Multi-modal biometric fusion based continuous user authentication for E-proctoring using hybrid LCNN-Salp swarm optimization

Himanshu Purohit1 · Pawan K. Ajmera1

Received: 21 June 2021 / Revised: 25 September 2021 / Accepted: 10 October 2021 / Published online: 10 November 2021
© The Author(s), under exclusive licence to Springer Science+Business Media, LLC, part of Springer Nature 2021

Abstract
In Covid 19, pandemic remote proctoring of the employee or human being is evolved as a big challenge for the information retrieval process. On the other side, memory-based system access authentication is becoming outdated and less preferred for live applications, especially where data security and customer privacy are crucial. Multi-modal authentication has outperformed the unimodal process with high accuracy and improved security in the user authentication field. Multi-modal biometric verification includes user attributes such as keystrokes, iris, speech, face, etc. For real-time execution of multi-modal biometric fusion-based live tracking for compatible applications. The study proposes an efficient continuous biometric user authentication system for a new challenge of pandemic time, a live online authentication of the evaluation process (CBUA-OE). The proposed CBUA-OE system can address the challenges associated with live proctoring and is also compatible with real-time implementation, deployment of authentication systems. The modified wolf optimization algorithm and CUBA-OE’s optimal feature fusion algorithm give an edge over the other contemporary methods and make it more robust. In modern forms of authentication, the classification stage affects the overall outcome of the system, and the model’s performance is also a factor of varying quality of datasets. In contrast, a hybrid LCNN-Salp swarm optimization-based classifier is more efficient and consistent in continuous user authentication. Here the performance of the proposed hybrid LCNN-Salp swarm optimization classifier is analyzed with different standard datasets. The results are compared with the existing state-of-art classifiers regarding the accuracy, precision, recall, and F-measure. This projected work is novel in terms of usability factors and scalability to live tracking systems.

Keywords Biometric system · Modified wolf optimization · Optimal feature fusion · LCNN

1 Introduction

Client confirmation depends on “something the client knows” for many years [1]. This strategy is exceptionally famous in personality validation, yet research has demonstrated that PINs and passwords don’t offer adequate insurance. A validated record and secret key are needed when you sign in to the standard login framework. Nevertheless, beneath this validation system, the mechanism can just distinguish the client from the login data. It is obscure who is utilizing the framework [2]. One disadvantage of the personal computer (PC) validation framework is that when a client leaves a space at short stretches, others can sign into the PC and access a particular archive or demonstrate that they are approved clients to reestablish data. Nobody realizes who utilized the PC after that. Such security weaknesses are not satisfactory in specific applications containing delicate information, such as bank monetary records or individual client data, military, industry, and exchange protection [3, 4]. Clients can physically bolt the screen before leaving or reappearing the terminal to forestall this harm under typical login conditions. That causes many issues for the client, particularly when the client is occupied with doing different things. Clients may sometimes skip the log-off cycle to try not to rehash the log-off and re-login measure. So, the data assurance is no more there. Nonetheless, these terms don’t exist in the uninvolved persistent verification framework [5].
Biometrics is the way toward recognizing an individual dependent on their physical or social guidelines. Actual ascribes incorporate facial, unique mark, iris, and hand calculation, while biometric designs incorporate voice, mark, keystroke, and walk. Biometric validation has numerous points of interest over conventional verification techniques [6]. Replicating biometric properties is hard to share and appropriate dependably and is considered exceptionally secure along these lines. Be that as it may, for current biometric frameworks, psychological information can cause commotion and changes in gleaming levels [7]. In expansion, the exactness of these biometric frameworks is influenced by enormous intra-class contrasts, uniqueness, and non-all-inclusiveness [8]. Actual biometrics needs sumptuous equipment to be reliable and vivacious against falsification assaults, accordingly expanding the expense of the gadget.

At last, a great deal of these biometric frameworks needs active client participation, which aggravates the clients [9]. Biometrics-based unmistakable confirmation and approval (BIA) systems save the customer’s reference biometric templates (BT), for instance, finger impression and iris codes in the backend. If the backend is entered, it will allow the spillage of customer’s private data, allowing competitors to use their custom characters and evade BIA settings [10, 11]. For example, in 2015, the working environment of personnel the board showed up at a compromise that delivered 5.6 million fingerprints of government personnel searching for confirmed status in the United States. Secure sections or encryption are used to guarantee BTs in customary fragments. Security factors apply to various biometrics, yet not too gigantic degree biometrics [12]. The encryption BT raises the going with troubles: (a) the BTs should be unscrambled to facilitate with the affirmation of the as of late given biometrics readings, (b) the translating keys related with the mixed designs ought to be taken care of some spot close (reasonably and really), and (c) encrypted configurations may be split if the backend is entered. Since BTs require lifetime upkeep, it is essential to pick structures and frameworks that are okay for a significant long an ideal opportunity (for instance, 40–50 years), which can be outstandingly irksome [13].

Despite the choice to complete the test with a mystery word, security components should be viewed when offering web tests. It isn’t absurd to acknowledge that one understudy can purposely give their mystery key to another, considering that the other individual will take the appraisal for the understudy. An evaluation system should be set up to choose if an understudy is enlisted for the assessment. Regardless of how there is no 100% affirmation that an understudy will create the test, there are ways to deal with assessing that it is so careful to say who is forming the test [14]. One way to achieve this is with a biometric structure that controls the components of keystroke of the up-and-comer appearing for the appraisal. The characteristics of keystroke components are assorted for each individual and are considered solely and aggregate. By assessing flight time or the advancement time from one "key" to another event, the customer can make a profile by forming a “signature”. By differentiating the components of pressing this key analyzer button, we can choose if the customer is enlisted [15, 16].

The front-most favourable position of the online test is that far away up-comers can do it, the appraisal of the suitable reactions is completely mechanized in the multiple-choice question (MCQ question), and other article type question can be surveyed actually or thus, dependent upon the nature and necessities of the requests. Additionally, online tests can be taken at whatever point, while the nonattendance of test undertakings doesn’t occur in standard test conditions, duplication, and course of action. The cost of online tests is particularly less stood out from normal test conditions [17]. In web learning, experimentation is gotten together with educating and learning segments. Under online tests, there is no quick contact with understudies, instructors, or chiefs, so prosperity is critical in a web learning environment. The possibility of the online learning environment will shield them from various security perils. Online tests, an essential piece of the learning environment, are extraordinarily participatory, provoking character changes and more dangerous attacks [18]. One of the critical targets of understudy affirmation is to ensure certifiable participation with solitary understudy during the online appraisal. A customer ID and a considerable mystery word are insufficient to check an understudy’s character on the web. Online decisions and the online security cycle can help you with murdering coercion. We use biometrics to help the decency of security control, approval, and online assurance measure. Under-study e-perception uses fingerprints and cameras to thwart cheating and misleading with [19, 20]. The main objectives of the proposed technique are given as follows:

- To design and analyze a technique to authenticate E-examinations continuously and transparently.
- To design an optimal biometric system for examiner authentication.
• To analyze the reliability of the biometric system through different test vectors.
• To propose a hybrid optimization technique to enhance the security in online examination platforms.

The rest of this paper is planned as follows: Sect. 2 portrays the previous techniques used for biometric authentication systems. In Sect. 3, problem methodology and system model were present. In segment 4, the researchers provide a formal explanation of the proposed approach. Test systems and results are given in Sect. 5. We conclude in Sect. 6 with a description of the various challenges and open issues requiring further investigation to implement this approach entirely.

2 Related works

Peng et al. [21] proposed wear glasses with a steady negative solidified Glass Guard. Glass Guard isolates the owner and an impostor with social biometrics from six sorts of touch movements and voice orders that are generally open customary customer joint efforts. Using data accumulated from 32 Google Glass customers, after 3.5 customer events, Glass guard has a 99% ID rate and 0.5% counterfeit alarm speed, with a typical of 3.5 customer events and all customer events. As demonstrated by the program’s five ordinary circumstances, the system area rate is over 93%, and the counterfeit alert rate is below 3% after five customer events.

Ali et al. [22] have presented research on keystroke biometrics (KB), and reviews of keystroke biometric structures can be used as an early phase for newcomers to the field. Furthermore, a couple of references are delivered from time to time, differentiating them subject to different procedures and strategies used in other examinations. It fills in as a wellspring of viewpoints for various examiners to evaluate their work to choose the orientation of future investigation. Reassure biometric systems are unrecognizable, interestingly with multiple zones, and basically, no analysis has been done on them stood out from other biometric structures. But generally, less exact than other biometric procedures, KB offers various central focuses: simplicity, straightforwardness, and mischief to the customer.

Ullah et al. [23] have investigated the approval of understudies with text-based and picture-based troubles. Their assessment showed that 70 online individuals from nine countries had completed a five-week online route and were standing up to the peril of mercilessness. (i) Excellent review prompts a development in substance requesting (p < 0.01), (ii) another doable facts section strategy than text requests (p < 0.01). Reenactme Abuse diversion is used to gauge the impact of database bundles at different levels. Security examination subject to the abuse condition conferred responses to outcast allies, database size, and affirmation in the response cycle all add to the achievement of the deception attack. This way, to help some inadmissible individuals, it is imperative to introduce such an examination that reduces the sharing of confirmations by understudies.

Ullah et al. [24] aimed to brace understudy’s characters with dynamic profile questions. In five weeks, 31 online individuals from five countries checked out the examination. The delayed consequences of their usage and security examination were dissipated. Dynamic profile necessities are more capable than text and picture-based essentials (p < 0.01). Fake individual abuse is reflected in messages and telephones. Regardless, the email deception attack was not successful, and understudies had the choice to respond persistently using an outcast test situation, achieving a 93% correct answer in the online test. Phone information and pester response time are astounding from understudy time (p < 0.01).

Prakash [25] proposed a continuous authentication (CA) system that consistently screens the customer before marking the PC. The CA system shields intruders from starting the structure. It dormany yields the form without interrupting the customer task measure. Here, the score-level mixing gel is proposed for mass improvement measure and torpid glass fire-based ID measure. The essential goal of their specific method is to join customer biometric incorporates and achieve the best-delayed consequences of steady customer confirmation. Their clear advancement involves four modules: the getting ready module, the workmanship extraction module, the aggregation module, and the approval module. Finally, a specific affiliation technique is used for far-away biometric affirmation.

Yang et al. [26] proposed Carry on Sense, an exact and compelling consistent confirmation framework for security deliberate portable applications utilizing contact conduct biometrics. By considering the elements of four unique sensors, they make a restrictive model using one-class SVM (OCSVM) and disengagement woodland (iForest) and figure the precision of each sort utilizing this model. Afterwards, they determined each kind of certainty level using the Bayesian hypothesis. They accomplished the exactness of the sensor work range through a creative
anticipated framework. They directed a few tests to affirm the viability of the proposed strategy. Their test outcomes show that a specific technique can successfully decide a client’s character.

Nunes et al. [27] developed SNUSE, a multi-customer secure system approach to manage re-enlisting on BIA structures. They train SNUSE to reflect its inactive limit and evaluate its sufficiency and precision using two biometric methodologies, one-of-a-kind imprint and iris separating. The biometric thought of the SNUSE key doesn’t impact the precision of the extraction program, and their test results are indicated each second by a supportive module using standard PC labourers. Executing their model achieves acknowledgement accuracy of more than 90% Genuine Acceptance Rate (GAR) and fewer than 5% False Acceptance Rate (FAR).

Neha et al. [28] proposed a lead biometric count program-level security for customer affirmation. Regardless, they drove risk assessments for various exercises. The keystroke ensures complete security and sets the standard multimode modes close to the beginning of the natural gathering. An appraisal of their proposed affirmation instrument has been seemed dependent on fake affirmation rate of false acceptance rate (FAR), fake excusal rate or false rejection rate (FRR), and comparable slip-up rate or equal error rate (EER). The standing multi-particular check achieved an FRR of 1.2%, FAR of 0.89%, and EER of 1.04% with J48 course of action computation. Even though the tireless keystroke confirmation has been analyzed when (no. of keystrokes pressed) full to get an interloper.

Wang et al. [29] represented BodyPIN, an unending customer confirmation system that fathoms far-off correspondences using Wi-Fi things. In the wake of examining the system work, the structure can follow the character of the current customer. If the check crashes and burns, induction to system security will now be set up. Since the customer describes different ascribes from customer to customer, it is hard to use the latest Rich Wireless User ID direct on the BodyPIN. The system interferes with the customer’s activities, which is uncommonly problematic and gravely orchestrated. In this examination, the makers developed a BodyPIN of a bioelectromagnetic field to evaluate the effect of two pi-Wi-Fi signals on the BodyPIN and to get a customer choosing component. They dispose of the connected Wi-Fi signal features to allow the customer to perceive the identifiers subject to the related login plan. There are accurate models with Wi-Fi NICs things without extra or submitted far-off hardware. As shown by various conventional limits, the construction has been exhibited to achieve lightweight, overwhelming and trustworthy approval work.

Kiyani et al. [30] have proposed keystroke components: a predictable customer affirmation system with lead biometric structures. Every limit offers another technique for recognizing the customer, which chooses the credibility of the current customer subject to the authentic thought of every limit. The makers developed a two-stage system with alerts and end limits using the novel study of two-passage bundle learning and the constant uncertainty model (R-RCM). Their specific computation masterminds each activity subject to the board’s fire glass capacity, which uses R-RCM hyper-limits to assess the certified trustworthiness of the customer’s genuine lead. The system chooses if the customer can use the structure based on assessing the new trust and the endpoint.

3 Problem methodology

We proposed a fitting practical adjustment and grouping calculation to recognize facial pictures utilizing diverse informational indexes in past work. Energetic and LTP capacities are being used to extricate capacities from denoised facial images. Firefly’s high-level streamlining calculation is used to choose ideal picture vectors. By selecting the ideal highlights from the chosen highlights, you will get a bunch of extraordinary highlights. These ideal properties are depicted utilizing the profound conviction organization (DBN) classifier. The DBN classifier accomplished 98.92% exactness in the ORL data set, 97.92% precision in the essential data set, and 98.12% exactness in the FOSEG data set.

As a rule, the primary test in web-based learning is the trouble in guaranteeing the believability of distance inspectors in taking on the web tests. Nonetheless, in numerous nations, the decision of online motivation is restricted. Furthermore, limitless validation is significant for some online applications that need to follow a client’s personality all through a meeting, not just toward the start of the session [21–25]. Such a persistent ID can be accomplished utilizing any biometric test; Traditional client accreditations, such as username and secret phrase check, approve “login” confirmation techniques [23]. Online sampling methods can lead to cyber-attacks, leading to unauthorized access to DoS or sensitive information. To prevent such attacks and avoid the risk of a fake person, we used intelligent techniques of continuous detection. We offer an effective continuous biometric user authentication system for online tests (CBUA-OE) for further improvement. The main contributions of the proposed CBUA-OE technique are as follows:

- First, we extract different soft and spectral-domain biometric features such as mouse, touch, and keystroke from the real-time data set. We introduced a modified wolf optimization (MWO) algorithm to compute
matching score values with the help of different soft biometric weights.

- Second, we illustrate an optimal feature fusion (OFF) algorithm to fuse optimal weight features of multiple biometric responses.
- Then, a hybrid LCNN-Salp swarm optimization-based classifier used for continuous user authentication classifies examiners’ presence and interaction.

3.1 System model of CBUA-OE technique

We used a specific method for generating tester contacts/contacts from biometric data statistics in this segment. Figure 1 shows the process of the planned procedure. User verification is a significant safety confront in an online exam environment. Login is complicated because it is impossible to identify users in an online test visually. In this method, feature extraction is used to calculate the value of the usable point using different soft biometric weights using the MWO method. Several issues need to be considered to create an effective biometric authentication system, especially the acquisition and classification of features. During taxonomy, individual biometric data are converted into the highest vectors of nature. The proposed biometric authentication scheme consists of five stages: data collection, data denomination, feature extraction, optimization, and classification.

4 Continuous biometric user authentication system for online examinations (CBUA-OE)

4.1 Optimal feature extraction using the modified wolf optimization algorithm

This section discusses the modified wolf optimization (MWO) algorithm employed for the optimal selection of feature sets. Here, the initial sets of features are fixed randomly. The best set of features can be found by reducing the range and position of the sensitive spot. The modified wolf optimization algorithm is designed by combining two new optimization methods, the Weil optimization algorithm and the Gray Wolf optimization algorithm.

4.1.1 Objective function

Here, the modified wolf optimization algorithm is employed to pick the finest relay set required for the
continuous packet transmission by all other sensor nodes in the network. Here, the objective function of the proposed optimization problem is to select the maximum number of paths with the minimal number of relay nodes. So the position of relay nodes is varied and checked for optimal deployment to reduce the number of relay nodes needed to be deployed. Therefore, the objective function is given as follows,

$$
\text{max}(L) = \min \left( B_R(n), \sum_{j=1}^{A} S_R^j(n) \right)
$$

where $L$ is the maximum length between sensor nodes required for perfect transmission without loss and minimum cost, $B_R(n)$ represent the number of data nearby to the base station; $S_R^j(n)$ number of data close to the sensor nodes $A^j$, and $j = 1, 2, \ldots, A$ denotes the number of sensor nodes. To achieve the above objective, the following conditions must be satisfied.

$$
S_R^j(n) \geq L^j
$$

$$
B_R(n) \geq \sum_{j=1}^{A} S_R^j(n) \geq \sum_{j=1}^{A} L^j
$$

The set of relay nodes (i.e., the optimal solution) and its position are selected at each iteration based on the maximum paths obtained for different solutions. They are often in a stringent social hegemonic hierarchy. The heads are made up of males and females known as Alpha, responsible for hunting, sleep, waking, and other decisions. Choices made by Alpha are permissible on the board. Beta and Delta Gray refer to classes two and three in the specific structure of wolves. In short, they are extra wolves with enough help to set up an alpha or group presentation [31, 32]. The remaining wolves represent omega, which is a small group of gray wolves. Alpha, beta, and deltoid mega wolves are responsible for monitoring (optimization) the MWO process.

### 4.1.2 Mathematical model of MWO

In MWO, the most significant inspiration is to surround a prey by leadership through $\alpha$, $\beta$ and $\delta$, which can be methodically reputable as beneath:

$$
M(k + 1) = M(K)C.P
$$

In the above Eq. (5), $P$ can be given as,

$$
P = |V \cdot M_I(k) - M(k)|
$$

Here, $M$ represent the modified wolf position, $M_I$ is the prey position, $C$, $V$ are the coefficient vectors, and the number of iterations is defined by $k$. The coefficient vectors $C$ and $V$ can be obtained by the equation below:

$$
C = 2c \cdot w_1 - c
$$

$$
V = 2 \cdot w_2
$$

where $c$’ is will be linearly decreased from 2 to 0 and $w_1$ and $w_2$ are the random vectors from [0,1]. The parameter $c$ is updated in every iteration within the range from 2 to 0 according to,

$$
c = 2 - k \left( \frac{2}{k} \right)
$$

At this point $K$ denotes the total number of iterations allowed. The updating of wolf’s position based one first three best solutions can be obtained as beneath:

$$
M_1 = |M_z(k) - C_1 \cdot P_z|
$$

$$
M_2 = |M_\beta(k) - C_2 \cdot P_\beta|
$$

$$
M_3 = |M_\delta(k) - C_3 \cdot P_\delta|
$$

where $P_z$, $P_\beta$ and $P_\delta$ are obtained as follows:

$$
P_z = |V_1 \cdot M_z - M|
$$

$$
P_\beta = |V_2 \cdot M_\beta - M|
$$

$$
P_\delta = |V_3 \cdot M_\delta - M|
$$

Based on the above Eqs. (12), (13) and (14), the explanation for next iteration will be obtain as follows:

$$
M(k + 1) = \frac{(M_1 + M_2 + M_3)}{3}
$$

The process of updating of wolf position takes place incessantly until the maximum iteration is achieved. The working function of the proposed optimal feature selection is given in the next section.
4.2 Weight fusion using optimal feature fusion (OFF) algorithm

Competition between team members for food leads to distribution and group mergers. A food deficit group is divided into OFF all the groups that show a wholly separated social structure when there is a food deficit group. OFF has seven phases: Startup Phase, Local Leader Phase, Global Leader Phase, Local Leader Learning Phase, Global Leader Learning Phase, Local Leader Completion Phase, and Global Leader Phase. These steps are described as follows:

4.2.1 Formation

An initial N optimal feature fusion algorithm population is generated, where FFO_i represents the ith FFO in the population. Each FFO_i is initialized as shown in Eq. (16):

$$FFO_{ij} = FFO_{minj} + \varphi \times (FFO_{maxj} - FFO_{minj})$$  \hspace{1cm} (16)

where FFO_{minj} and FFO_{maxj} are lower and upper limits of the search space in the jth dimension, and \( \varphi \) is a consistently dispersed random number in the range [0, 1].

4.2.2 Data phase

All spider monkeys, which are feature vectors in our case, are updated at this point based on the experience of their local leader and local team member—the FFO Exercise checks to update the FFO level to a new level. If the exercise is high, the FFO will not change its position. Here, the level update process is given in Eq. (17):

$$FFO_{newij} = FFO_{ij} + \varphi \times (LL_{kj} - FFO_{ij}) + \psi \times (FFO_{rij} - FFO_{ij})$$  \hspace{1cm} (17)

where FFO_{ij} is the jth dimension of ith FFO, LL_{kj} represent the kth local leader of that group, and FFO_{rij} is rth FFO chosen illogically within kth group in jth size such that r \( \neq \) i and \( \psi \) is consistently distributed random number in the range [-1, 1] (Fig. 2).
4.2.3 Environmental phase

Each FFO uses the knowledge of a global leader and the experience of neighboring points to update their position and find the best solution. The level update equation at this stage is as follows:

$$FFO_{newij} = FFO_{ij} + \phi \ast (GL_j - FFO_{ij}) + \psi \ast (FFO_{ij} - FFO_{ij})$$

where $GL_j$ is the location of group leader in jth dimension and $j = \{1, 2, 3, \ldots, D\}$ chosen randomly.

4.2.4 Region-wise phase

Unless any local leader is reorganized to a point known as the local leader limit, all members of this group will renew their positions through random startups or using the experience of a global leader. This is the confusion ratio given in Eq. (4):

$$FFO_{newij} = FFO_{ij} + \phi \ast (GL_j - FFO_{ij}) + \psi \ast (FFO_{ij} - LL_{ij})$$

4.3 Action classification using LCNN-SSO based classifier

The hybrid LCNN-Salp swarm optimization (LCNN-SSO) based classifier with a single unidirectional affirmed layer. In the specific utilitarian sort of how dormant segments and discernments interface was genuinely searing. This is certainly not a significant issue when versatility to show different sorts of affiliations. With a singular layer, by some coincidence, this can be incredibly trying. By reasonableness of the announcement, we fixed this issue by including more layers. Inside LCNN, this is reliably harmed since we first need to pick how and where to join extra nonlinearity. We could stack different layers of LSTMs more than one another. This outcome is in a structure that is gainfully versatile because of the blend of several immediate layers. Specifically, information may be epic at various degrees of the stack. For example, we should keep assembled level information about money-related budgetary conditions (bear or truly slanting business division) open at an epic level. In contrast, at a lower level, we record shorter-term transient parts.

4.3.1 Mathematical dependencies

At duration point $t$, the terms mini pack $Y_t \in R^{n \times d}$ (no. of models: $n$, no. of information sources: $d$). When layer $l$ ($l = 1, \ldots, T$) is $G^{(l)}_t \in R^{n \times h}$ have secured condition (no. of units hidden: $h$), the yield variable layer $Out_t \in R^{n \times q}$. A confirmed layer is affirming work $h_{1}$ for level $l$. We figure the checked condition of level $l$ as already, utilizing $Y_t$. As information, for each following layer, the confirmed condition of the past level is utilized in its domicile.

$$G^l_t = h_1(Y_t, G^l_{t-1})$$
At long last, the yield of the yield layer is essentially picked the confirmed condition of camouflaged layer L. We utilize the yield work g to point out as,

\[ Out_t = k_1(G_t^{(L)}) \]  

(21)

Specifically, we can pick a standard LCNN, the LSTM, to fathom the model. An LCNN is a class of fake neural systems that builds up the standard feed-forward neural structure with coats in affiliations. Unlike a feed-forward neural network, an LCNN can process the consecutive obligations by having a convulsive camouflaged express whose start at each constant improvement store of the past progress. Right now, the structure can show dynamic passing leads. Given improvement information, where \( y_t \) denotes the information at jth duration point, an LCNN fortifies it is sporadic confirmed \( g_t \) input state by

\[ g_t = \begin{cases} 0, & \text{if } t = 0 \\ \phi(g_{t-1}, y_t), & \text{otherwise} \end{cases} \]  

(22)

where \( \phi \) denotes limitation of nonlinear, for instance, a determined sigmoid limit or hyperbolic deviation work. Then again, the LCNN required a yield y. For specific tasks, for example, hyper-powerful picture course of action, this only needed one yield, i.e., \( y_t \). In the standard LCNN type, which upload standard of the dull covered state is ordinarily executed as seeks after:

\[ g_t = \phi(U_{yt} + V_{g_{t-1}}) \]  

(23)

U and V are the terms in grids dedicating present movement and the foundation of unpredictable secured units at the past advancement. An LCNN can display a likelihood allotment all through the going with a fragment of the social occasion information, given its current input state \( h_t \). By getting a stream over game-plan information of length variable. Let y1, y2 and \( y_n \) Be the social occasion likelihood, which can be deteriorated into A broken layer with standard repetitive concealed units is appeared in (24), which registers a weighted direct total of wellsprings of information and in this manner applies a nonlinear utmost. Abnormally, based on LSTM dreary layer makes a memory part \( b_t \) at duration t. The beginning units of LSTM can be figured by

\[ g_t = \text{out}, \text{tanh}(b_t) \]  

(24)

where \( \text{tanh}() \) denotes digression hyperbolic capacity and \( \text{out} \) is the yield door that decides the piece of the content memory that will be uncovered. The yield door is refreshed by

\[ g_t = \text{out}, \text{tanh}(b_t) \]  

(25)

where \( \sigma() \) is a sigmoid key limit and terms U mean weight; e.g., Uoi denotes information yield cross weight section and addresses Woc the storage-yield weight framework. The storage cell \( b_t \) is revived by including a new substance of storage cell \( b_t \). And some discarding portions of the present memory content. The data entryway modifies how much the new memory information is added to the memory cell. How much substance of the current memory cell is ignored is picked by the neglected door \( g_t \).

The conditions that figure these two entryways are according to the accompanying:

\[ j_t = \sigma(U_jy_t + U_{jb}h_{t-1} + U_{bj}b_{t-1}) \]  

(26)

\[ p_t = \sigma(U_py_t + U_{pb}h_{t-1} + U_{pb}b_{t-1}) \]  

(27)

The failure of the numerically simulated synthetic neural network (LCNN-SSO) for signal classification leads to the enslavement of the initial centers of the slaves and significantly affects the final groups of nodes. When clustering data objects, the most accurate cluster group results can be achieved by selecting a data model for accurate data distribution, selecting cluster centers correctly, and updating the clustering center. The idea of selecting cluster centers for the optimal LCNN classifier: first, k rejects isolated points (k data objects and other objects that are rapidly added to the Euclidean distance of the cluster data); Calculate all the centers of the remaining objects, select the point closest to the center of the first point, and repeat to find the point farthest from the starting point (the selected focus will no longer participate in the selection of the next center). The hierarchical system moves on to the next step until a point is found.

4.3.1.1 Initialization step In the introduction step, the k-implies calculation instates \( \mu \) of group \( c_j \), i.e.,

\[ h_j^{(1)} = \{ y_p : y_p \in \times, h_j^{(1)} \neq y_p, 1 \leq j \leq k, j \neq i \} \]  

(28)

Different types of SSO can use different methods. However, the most ordinary method is to use random data points other than x to extract each centroid.

4.3.1.2 Assignment step Presently, every data point is named to a bundle whose centroid gives minimal squares in the gatherings.

\[ c_j^{(i)} = \{ y_n : ||y_n - \mu_i^{(i)}||^2 \leq ||y_n - \mu_j^{(i)}||^2, \forall j, 1 \leq i \leq k \} \]  

(29)

Over time, \( y_n \) is only assigned to one cluster with \( j \) one i. Overtime \( y_n \) can be assigned to an additional cluster, which reduces the cluster size of the squares. The data summit here does not belong to multiple clusters.
4.3.1.3 Update step During the update phase, Centroids K- or c calculates the following iterations based on data from each cluster period.

$$h_j^{(k+1)} = \frac{1}{\sum_{i=1}^{c(k)} x_i} \sum_{i=1}^{c(k)} x_i$$

For a given threshold $\xi \geq 0$, if $|h_j^{(k+1)} - h_j^{(k)}| \leq \xi$, $\forall j, 1 \leq j \leq t$, this stops the iteration process because the algorithm has already reduced it. Otherwise, it returns to the work position and drops sets $k = k + 1$. The working process of the proposed LCNN-SSO classifier is given in Algorithm 1.

5 Results and discussion

In this section, we will evaluate the effectiveness of specific CBUA-OE devices with existing advanced equipment. Data availability for performance evaluation is a significant obstacle to developing user authentication systems [33]. The primary database is currently unavailable to hundreds of users. However, this database does not meet our requirements because it requires many users to select representatives. In addition, we emphasize a small number of models per user to reduce the data collection burden of users. Therefore, we have created a database larger than the one currently used by modern methods.

The entire exercise is analyzed in terms of performance matrix parameters. Essential parameters are given below:

$$TPR = \frac{TP}{Actual \ Positive} = \frac{TP}{(TP + FN)}$$

$$FNR = \frac{FN}{Actual \ Negative} = \frac{FN}{(TP + FN)}$$

$$TNR = \frac{TN}{Actual \ Negative} = \frac{TN}{(TN + FP)}$$

$$FPR = \frac{FP}{Actual \ Negative} = \frac{FP}{(TN + FP)}$$

$$Precision = \frac{TP}{(TP + FP)}$$

$$Recall \ rate = \frac{TP}{(TP + FN)}$$

$$F \ measure = 2 \cdot (Precision \cdot \ Recall \ rate)/(Precision + \ Recall \ rate)$$

$$Accuracy = \frac{TP + TN}{(TP + TN + FP + FN)}$$

$$Specificity = \frac{TN}{(TN + FP)}$$

Here TP is for true/correct or genuine user and system also taking it as a genuine user and TN indicates truly negative person means impostor or not allowed category. Similarly, FP is a false positive user who is mistakenly considered as a genuine user. FN is the right user, but the system has been interpreted as negative/imposter user. Specificity and FPR are complementary; by subtracting specificity from 1, FPR can be obtained. F Measure is the mid-way to take advantage of both recall rate and precision [33, 34].

5.1 Dataset descriptions

The proposed CBUA-OE technique is analyzed through multi-biometric data’s is fingerprint, face, and keystroke. All the dataset used are cited at [35-41]. The facial database details are given as follows:

- **ORL database** It measures 112 × 92 and contains 400 images. 40 people, 10 pictures per person. In the anterior view, the faces rotate vertically and slightly to the left and right. For example, we reduced face image factorization to 2576 (pixels) × 400 (face) and original face image formatting to 10,304 (pixels) × 400 (face). To avoid very large values, divide the data array by 100. This category does not significantly affect the performance of MF systems. Some models are shown in Fig. 3 [39].

- **Yale face database** It contains 165 grayscale images in GIF format of 15 persons. There is 11 imagery per subject, one per dissimilar facial expression or configuration: center-light, glasses, happy, left-light, w/no glasses, normal, right-light, sad, and sleepy, surprised, and wink. Some samples are shown in Fig. 4 [40].

- **FASSEG dataset** It comprises four subsets (multipose01, frontal03, frontal02, and frontal01), including several facial images. In face segmentation, the FASSEG dataset is very useful for preparation and difficult the routine method. The subset (multipose01) consists of 200 facial images with ground-truth masks for six classes (background, mouth, eyes, nose, skin, and hair) [41]. The subsets (frontal01 and frontal02) consist of 70 RGB images with labeled ground truth masks. At last, the frontal03 subset contains 150 face masks captured in different face expressions, orientations, and illumination conditions. Some samples are shown in Fig. 5.
• **KEY STROKE data sets** We have used a dataset prepared by Kevin Killourhy and Roy Maxion [35]. The data consist of keystroke-timing information from 51 subjects (typists), each typing a password (.tie5R-oanl) 400 times. Keystroke100 dataset is also used for experiments. Keystroke100 benchmark dataset is for research on pressure-sensitive keystroke dynamics and typing biometrics. This dataset contains keystroke/typing patterns of 100 users typing the password “try4-mbs” [36, 37].

• **Finger print datasets** FVC 2004 datasets 1 and 2 were used for experiments. Here for each database, a total of 120 fingers and 12 impressions per finger (1440 impressions) were gathered. As in previous editions, the size of each database to be used in the test was established as 110 fingers wide (w) and eight impressions per finger deep (d) (880 fingerprints in all). The dataset optical sensor was used to get 640*480 (307 k pixels), 100*8 impressions of each print, and 500 dpi. For DB2 328*364 (119 k pixels), 100*8 impressions with 500 dpi [38].

After the multiple biometric data fusion, we compute the consolidated dataset, consisting of fingerprint, face, and keystroke of users. Here, we consider the user’s different keystrokes are press-press, release-press, and hold duration. Figure 6 shows the fused database of three different users (are U1, U2, and U3).

5.2 Comparative analysis of proposed and existing techniques

In this section, we examine and contrast the presentation of the planned LCNN-SSO classifier with existing classifiers SVM, KNN, LSTM and DBM in terms of different
presentation metrics: accuracy, precision, recall, etc. F-measure, sensitivity, and specificity. Table 1 describes the performance of classifiers over different datasets are ORL, YALE, and FASSEG. The proposed LCNN-SSO classifier’s concert is compared with the existing classifiers are SVM, KNN, LSTM, and DBN. Figure 7 clearly shows the accuracy comparison of planned and current classifiers for three databases: ORL, YALE, and FASSEG. It depicts the average accuracy of the proposed LCNN-SSO classifier is 14% higher than the existing state-of-art classifiers. For the ORL database, the accuracy of the proposed LCNN-SSO classifier is 28%, 20%, 8%, and 0.2% higher than the SVM, KNN, LSTM, and DB classifier, respectively. For the YALE database, the accuracy of the proposed LCNN-SSO classifier is 32%, 17%, 9.3%, and 1.3% higher than the SVM, KNN, LSTM and DB classifier, respectively. For the FASSEG database, the accuracy of the proposed LCNN-SSO classifier is 31%, 14%, 5.8%, and 1% higher than the SVM, KNN, LSTM, and DB classifier, respectively.

Figure 8 clearly shows the precision judgment of planned and existing classifiers for three databases: ORL, YALE, and FASSEG. It depicts the average precision of the proposed LCNN-SSO classifier is 15% higher than the current state-of-art classifiers. For the ORL database, the precision of the proposed LCNN-SSO classifier is 37.2%, 25.7%, 5.7%, and 1.5% higher than the SVM, KNN, LSTM, and DB classifier, respectively. For the YALE database, the precision of the proposed LCNN-SSO classifier is 31%, 23.4%, 6.2%, and 0.2% higher than the SVM, KNN, LSTM and DB classifier. For the FASSEG database, the precision of the proposed LCNN-SSO classifier is 15.6%, 19.5%, 7.1%, and 1.8% higher than the SVM, KNN, LSTM and DB classifier.

Figure 9 clearly shows the recall judgment of planned and existing classifiers for three databases: ORL, YALE, and FASSEG. It depicts the average recall of the proposed LCNN-SSO classifier is 11% higher than the current state-of-art classifiers. For the ORL database, the recall of the proposed LCNN-SSO classifier is 32%, 20%, 4.3%, and 0.3% higher than the SVM, KNN, LSTM and DB classifier. For the YALE database, the recall of the proposed LCNN-SSO classifier is 32%, 20%, 4.3%, and 0.3% higher than the SVM, KNN, LSTM and DB classifier. For the FASSEG database, the recall of the proposed LCNN-SSO classifier is 28%, 18%, 3.2%, and 1.2% higher than the SVM, KNN, LSTM and DB classifier.

Figure 10 clearly shows the F-measure judgment of planned and existing classifiers for three databases: ORL, YALE, and FASSEG. It depicts the average F-measure of the proposed LCNN-SSO classifier is 18% higher than the current state-of-art classifiers. For the ORL database, the F-measure of the proposed LCNN-SSO classifier is 9.5%, 7.7%, 7.2%, and 1% higher than the SVM, KNN, LSTM, and DB classifier, respectively. For the YALE database, the F-measure of the proposed LCNN-SSO classifier is 9.6%, 17.7%, 9.67%, and 7.3% higher than the SVM, KNN, LSTM, and DB classifier, respectively. For the FASSEG database, the F-measure of the proposed LCNN-SSO classifier is 6.57%, 5.2%, 3%, and 2.8% higher than the SVM, KNN, LSTM, and DB classifier.

Figure 11 clearly shows the sensitivity judgment of planned and existing classifiers for three databases: ORL, YALE, and FASSEG. It depicts the average sensitivity of the proposed LCNN-SSO classifier is 4.2% higher than the existing state-of-art classifiers. For the ORL database, the sensitivity of the proposed LCNN-SSO classifier is 6.07%, 4.9%, 4.5%, and 2.6% higher than the SVM, KNN, LSTM and DB classifier. For the YALE database, the sensitivity of the proposed LCNN-SSO classifier is 5.3%, 4%, 1.56%, and 1.57% higher than the SVM, KNN, LSTM and DB classifier. For the FASSEG database, the sensitivity of the proposed LCNN-SSO classifier is 8%, 6%, 5.5%, and 0.7% higher than the SVM, KNN, LSTM and DB classifier.

Figure 12 clearly shows the specificity assessment of planned and existing classifiers for three databases: ORL, YALE, and FASSEG. It depicts the average specificity of the proposed LCNN-SSO classifier is 3% higher than the current state-of-art classifiers. For the ORL database, the specificity of the proposed LCNN-SSO classifier is 3.4%, 3%, 3.2%, and 2.6% higher than the SVM, KNN, LSTM and DB classifier. For the YALE database, the specificity of the proposed LCNN-SSO classifier is 2%, 1.9%, 4.4%, and 4.8% higher than the SVM, KNN, LSTM and DB classifier. For the FASSEG database, the specificity of the proposed LCNN-SSO classifier is 5.5%, 4.3%, 4%, and 2% higher than the SVM, KNN, LSTM and DB classifier.

Figure 13 shows the false positive rate (FPR) assessment of planned and existing classifiers for three databases: ORL, YALE, and FASSEG. It highlights the average FPR
of the proposed LCNN-SSO classifier is at least 35% lower than the existing state-of-art classifiers. For the ORL database, the FPR of the proposed LCNN-SSO classifier is 44%, 41%, 42%, and 37%, lower than SVM, KNN, LSTM, and DBM classifier, respectively. For the YALE database, the FPR of the proposed LCNN-SSO classifier is 31%, 30%, 49%, and 52% lower than the SVM, KNN, LSTM and DBM classifier. For the FASSEG database, the specificity of the proposed LCNN-SSO classifier is 54%, 48%, 44%, and 30% higher than the SVM, KNN, LSTM and DBM classifier.

Table 2 describes the presentation contrast of planned CBUA-OE and obtainable techniques: FO-DBN, IILBDL and IKLDA + PNN in terms of accuracy, precision, recall, F-measure, sensitivity, and specificity. For the ORL database, the accuracy of the proposed CBUA-OE technique is
7%, 7%, and 14% higher than the existing FO-DBN, IILBDL, and IKLDA + PNN techniques, shows in Fig. 14. The precision of the proposed CBUA-OE technique is 17%, 1.6%, and 21.3% higher than the existing FO-DBN, IILBDL, and IKLDA + PNN techniques. The recall of the proposed CBUA-OE technique is 4.7%, 13.9%, and 6.6% higher than the existing FO-DBN, IILBDL, and IKLDA + PNN techniques. The F-measure of the proposed CBUA-OE technique is 5.4%, 4%, and 6% higher than the existing FO-DBN, IILBDL, and IKLDA + PNN techniques. The sensitivity of the proposed CBUA-OE technique is 1.7%, 0.4%, and 5.5% higher than the existing FO-DBN, IILBDL, and IKLDA + PNN techniques. The specificity of the
proposed CBUA-OE technique is 2.8%, 1.4%, and 3% higher than the existing FO-DBN, IILBDL, and IKLDA + PNN techniques. The FPR of the proposed CBUA-OE technique is 42%, 51%, and 57% lower than the existing FO-DBN, IILBDL, and IKLDA + PNN methods.

Table 3 describes the performance comparison of proposed CBUA-OE and existing techniques are FO-DBN, IILBDL, and IKLDA + PNN in terms of accuracy, precision, recall, F-measure, sensitivity, and specificity. The proposed CBUA-OE technique’s accuracy is 8.7%, 14.6%, and 15% higher than the existing FO-DBN, IILBDL, and IKLDA + PNN for the YALE database show in Fig. 15.

The precision of the proposed CBUA-OE technique is 4.5%, 3.3%, and 15.2% higher than the existing FO-DBN, IILBDL, and IKLDA + PNN techniques. The recall of the proposed CBUA-OE technique is 15.4%, 1.1%, and 12.5% higher than the existing FO-DBN, IILBDL, and IKLDA + PNN techniques. The F-measure of the proposed CBUA-OE technique is 5.4%, 4%, and 6% higher than the existing FO-DBN, IILBDL, and IKLDA + PNN techniques.
techniques. The sensitivity of the proposed CBUA-OE technique is 2.6%, 2.3%, and 3.1% higher than the existing FO-DBN, IILBDL, and IKLDA + PNN techniques. The specificity of the proposed CBUA-OE technique is 2.6%, 1.3%, and 3.2% higher than the existing FO-DBN, IILBDL, and IKLDA + PNN techniques. The FPR of the proposed CBUA-OE technique is 43%, 51%, and 57% lower than the existing FO-DBN, IILBDL, and IKLDA + PNN methods.

Table 4 describes the performance comparison of proposed CBUA-OE and existing techniques are FO-DBN, IILBDL, and IKLDA + PNN in terms of accuracy, precision, recall, F-measure, sensitivity, and specificity. For the ORL database, the accuracy of the proposed CBUA-OE technique is 12.2%, 10%, and 13% higher than the existing FO-DBN, IILBDL, and IKLDA + PNN methods shows in Fig. 16. The precision of the proposed CBUA-OE technique is 5.4%, 2.1%, and 11% higher than the existing FO-
DBN, IILBDL, and IKLDA + PNN techniques. The recall of the proposed CBUA-OE technique is 6.1%, 1.4%, and 6.5% higher than the existing FO-DBN, IILBDL, and IKLDA + PNN techniques. The F-measure of the proposed CBUA-OE technique is 3.3%, 1.1%, and 4.3% higher than the existing FO-DBN, IILBDL, and IKLDA + PNN techniques. The sensitivity of the proposed CBUA-OE technique is 7.8%, 1.7%, and 4.7% higher than the existing FO-DBN, IILBDL, and IKLDA + PNN techniques. The specificity of the proposed CBUA-OE technique is 8.7%, 1.1%, and 4% higher than the existing FO-DBN, IILBDL, and IKLDA + PNN techniques. The FPR of the proposed CBUA-OE technique is 46%, 52%, and 72% lower than the existing FO-DBN, IILBDL, and IKLDA + PNN methods (Table 4). All the acronyms used in the article are highlighted below (Table 5).

Table 3 Comparative analysis of proposed and existing techniques for YALE database

| Metrics (%) | Techniques                  |
|-------------|-----------------------------|
|             | CBUA-OE | FO-DBN | IILBDL | IKLDA + PNN |
| Accuracy    | 99.24   | 84.35  | 98.82  | 77          |
| Precision   | 99.12   | 83.93  | 81.20  | 80.20       |
| Recall      | 98.17   | 85.92  | 84.90  | 83.02       |
| F-measure   | 96.45   | 85.73  | 83.15  | 80.50       |
| Sensitivity | 95.27   | 92.29  | 90.12  | 89.80       |
| Specificity | 95.67   | 92.53  | 91.25  | 90.12       |
| False positive rate | 4.33 | 7.47 | 8.75 | 9.88 |

Fig. 15 Comparative analysis of planned and existing techniques for YALE database

Table 4 Comparative analysis of proposed and existing techniques for FASSEG database

| Metrics (%) | Techniques                  |
|-------------|-----------------------------|
|             | CBUA-OE | FO-DBN | IILBDL | IKLDA + PNN |
| Accuracy    | 99.13   | 86.12  | 96.10  | 98.12       |
| Precision   | 95.87   | 85.25  | 83.45  | 80.60       |
| Recall      | 97.29   | 90.92  | 89.56  | 85.32       |
| F-measure   | 96.47   | 92.29  | 91.25  | 89.24       |
| Sensitivity | 95.08   | 90.60  | 89.00  | 83.52       |
| Specificity | 95.39   | 91.60  | 90.52  | 83.54       |
| False positive rate | 4.61 | 8.4 | 9.48 | 16.46 |

All the acronyms used in the article are highlighted below (Table 5).
Fig. 16 Comparative analysis of planned and existing techniques for FASSEG database

Table 5 List of acronym used in the article

| Sr. no. | Acronym     | Details                                                                 |
|-------|-------------|-------------------------------------------------------------------------|
| 1     | KB          | Key stroke biometrics                                                   |
| 2     | BIA         | Biometrics based unmistakable confirmation and approval                 |
| 3     | BT          | Biometric template                                                      |
| 4     | CA          | Continuous authentication                                               |
| 5     | CBUA-OE     | Continuous biometric user authentication system for online evaluation   |
| 6     | CNN         | Convolution neural network                                              |
| 7     | DBM Classifier | Density based modular classifier                                   |
| 8     | ERR         | Equal error rate                                                        |
| 9     | FASSEG Database | Face Semantic Segmentation Repository (Frontal 1 Frontal 2 databases) |
| 10    | FNR         | False negative rate                                                     |
| 11    | FO-DBN,     | Deep belief network                                                     |
| 12    | FPR         | False positive rate                                                     |
| 13    | GAR         | Genuine acceptance rate                                                 |
| 14    | IILBDL      | Identity-by-descent probabilities at a locus L Deep learning classifier  |
| 15    | IKLDA + PNN | Improved Kernel linear discriminate analysis + probabilistic neural network |
| 16    | KNN         | K Nearest neighbor classifier                                            |
| 17    | LCNN        | A LCNN is a class of fake neural system that builds up the standard feed forward neural structure with coasts in affiliations |
| 18    | LSTM        | Long short-term memory                                                  |
| 19    | MWO         | Modified wolf algorithm                                                 |
| 20    | OFF         | Optimal feature fusion                                                  |
| 21    | ORL database | Our database of faces, 1992                                              |
| 22    | SVM         | Support vector machine classifier                                        |
| 23    | TNR         | True negative rate                                                       |
| 24    | TPR         | True positive rate                                                       |
| 25    | WIFI        | Wireless fidelity                                                        |
| 26    | YALE database | Yale face database created by Yale University for research and analysis |
6 Conclusion

The study proposed a continuous biometric user authentication system for online examinations for recognizing the normal and abnormalities. Here, MWO algorithm features are utilized to extract the features from the facial data. Then, the OFF algorithm selects the most favourable feature vectors and combines the facial images from different records. A set of most overriding discriminative features is obtained by choosing the optimal features from the extract features. These best features are secret through the LCNN-S5O classifier. From simulation results, we observe that the average accuracy of the proposed CBUA-OE technique is 9.3%, 12.7%, and 11.7% higher than the existing techniques with ORL, YALE, and FASSEG databases. The average precision of the proposed CBUA-OE technique is 13.3%, 7.6%, and 8.4% higher than the existing techniques with ORL, YALE, and FASSEG databases. The average recall of the proposed CBUA-OE technique is 11.73%, 9.6%, and 4.6% higher than the existing techniques with ORL, YALE, and FASSEG databases, respectively. The average sensitivity of the proposed CBUA-OE technique is 2.5%, 7.5%, and 4.7% higher than the existing techniques with ORL, YALE, and FASSEG databases, respectively. The average specificity of the proposed CBUA-OE technique is 2.4%, 2.42%, and 4.6% higher than the existing techniques with ORL, YALE, and FASSEG databases, respectively. The average FPR is 35%, 39%, 42%, and 48% lower than the existing techniques with ORL, YALE, and FASSEG databases. The average F-measure of the proposed CBUA-OE technique is 5.4%, 8.5%, and 2.9% higher than the existing techniques with ORL, YALE, and FASSEG databases, respectively. The average accuracy of the proposed CBUA-OE technique is 9.6%, 11.7%, and 2.4% higher than the existing techniques with ORL, YALE, and FASSEG databases. The average specificity of the proposed CBUA-OE technique is 2.4%, 2.42%, and 4.6% higher than the existing techniques with ORL, YALE, and FASSEG databases, respectively. The average FPR is 35%, 39%, 42%, and 48% lower than the existing FO-DBN, IILBDL, and IKLDA + PNN techniques.

Author contributions All authors whose names appear on the submission drafted the work.

Funding The authors did not receive support from any organization for the submitted work.

Data availability The datasets used during and/or analyzed during the current study are available at below given links. We are highly thankful to all the data set provider institute and agencies. Keystroke Dynamics—Benchmark Data Set (cmu.edu), Typing Biometrics Keystroke Dataset (cubk.eduku.hk), FVC2004—Third International Fingerprint Verification Competition (unibo.it), The Database of Faces (cam-orl.co.uk), Yale Face Database (ucsd.edu), GitHub—massimomauro/FASSEG-repository: Datasets for multi-class and multi-pose face segmentation.

Code availability The Code generated during and/or analyzed during the current study are available from the corresponding author on reasonable request.

Declarations

Conflict of interest The authors declare that they have no conflict of interest.

Consent to participate All authors read and approved the final manuscript.

Consent for publication All authors have approved the version to be published.

References

1. Niinuma, K., Park, U., Jain, A.K.: Soft biometric traits for continuous user authentication. IEEE Trans. Inf. Forensics Secur. 5(4), 771–780 (2010)
2. Moini, A., Madni, A.M.: Leveraging biometrics for user authentication in online learning: a systems perspective. IEEE Syst. J. 3(4), 469–476 (2009)
3. Frank, M., Biedert, R., Ma, E., Martinovic, I., Song, D.: Touchalytics: on the applicability of touchscreen input as a behavioral biometric for continuous authentication. IEEE Trans. Inf. Forensics Secur. 8(1), 136–148 (2012)
4. Tsai, P.W., Khan, M.K., Pan, J.S., Liao, B.Y.: Interactive artificial bee colony supported passive continuous authentication system. IEEE Syst. J. 8(2), 395–405 (2012)
5. Mondal, S., Bours, P.: A computational approach to the continuous authentication biometric system. Inf. Sci. 304, 28–53 (2015)
6. Saevane, H., Clarke, N., Furnell, S., Biscione, V.: Continuous user authentication using multi-modal biometrics. Comput. Secur. 53, 234–246 (2015)
7. Murillo-Escobar, M.A., Cruz-Hernández, C., Abundiz-Pérez, F., López-Gutiérrez, R.M.: A robust embedded biometric authentication system based on fingerprint and chaotic encryption. Expert Syst. Appl. 42(21), 8198–8211 (2015)
8. Liu, C.L., Tsai, C.J., Chang, T.Y., Tsai, W.J., Zhong, P.K.: Implementing multiple biometric features for a recall-based graphical keystroke dynamics authentication system on a smart phone. J. Netw. Comput. Appl. 53, 128–139 (2015)
9. Rodwell, P.M., Furnell, S.M., Reynolds, P.L.: A non-intrusive biometric authentication mechanism utilizing physiological characteristics of the human head. Comput. Secur. 26(7–8), 468–478 (2007)
10. Azzini, A., Marrara, S., Sassi, R., Scotti, F.: A fuzzy approach to multi-modal biometric continuous authentication. Fuzzy Optim. Decis. Mak. 7(3), 243 (2008)
11. Bours, P.: Continuous keystroke dynamics: A different perspective towards biometric evaluation. Inf. Secur. Techn. Rep. 17(1–2), 36–43 (2012)
12. Srinivasa, K.G., Gosukonda, S.: Continuous multi-modal user authentication: coupling hard and soft biometrics with support vector machines to attenuate noise. CSI Trans. ICT 2(2), 129–140 (2010)
13. Wójtowicz, A., Joachimiak, K.: Model for adaptable context-based biometric authentication for mobile devices. Pers. Ubiquitous Comput. 20(2), 195–207 (2016)
14. Ramu, T., Arivoli, T.: A framework of secure biometric-based online exam authentication: an alternative to the traditional exam. Int. J. Sci. Res. 4(11), 52–60 (2013)
15. Fayyoumi, A., Zarrad, A.: Novel solution based on face recognition to address identity theft and cheating in online examination systems. Adv. Internet Things 4, 5–12 (2014)
16. Traoré, I., Nakkabi, Y., Saad, S., Sayed, B., Ardigo, I.D., de FariaQuinan, P.M.: Ensuring online exam integrity through continuous biometric authentication. In: Traoré, I., Awad, A., Wongang, I. (eds.) Information Security Practices. pp. 73–81. Springer, Cham (2017)
17. Sabbah, Y.W., Saroit, I.A., Kob, A.M.: A smart approach for bimodal biometric authentication in home-exams (SABBAH model). Biometrics Bioinform. 4, 32–45 (2012)
18. Fluck, A., Pullen, D., Harper, C.: Case study of a computer-based examination system. Australas. J. Educ. Technol. (2009). https://doi.org/10.14742/ajet.1126
19. Adebayo, O., Abdulhamid, S.M.: E-exams system for Nigerian universities with an emphasis on security and result integrity (2014). arXiv preprint arXiv:1402.0921.
20. Ullah, A., Xiao, H., Barker, T., Lilley, M.: Evaluating security and usability of profile-based challenge questions authentication in online examinations. J. Internet Serv. Appl. 5(1), 2 (2014)
21. Peng, G., Zhou, G., Nguyen, D.T., Qi, X., Yang, Q., Wang, S.: Continuous authentication with touch behavioral biometrics and voice on wearable glasses. IEEE Trans. Hum. Mach. Syst. 47(3), 404–416 (2016)
22. Ali, M.L., Monaco, J.V., Tappert, C.C., Qiu, M.: Keystroke biometric systems for user authentication. J. Signal Process. Syst. 86(2–3), 175–190 (2017)
23. Ullah, A., Xiao, H., Barker, T.: A study into the usability and security implications of text and image-based challenge questions in the context of online examination. Educ. Inf. Technol. 24(1), 13–39 (2019)
24. Ullah, A., Xiao, H., Barker, T.: A dynamic profile questions approach to mitigate impersonation in online examinations. J. Grid Comput. 17(2), 209–223 (2019)
25. Prakash, A.: Continuous user authentication-based score level fusion with hybrid optimization. Clust. Comput. 22(5), 1929–1949 (2019)
26. Yang, Y., Guo, B., Wang, Z., Li, M., Yu, Z., Zhou, X.: BehaveSense: continuous authentication for security-sensitive mobile apps using behavioral biometrics. Ad Hoc Netw. 84, 9–18 (2019)
27. Nunes, I.D.O., Eldelfrawy, K., Lepoint, T.: SNUSE: a secure computation approach for large-scale user re-enrollment in biometric authentication systems. Future Gen. Comput. Syst. 98, 259–273 (2019)
28. Chatterjee, K.: Continuous user authentication system: a risk analysis based approach. Wirel. Pers. Commun. 108(1), 281–295 (2019)
29. Wang, F., Li, Z., Han, J.: Continuous user authentication by contactless wireless sensing. IEEE Internet Things J. 6(5), 8323–8331 (2019)
30. Kiyani, A.T., Lasebue, A., Ali, K., Rehman, M.U., Haq, B.: Continuous user authentication featuring keystroke dynamics based on robust recurrent confidence model and ensemble learning approach. IEEE Access (2020). https://doi.org/10.1109/ACCESS.2020.3019467
31. Purohit, H., Ajmera, P.K.: Optimal feature level fusion for secured human authentication in multimodal biometric system. Mach. Vis. Appl. 32, 24 (2021)
32. Vasanthi, M., Seetharaman, K.: Facial image recognition for biometric authentication systems using a combination of geometrical feature points and low-level visual features. J. King Saud Univ. Comput. Inf. Sci. (2020)
33. Sunaryono, D., Siwaswanto, J., Anggoro, R.: An android-based course attendance system using face recognition. J. King Saud Univ. Comput. Inf. Sci. 33, 304–312 (2021)
34. Purohit, H., Ajmera, P.K.: Multi-modal biometric systems: a brief study. Int J. Innov. Technol. Explor. Eng. 8(7), 108–111 (2019)
35. Killourhy, K.S., Maxion, R.A.: Comparing anomaly detectors for keystroke dynamics. In: Proceedings of the 39th Annual International Conference on Dependable Systems and Networks (DSN-2009), pp. 125–134, Estoril, Lisbon, Portugal, June 29–July 2, 2009. IEEE Computer Society Press, Los Alamitos, California, 2009.
36. Loy, C.C., Lai, W.K., Lim, C.P.: Keystroke patterns classification using the ARTMAP-FD neural network. In: Proceedings of the International Conference on Intelligent Information Hiding and Multimedia Signal Processing, Taiwan, 2007 (IIHSMSP 2007)
37. Loy, C.C., Lim, C.P., Lai, W.K.: Pressure-based typing biometrics user authentication using the fuzzy ARTMAP Neural Network. In: Proceedings of the International Conference on Neural Information Processing, Taiwan, 2005 (ICONIP 2005)
38. FVC2004—Third International Fingerprint Verification Competition (unibo.it)
39. The Database of Faces (cam-ocr.co.uk)
40. GitHub—massimomauro/FASSEG-repository: Datasets for multi-class and multi-pose face segmentation
41. Yale Face Database (uscd.edu)

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Himanshu Purohit obtained his Bachelor’s degree in Electronics and Communication Engineering from University of Rajasthan, India. Then he obtained his Master’s degree in Communication Engineering and currently pursuing PhD in Signal Processing majoring in Multimodal Biometric authentication, both from BITS Pilani, India. Currently, he is working as Head Corporate Interface, SPSU University, Udaipur, India. His current research interests are Multimodal Biometric Fusion, Cryptography, Artificial Intelligence.

Pawan K. Ajmera received the B.E. in Industrial Engineering degree from the Dr. Babasaheb Ambedkar Marathwada University, Aurangabad, Maharashtra, in 2001. Then obtained the M.E. degree (2005) and Ph.D. degree both from the Swami Ramanand Teerth Marathwada University, Nanded, Maharashtra, in 2012. He has vast academic experience. He is currently working as an Assistant Professor in the Department of Electrical and Electronics Engineering at BITS PILANI, India. His research interests are in signal processing, speech recognitions, biometrics authentication system design, robotics and artificial intelligence.