T, Venkatesan VP, Senthamaraikannan K. A comprehensive survey on various biometric systems. Int J Appl Eng Res. 2018;13(5):2276–97.
7. Dargan S, Kumar M. A comprehensive survey on the biometric recognition systems based on physiological and behavioral modalities. Expert Syst Appl. 2020;143(c):113114. doi:10.1016/j.eswa.2019.113114.
8. Das A, Degeling M, Wang X, Wang J, Sadeh N, Satyanarayanan M. Assisting users in a world full of cameras: a privacy-aware infrastructure for computer vision applications. In: Proceedings of the 2017 IEEE Conference on Computer Vision and Pattern Recognition Workshops (CVPRW); 2017 Jul 21–26; Honolulu, HI, USA.
9. Wang Y, Tian Y, Zhu J, She H, Jiang Y, Jiang Z, et al. A hand gesture recognition strategy based on virtual-dimension increase of EMG. Cyborg Bionic Syst. 2024;5(4):0066. doi:10.34133/cbsystems.0066.
10. Soleymani S, Dabouei A, Taherkhani F, Iranmanesh SM, Dawson J, Nasrabadi NM. Quality-aware multimodal biometric recognition. IEEE Trans Biom Behav Identity Sci. 2021;4(1):97–116. doi:10.1109/tbiom.2021.3131664.
11. Mohsin AH, Zaidan AA, Zaidan BB, Albahri AS, Albahri OS, Alsalem MA, et al. Real-time remote health monitoring systems using body sensor information and finger vein biometric verification: a multi-layer systematic review. J Med Syst. 2018;42(12):1–36. doi:10.1007/s10916-018-1104-5.
12. Adetunji AB, Oguntoye JP, Fenwa OD, Omidiora EO. Reducing the computational cost of SVM in face recognition application using hybrid cultural algorithm. IOSR J Comput Eng. 2018;20(2):76–85. doi:10.9790/0661-2002047685.
13. Babatunde RS, Olabiyisi SO, Omidiora EO, Ganiyu RA. Local binary pattern and ant colony optimization-based feature dimensionality reduction technique for face recognition systems. Br J Math Comput Sci. 2015;11(5):1–14. doi:10.9734/bjmcs/2015/19490.
14. Yin X, Zhu Y, Hu J. Contactless fingerprint recognition based on global minutia topology and loose genetic algorithm. IEEE Trans Inf Forensics Secur. 2019;15:28–41. doi:10.1109/tifs.2019.2918083.
15. Adedeji OT, Alade OM, Oguntoye JP. Comparative analysis of feature selection techniques for fingerprint recognition based on artificial bee colony and teaching learning based optimization. LAUTECH J Comput Inform. 2021;2(1):25–34.
16. Oguntoye JP, Awodoye OO, Oladunjoye JA, Faluyi BI, Ajagbe SA, Omidiora EO. Predicting COVID-19 from chest X-Ray images using optimized convolution neural network. LAUTECH J Eng Technol. 2023;17(2):28–39.
17. Ahmed A, Hassanien AE, Bhattacharyya. A novel chaotic chicken swarm optimization algorithm for feature selection. In: Proceedings of the 2017 Third International Conference on Research in Computational Intelligence and Communication Networks (ICRCICN); 2017 Nov 3–5; Kolkata, India.
18. Abolarinwa MO, Asaju-Gbolagade AW, Adigun AA, Gbolagade KA. A proposed framework for optimum feature selection using improved chicken swarm optimization algorithm for face recognition system. Univ Ib J Sci Log ICT Res. 2022;8(1):12–8. doi:10.36108/ujees/2202.40.0260.
19. Rizk MR, Farag HH, Said LA. Neural network classification for iris recognition using both particle swarm optimization and gravitational search algorithm. In: Proceedings of the 2016 World Symposium on Computer Applications & Research (WSCAR); 2016 Mar 12–14; Cairo, Egypt.

20. Olayiwola DS, Olayiwola AA, Oguntoye JP, Awodoye OO, Ganiyu RA, Omidiora EO. Development of a fingerprint verification and identification system using a gravitational search algorithm-optimized deep convolutional neural network. Adeleke Univ J Eng Technol. 2023;6(2):296–307. doi:10.4314/fuoyejet.v9i1.10.
21. Verma S, Sahu SP, Sahu TP. Two-stage hybrid feature selection approach using levy's flight-based chicken swarm optimization for stock market forecasting. Comput Econ. 2024;63(6):2193–224. doi:10.1007/s10614-023-10400-8.
22. Hafez AI, Zawbaa HM, Emary E, Mahmoud HA, Hassanien AE. An innovative approach for feature selection based on chicken swarm optimization. In: Proceedings of the 7th International Conference of Soft Computing and Pattern Recognition (SoCPaR); 2015 Nov 13–15; Fukuoka, Japan.
23. Wang H, Chen Z, Liu G. An improved chicken swarm optimization algorithm for feature selection. In: Proceedings of the International Conference on Wireless Communications, Networking and Applications (WCNA 2021); 2021 Dec 17–19; Berlin, Germany. doi:10.1007/978-981-19-2456-9_19.
24. Kumari N, Dwivedi RK, Bhatt AK, Belwal R. Automated fruit grading using optimal feature selection and hybrid classification by self-adaptive chicken swarm optimization: grading of mango. Neural Comput Appl. 2022;34(2):1285–306. doi:10.1007/s00521-021-06473-x.
25. Kuo HC, Lin CH. Cultural evolution algorithm for global optimizations and its applications. J Appl Res Technol. 2013;11(4):510–22. doi:10.1016/S1665-6423(13)71558-X.
26. Wei GU. An improved whale optimization algorithm with cultural mechanism for high-dimensional global optimization problems. In: Proceedings of the 2020 IEEE International Conference on Information Technology, Big Data and Artificial Intelligence (ICIBA); 2020 Nov 6–8; Chongqing, China.
27. Meng X, Liu Y, Gao X, Zhang H. A new bio-inspired algorithm: chicken swarm optimization. In: Proceedings of the International Conference in Swarm Intelligence; 2014 Oct 17–20; Hefei, China.
28. Deb S, Gao XZ, Tammi K, Kalita K, Mahanta P. A new teaching-learning-based chicken swarm optimization algorithm. Soft Comput. 2020;24(7):5313–31. doi:10.1007/s00500-019-04280-0.
29. Phan HD, Ellis K, Barca JC, Dorin A. A survey of dynamic parameter setting methods for nature-inspired swarm intelligence algorithms. Neural Comput Appl. 2020;32(2):567–88. doi:10.1007/s00521-019-04229-2.
30. Jain AK, Ross A, Pankanti S. Biometrics: a tool for information security. IEEE Trans Inf Forensics Secur. 2006;1(2):125–43. doi:10.1109/tifs.2006.873653.
31. Klare BF, Burge MJ, Klontz JC, Bruegge RW, Jain AK. Face recognition performance: role of demographic information. IEEE Trans Inf Forensics Secur. 2012;7(6):1789–801. doi:10.1109/tifs.2012.2214212.
32. De Marsico M, Galdi C, Nappi M, Riccio D. Firme: face and iris recognition for mobile engagement. Image Vis Comput. 2014;32(12):1161–72. doi:10.1016/j.imavis.2013.12.014.
33. Thiyaneswaran B, Padma S. Iris recognition using left and right iris feature of the human eye for biometric security system. Int J Comput Appl. 2012;50(12):37–41.
34. Tong Y, Wheeler FW, Liu X. Improving biometric identification through quality-based face and fingerprint biometric fusion. In: Proceedings of the 2010 IEEE Computer Society Conference on Computer Vision and Pattern Recognition-Workshops; 2010 Jun 13–18; San Francisco, CA, USA.
35. Yadav AK. Deep learning approach for multimodal biometric recognition system based on fusion of iris, fingerprint and hand written signature traits. Turk J Comput Math Educ. 2021;12(11):1627–40. doi:10.17762/turcomat.v12i11.6098.
36. Heidari AA, Mirjalili S, Faris H, Aljarah I, Mafarja M, Chen H. Harris hawks optimization: algorithm and applications. Future Gener Comput Syst. 2019;97:849–72. doi:10.1016/j.future.2019.02.028.
37. Makas H, Yumuşak N. Balancing exploration and exploitation by using sequential execution cooperation between artificial bee colony and migrating birds optimization algorithms. Turk J Electr Eng Comput Sci. 2016;24(6):4935–56.
38. Liu Y, Liu Q, Tang Z. A discrete chicken swarm optimization for travelling salesman problem. In: Proceedings of the Fourth International Conference on Physics, Mathematics and Statistics (ICPMS); 2021 May 19–2; Kunming, China.

39. Hussein MM, Mutlag AH, Shareef H. An improved artificial neural network design for face recognition utilizing harmony search algorithm. In: Proceedings of the IOP Conference Series: Materials Science and Engineering; 2020 Dec 16–17; Baghdad, Iraq.
40. Zhang Y, Yan L. Face recognition algorithm based on particle swarm optimization and image feature compensation. SoftwareX. 2023;22(9):101305. doi:10.1016/j.softx.2023.101305.
41. Rostami M, Berahmand KN. Review of swarm intelligence-based feature selection methods. Eng Appl Artif Intell. 2021;100(1):104210. doi:10.1016/j.engappai.2021.104210.