Array 14 (2022) 100171

Contents lists available at ScienceDirect

Array

journal homepage: www.sciencedirect.com/journal/array

A multi-agent based enhancement for multimodal biometric system at border control

Susara S Thenuwara [a,*], Chinthaka Premachandra [a], Hiroharu Kawanaka [b]

[a] Department of Electronic Engineering, Shibaura Institute of Technology, Tokyo, Japan
[b] Department of Electrical and Electronic Engineering, Mie University, Kurimamachiya, Tsu, Mie, Japan

ARTICLE INFO

Keywords:
Artificial intelligence
Biometrics
Multi-agent system
Border control system

ABSTRACT

Border criminals and unauthorized immigrants are dramatically increasing within the last few years in globally due to the absence of proper authorization methods at the border locations. Usually, passenger controls done by trained immigration officers who compare the passport and the physical appearance at the border while some of the countries done by automated border control (ABC) systems. ABC is one of the applicable real-world applications of the biometric domain which commonly implements with fingerprint and face (multimodal) biometric authorization. However, selecting an appropriate classification method is a challenging task at the decision-making stage. This paper proposes a novel architecture for multimodal biometric authorization engaged with the multi-agent system (MAS) to come up with the optimal solution by using the co-feature of MAS, such as coordination, corporation, and negotiation features. The experiment was done with four available multimodal datasets, namely, the National Institute of Standard Technology (NIST) multimodal, SDUMLA-HMT multimodal, BANCA and PRIVATE databases have been reported to demonstrate the efficiency of the proposed method. The experimental result delivers an excellent performance comparing with previous ABC systems at the authentication phase and computationally fast.

1. Introduction

Biometrics are measures of biological patterns belong to individuals such as fingerprint, iris pattern, voice, and face [1]. Face-biometric and fingerprint can be identified as cost-effective and easy access traits in the biometric domain. It has only become available over the last few years, due to significant advances in the field of computer security [2]. Furthermore, face and fingerprint biometrics do not need to be remembered and cannot be easily lost. This makes it much easier for the user and it cannot be easily stolen or loaned to a friend [3]. Biometric technologies consume those traits and authorize the person for a certain task called biometric authorization systems [4]. There are two types of biometric authentication systems; multimodal and unimodal. Most of the research has been conducted using multimodal systems as it has many improvements over the unimodal systems [4]. Even though there are spoofing attacks on single biometrics, multimodal biometric systems are still placing their strength at the upper level [5]. Passenger flow control using biometric traits can be identified as a significant advancement of the biometric domain [4]. Traditional border control is done by trained immigration officers who compare the passport or travel identity documents and physical appearance of the passenger at the border locations [5]. Rely on the passport face image is a vulnerable factor of the whole authorization process [14]. Due to this loop-hole drugs, frauds, crimes are on the rise in an uncontrollable level. Hence, these threats have severely affected many key sectors in the country, such as national security, finance, and tourism. On the other hand, illegal immigrants are a burning issue in some countries. Therefore, biometrics-based authorization methods are very popular in passenger flow control and significant trend in researchers since the last decade [12].

1.1. Automated border control (ABC)

ABC at the border (e-Gates), is one of the main critical real-world applications in the biometric domain in recent years ([1,8,9]). However, few biometric traits can be used for automated border controls in border locations stated in the International Civil Aviation Organization (ICAO) [1]. There are several organizations responsible for passenger control at border points such as ICAO, IATA, and CEN. These organizations specially ICAO recommend some features of biometric data such

* Corresponding author.
E-mail address: susara@susara.lk (S.S. Thenuwara).

https://doi.org/10.1016/j.array.2022.100171
Received 9 April 2022; Accepted 19 April 2022
Available online 22 April 2022

as image resolution, angle, position, and depth [1]. This research has been conducted with two biometric traits (face and fingerprint) with ICAO recommended standard. Despite that, there was high accuracy of the iris traits in recognition strategy, the combination of fingerprint and face traits deliver reliable results in the time-critical environment due to many reasons such as processing time, sensor cost, capturing time and privacy [8]. Fig. 1 shows the evaluation of the ABC system with a timeline. Evaluation of ABC systems was started with an access control system that can be used for specific user groups and continuously growing with biometrics up to today's eBorder system to handle the unknown risk travelers. Several factors influencing the performance of ABC's dramatically increase during the time frame.

Automated biometric authorization systems are significant advances with engaging the machine learning techniques within the last few years [6]. Even though many classification algorithms deliver high performance at the research level, there are not reliable results in real-world applications such as time-critical environments with large databases [7]. Obtaining a reliable result from one single classification and implement with real-world applications difficult task as it has influenced other factors. Therefore, combining classifiers (multi-classifiers) are more reliable and widely used [9]. However, the optimal choice of the combination method is another difficult task at the decision-making stage [10]. Simply, finding a fusion method for the final adopted version is a difficult process and there is no chance to change the final output after the fusion process is done. The basic idea is behind the strategy is to reach an optimal solution using different classification techniques. That inbuilt testing strategy is a very important part of the multi-classifier technique and the final decision-making process [17]. The balance between false-positive rate (FPR) and false-negative rate (FNR) is the most critical task among those issues [11]. Our approach is to negotiate a strategy using agent-based architecture and come up with an optimal result.

1.2. Issued with existing systems

By considering the existing technology and utilize the ABC system in border following conclusion can be made. Europian Union (EU) e-Gate system rejection rate one out of eight [5] and it may vary in other countries. All rejections transferred to the manual gate with the guidance of immigration control. Sydney Airport reduces 43% automated system after 2012 due to the increase of failure rate as well as privacy cases [2]. However, there are some controllable factors such as quality of biometrics, acceptance, and accuracy of the ABC system, airport logistics, skill rate of immigration officers, and human-machine interface problems. Other factors like passenger awareness and disabilities are not controllable. Traditional automated biometric recognition systems are varying from the ABC system as shown in Table 1. Iris recognition immigration system in the UK (IRIS) and EU e-Gates are good examples for semi-automated ABC systems [5].

1.3. Intelligent multi-agent paradigm

Agent-based architecture interactive with its environment gives dynamic and flexibility as it has a corporation, coordination, and negotiation features at the decision-making stage [34]. In our previous research "Multi-agent approached to face recognition at border control", we used two popular recognition algorithms principal component analysis (PCA) and linear discriminant analysis (LDA) with engaging the multi-agent paradigm to recognize the face (unimodal) and authorize the passenger [13]. However, there are many difficulties in unimodal biometric with a large database in the practical case, hence it was implemented with classical algorithms [6]. To overcome such issues, we proposed a multi-classifier, multimodal, multi-agent-based architecture in this paper. Agents can carry out classification task and a multi-agent concept gives the direction of the final decision of the multi classifier agents [47]. This can be identified as a novel concept to make the decision-making process in biometric authorization systems and it overcomes the inabilities of other combination methods as well as efficient handling problems of the fusion [6]. There are many multimodal biometric recognition systems available at the moment to authorize the persons in different real-world scenarios [8]. However, while maintaining optimum results in time-critical applications are considerably difficult (e-Gates) [2]. Combination of fingerprint and face traits are the main ingredient of our research and relatively applicable when

Table 1
Comparison of biometric recognition and ABC system [1].

Biometric recognition system	The automated border control system
The location of capturing and recognition does not matter.	Capturing and recognition location is matter
Huge noise and different lighting condition in capturing and recognition phases	Less noise and similar lighting condition in capturing and recognition phases
Multiple faces in image many	Only a single face image at a time
Facial expressions, angles are obstacles in the recognition phase	Fewer obstacles in the recognition phase
Find the identity from a large population	Find identity from a small population
More training images	Less training images

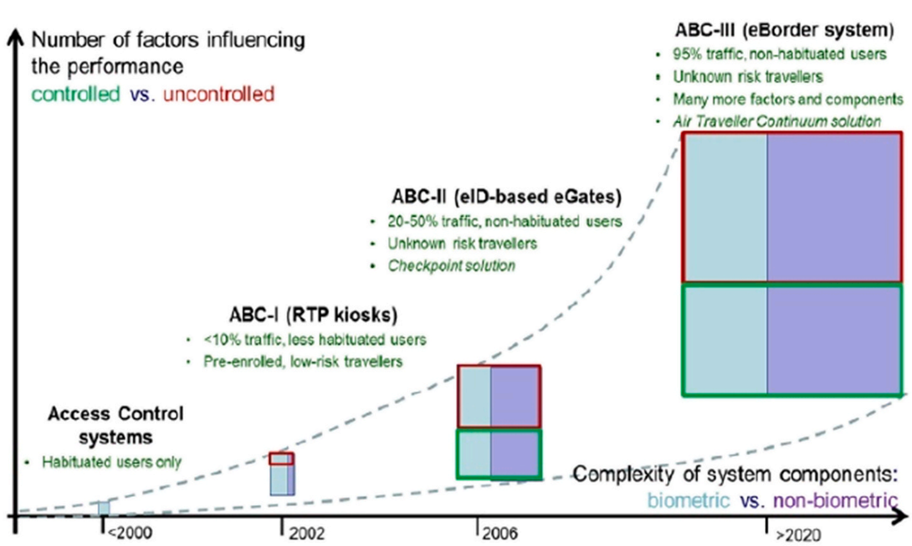

Fig. 1. Evolution of ABC system with a timeline that starts from access control systems to eBoder system [5].

considering other traits such as:

- Availability, the flexibility of the authorization process
- Relatively cheap and easy to adopt
- Universality – in case of disability can use other traits
- Similar class problem-like similar faces like twins [7].

The method we proposed is the agent-based architecture in the final decision-making process of authorization strategy. The individual agents perform as a classification task to identify the biometric traits. The main point is agent could "punish" the other agents with the performance matrix to deliver the optimal result. An intelligent agent is a small computer entity that has negotiation ability, reactive and proactive features [13]. They can communicate with each other using standard protocols as well as make active to deliver the common goal [34]. Fig. 2 shows a basic overview of the agent-based proposed architecture of the multimodal biometric authorization system. The collection of agents (multi-agent) have four mail layers which are:

- Controller layer: This layer waiting for the user biometrics to activate the internal agents. This layer can be deciding the punishment of agents based on communication results to win the common goal.
- Decision layer: This layer makes sure the outputs of all classifier agents after the reasoning done. The basic idea behind this is to search the optimum result and eliminate the other agents.
- Communication layer: This layer responsible for internal communication among the agents. It has a proper action plan during the negotiation process and some decision-making ability of the communication process. However, agents are automatically deciding the current result change or not based on the other agent messages.
- Classifier layer: this layer superintends of classifier algorithm in agents. Agents have different classifiers to recognize the feature of the image.

In this architecture, the confidence level is an important factor in fusion (combine of classifier) while communicating among agents. In this paper, we called it "*confidence level*" and all classifiers are output the confidence level to reach the common goal [49]. The decrease in the confidence level is the sensitivity measure of the testing phase of the proposed method. Furthermore, our main aim is to analyze and

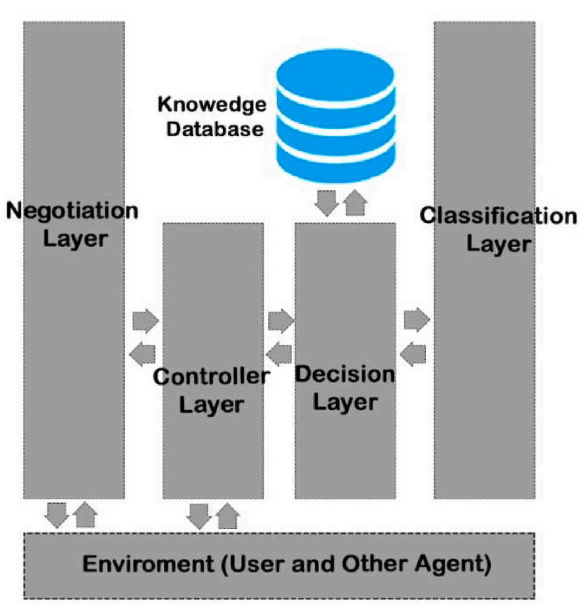

Fig. 2. The basic structure of the agent. The knowledge base has information about other agents.

investigate the sensitivity of the classifier. To evaluate the experiment four databases have been used namely: National Institute of Standard Technology (NIST) multimodal dataset [2], SDUMLA-HMT multimodal database [18], BANCA database [42] and PRIVATE database. Two experiments have been carried out. One for measure and compare the accuracy with previous fusion models and others for comparison with existing ABC system using private dataset.

The contribution of the research as follows:

(1) To the development of a multimodal multi-agent-based passenger authentication system.
(2) Evaluate the proposed system using multimodal publicly available databases and compare it with previous fusion methods.
(3) Evaluate with other ABC systems to analyses the stability of the proposed system.

The remaining sections of the paper organized as follows. Section 2 describes related works. Section 3 delivers the proposed methodology. Section 4 discusses the design and implementation of hardware. Section 5 discusses the experimental results. Finally, conclusions are drawn in section 6.

2. Related work

In the recent past, many researchers have been conducted multimodal biometric research with engaging machine learning algorithms. Our previous research on "Multi-agent approached to face recognition at border control" done with principal component analysis (PCA) and linear discriminant analysis (LDA) fusion model [13] and "Hybrid Approach to Face Recognition System using PCA & LDA in Border Control" [44] done without multi-agent approach. There are many types of research are going on deep learning method to authorize the person autonomously. In the following section, we gave priorities for face and fingerprint biometrics and fusion methods due to some recommendations of ICAO standards for automated passenger flow control systems [1].

Hiren D Jochi presented a multi-agent biometric authentication system for person identification and verification using fingerprint and face recognition (BIOMET) [14]. A fingerprint's unique nature makes it ideal for use in automatic recognition systems. A fingerprint consists of a series of ridges and grooves which unique characteristics. This method used the score level fusion method and face acceptance rate higher than the fingerprint trait. The experiment carried out their database which includes 200 individuals. However, not used public access databases and less amount of dataset size it disadvantages of the method. Furthermore, score level fusion methods more suitable to handle fewer images [13]. El Mehdi Cherrat et al. discussed the Convolutional neural networks (CNN) approach for multimodal biometric identification systems using the fusion of fingerprint, finger-vein, and face images [15]. In this latest research, individual and dual biometric fusion results also presented. CNN with SoftMax won the higher accuracy with SDUMLA-HMT multimodal dataset which contains 41,340 individual traits. The experiment done with only one dataset and used finger vein traits can be considered as disadvantages. Abderrahmane Herbadji et al. have been subjected to combining multiple biometric Traits using asymmetric aggregation operators for improved person recognition [16]. This paper addresses the fusion method (Asymmetric Aggregation Operators) for multimodal biometrics using publicly available databases and compared to score level fusion (min, max, t-norms, symmetric-sum). The experiment shows the multimodal accuracy higher (99.40%) than unimodal systems with asymmetric aggregation fusion technique.

David White et al. discussed passport officers' errors in face matching [19]. The photo id is widely used in the security domain. Passport officers are highly training people who can compare the photo id and physical appearance at the borders. The researchers concluded that passport officers have poor performance at each level. In some cases, they identified accurate results are not related to the length of experience or the training. Finally, they brought forward, “Passport staff misses one in seven fake IDs” in the Australian context. This implies that there is a huge demand in the face recognition domain, and Waldemar Wójcik et al. discussed face recognition: issues, methods, and alternative applications [20]. Face recognition is the most successful application of the image analysis domain and recently getting more attention. All machine learning approaches for face recognition such as an artificial neural network (ANN), conventional neural network (CNN) applicable for extensive training data set, unfortunately, those approaches are inaccurate to model the classes in given only a single or a small number of training samples.

Girija Chetty et al. discussed a multi-agent approach in distributed face recognition [21]. The proposed system contains multi-layer architecture which can achieve high performance in term of the robustness of the complex face recognition system in various visual conditions. The primary objective of the research is further investigation of facial biometrics and its application of video surveillance and crime investigations. At the functional level, it consists of three layers, such as central, neighboring, and remote agents. Skin segmentation, skin region detection, and face fusion agents are responsible for face recognition. The layers are using a popular feature extraction algorithm called principal component analysis (PCA). The system has been developed in a Java framework called ABLE. However, System considers only a face recognition phase with distributed. The flow of the whole system and the communication protocol is unclear in the paper. In addition to that, Rajeev Gupta presented a multi-agent approach to face recognition [22]. The color segmentation, skin region detection, feature extraction, classification can be considered as part of the face recognition system in a distributed way. MAS is giving adequate functionality for such distribution and complex systems. Face images of the same person may different due to aging, expression, makeup, hairstyle, etc. Everyone has a face and ready to display it. This factor is a big advantage over the other biometrics. Proposed system using the agent-based solution for segmentation, skin region, feature extraction, and classification to come up with one emerging solution. However, that proposed system not evaluated with authentic biometric samples and not compared with the traditional system.

Wasim Shaikht et al. reviewed about face recognition using the multi-agent system [23]. The researchers brought forward traditional algorithms were decreased the performance due to illumination. Face tracking and face recognition can be solved by an agent-based solution using JADE (Java Agent Development Environment). Agents are communicating and coordinating with passing Asynchronous messages (ACL) with each other by performing their assigned task of face tracking and face recognition [22]. However, the proposed system not tested and evaluated. Feature extraction alone cannot give accurate results because there are many recognition agents are responsible such as color segmentation, skin area detection, etc. Later, Yanfei Zhu et al. discussed face feature extraction based on agents with a multi-camera System [24]. The proposed system considers each camera as an intelligent agent and it will capture the pose parameters of facial features from the environment. Images collecting from each camera can be better extract the features which can give a solution for false recognition due to angles. Fusion mechanism to find an optimal framework can be considered as the future work of their research. Adrian Kapczyński et al. proposed a simulation model of biometric authentication using a multiagent approach [25]. Multi-modal biometric systems are a concern with different authentication factors, algorithms, and distributed. They use key performance indicators as false acceptance and false rejection rates. Authentication factors are in serial or parallel architecture are consider as research challenges of their work. Finally, Deng Zhang et al. presented a robust intelligent face recognition framework using a GNP-based Multi-agent System [26]. Genetic Network Programming GNP-MAS method gives the highest robustness with compare to GNP-PCA. According to the experimental result, the proposed method came up with higher accuracy than GNP-PCA traditional method.

BIOPASS II Automated biometric border crossing systems based on electronic passports and facial recognition [27] can be considered as the highest accuracy ABC system. It gives more detail about RAPID and SmartGate which utilized with Portugal and Australia. The identification task is done with e-passport and physical appearance at the border (face) and applied in real situations. However, their system implemented in two countries and required prior registration means not sufficient enough to handle the other countries. Spreeuwers et al. evaluated automated face recognition for ABC systems on using actual data in Schiphol Airport [28]. The evaluation of their system given by authors and it shows in high accuracy of (verification rates of 99% at a FAR of 0.1%) with the digital image in passenger passports. Kosmerlj et al. discussed face recognition issues in a border control environment and proposed a system for authorizing passport holders using face identification [29]. They used few databases to analyze their method with Norwegian people and identified few constraints like hair, which can significantly impact with face recognition. They conclude with only unimodal (face) not sufficient to authorize the person at passenger flow control. Kwon and Moon proposed a method for passenger identification using face recognition which utilizes the Public Key Infrastructure (PKI) [30]. They maintain their system with ICAO standards. However, the accuracy of the system not enough to reach the ICAO level. Cantarero et al. presented multi-modal (face and fingerprints) biometric fusion implementation for the ABC system [31]. Their system implemented in Barajas Airport in Spain and shows high applicable for automated gates. Conde et al. done experiments at the same airport to analyze Face recognition in uncontrolled environments [32]. They used surveillance cameras to capture the passenger images in several locations and SVM used as classification. However, their system not sufficient enough to maintain accuracy due to various constraints such as illumination.

H. M. Nguyen et al. presented biometrics fusion with applications in passenger re-authentication for automated border control systems [44]. Their target focuses on face image recognition with cloth features which can be identified as low applicability for ABC systems however the overall accuracy of the system gains higher accuracy (99.20%). Table 2 shows the applicability, performance, cost, authorization delay, and overall performance in our point of view.

After a comprehensive study, we concluded the best approaches for multimodal biometric recognition in a time-critical environment with an intelligent agent-based solution using negotiation protocol. According to the previous researchers, there is a need for a system to authorize the persons using multimodal biometrics in the time-critical environment in an effective way. Therefore, the proposed solution used past researchers' contributions to get an idea about the most suitable algorithms in each step.

3. Proposed methodology

This section focuses on the proposed multi-agent-based multimodal concept. Multi-agent negotiation strategies are first discussed and then the multi-classifier and base classifier in outline. The system includes main three parts such as face and fingerprint capturing, MAS negotiation, and output of the authentication results. First, the images of the face and fingerprints of a passenger is captured. Then the preprocessing is applied to introduce the images to CNN from the captured face images and fingerprints. Then those pre-processed image data is used to detect the identification and authorization of the passengers. The passenger authorization is done by comparing with the previously stored face and fingerprint image data with the currently captured image data using multi-classifiers. In this paper, the selecting a most appropriate result from fusions is done based on a multi-agent method and is the main novelty of this work.

The proposed method occupies four classifiers as an agent and comparison of two classifies done by using error mean which can be obtained after introducing the test data set. Our methodology is based on

Table 2
Overview of ABC system in the literature review.

	Performance	Applicability	Cost	Authorization delay	Overall Performance
Jose Sanchez et al. [1]	Medium	Medium	Medium	High	Medium
H. M. Nguyen et al. [44]	High	Very Low	Medium	Low	Low
FastPass [46]	High	Medium	High	Low	Medium
BIOMET [14]	High	Medium	High	Low	High
BIOPASS II [27]	High	Medium	Medium	High	Very High
El Mehdi Cherrat et al. [15]	High	Medium	High	Medium	Medium
Kwon and Moon [30]	Medium	Low	Medium	High	Low
Conde et al. [32]	High	Low	High	High	Low
Spreeuwers et al. [28]	High	High	Medium	Medium	High
Thenuwara SS [44]	High	Medium	Low	Medium	Medium
Thenuwara SS [13]	Medium	High	Low	Medium	Low
Cantarero et al. [31]	High	Medium	Medium	Medium	High

the testing and evaluation process with fusion methods and assigning punishment to a lower *confidence level.* The advantages of the proposed method can be seen when tested with publicity available four datasets described in the experiment section. The evaluation has been done with majority voting and sum based fusion methods. Fig. 3 shows the basic overview of the proposed system and steps as follows;

Step 1: Capture the face and fingerprint biometrics and preprocess the images.

Step 2: Evaluate the Statistical values from multi-classifiers.

Step 3: Output of the classifiers used to negotiation of the MAS and let it choose an optimal value.

Step 4: Using the optimal value output recognition confidence level with authentication status.

3.1. Multi-agent negotiation strategy

As already mentioned in the introduction section, the *confidence level* is the measurement of performance at the classifier level. The "*confidence level*" used to identify the sensitivity of the classifier at the agent negotiation process in the proposed method. The final decision is drawn after negotiation among recognition agents and knowledgebase using the verification process. Fig. 4 shows the communication flow chart of the multi-agent-based system.

Input interface used for capturing two biometric traits and then preprocessing done before start the classification. Four classifiers have been selected for recognition and verification agents such as Convolutional Neural Networks (CNNs) with SoftMax [15], Support Vector Machine (SVM) [34], Linear Regression (LR) [33], and Radom Forest (RF). Comparison of two classifiers done by statistical significance of error mean of classification rate on test data sets. After that, we evaluate

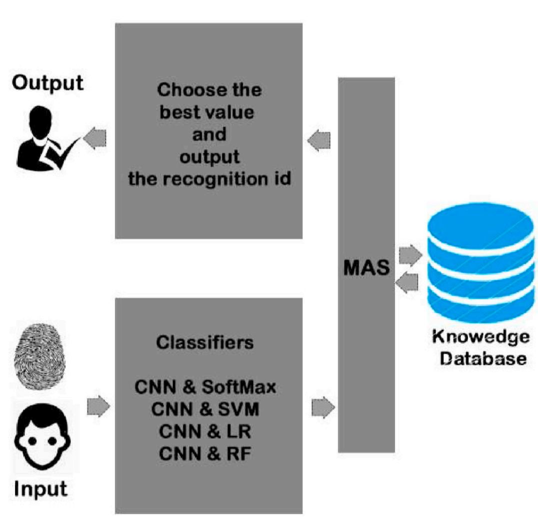

Fig. 3. Overview of the proposed multi-agent-based system.

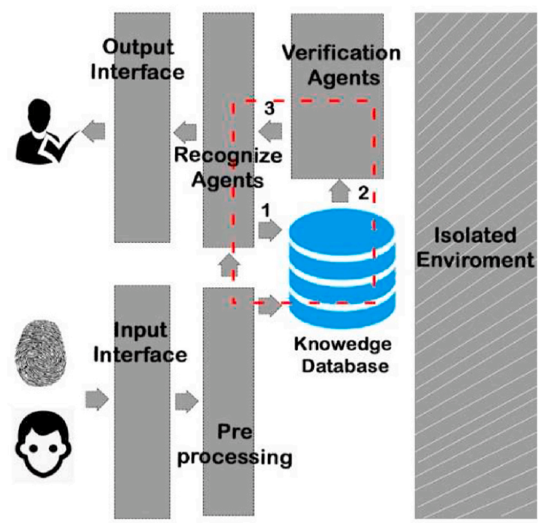

Fig. 4. Proposed multi-agent-based multimodal architecture. Number 1 represent predicted identity send from recognition agents. 2 represent verification input from knowledgebase and 3 represents verification output.

the p-values using a *t*-test to measure the degree of confidence. Next section stepwise describes the negotiation part of the multi-agent system in between verification agents, recognition agents, and knowledge base which represented in a red color square in Fig. 4. The output interface used to display the authentication message to the passenger to proceed with the next step of the immigration process.

All agents agreed to train the classifier and negotiate the result for the testing phase. The main idea of the process is assigned "punishment" based on the output of the recognition agents [39]. Classifier level action plan can be illustrated as follows:

Step1: Start the training process of all classifiers and calculate the training mean value for each classifier.

Step2: Start the negotiation process by comparing the measured values and calculate the punishment using equation (1). (to decline their level of confidence).

- Rank the difference between the test pattern and training mean for all classes
- Loop the following task for first N attributes
  a. Select one agent and let it select another one for punish.
  b. Check the class allocated to this attribute by the attacked agent, and the sensitivity of the appropriate classifier.
  c. Obtain the output of verification agents and they will produce "Yes" if the test sample correctly verified otherwise "No".
  d. Send the other agent a message proposing penalty by raising the agent's confidence level

Step3: Complete the negotiation process and the overall result takes from the highest confidence level with the recognition agent. It is the most suitable one for classify test patterns [40].

Fig. 5 shows the flowchart of the overall punishment-based negotiation process of the proposed method.

The agent punishment is a cyclic process and once the agent sends the message to downgrade the *confidence level* and receiver agent send back the punishment on the sender agent [48]. Likewise, this process has cyclic behavior until found the non-negative *confidence level.* A higher difference between the training mean and test pattern will higher chance to get a weak classifier [36]. The *confidence level* will decrease if there is not match with knowledgebase while monitoring using the verification level. Considering this autonomy punishment can be express as following Equation (1). Observed Significant Level (*P*-value) estimate by the degree of confidence result and used it like 95% which can consider the statistical difference when p-value lower than 0.05. We used the sum-based and majority vote-based fusion technique to evaluate the overall process.

$$Punishment_{\ i} = \frac{Dif_i \ \times Sen_i}{R_i \times \ L_n(N_{verfified\ ``NO"}) \ \times Rank} \tag{1}$$

where:

- Dif: Difference between test pattern i and training mean
- Sen: Sensitivity of ith pattern
- R: Rank of the ith and training mean
- Ln: Natural logarithm of output “no”
- Rank: Classifier rank factor

There is a threshold value during the cyclic behavior to change the individual agent’s result when it over the punishment value. Therefore, the agent can decide on an alternative path to reach the outcome. In Equation (1) natural logarithm used for non-negative from verification classifiers. The agent-based architecture developed with a Python-based multi-agent platform [35].

3.2. Multi-classifiers

Convolutional Neural Networks (CNNs) with SoftMax [15], Support Vector Machine (SVM) [34], Linear Regression (LR) [33], and Radom Forest (RF) are used as multi-classifiers. CNN has been used as a base that is under the supervised learning model. We did not train the models from scratch to develop the face and fingerprint CNN model. Visual Geometry Group (VGG) at Oxford University released the VGGNet model and there are two deep learning models VGG16 and VGG19. VGG19 network not practical this application due to a massive number of parameters and joint representation [26]. Here, the VGG 16 pre-trained model has been used, and lasts fully connected layers are replaced by a new one and the first four blocks in VGG16 wt were frozen. Sixteen weighted layers contain in VGG16 and achieved an accuracy of 93.44% with the ImageNet database [18]. Fig. 6 shows the structure of VGG16.

Finally, using these four classifications and multi-agent-based structures as well as using different datasets will deliver a fascinating result for real-time application. The next section illustrates two experiments in detail.

3.2.1. Data preprocessing

Data preprocessing is an important stage before the classification process. Image resizing and data augmentation has been done as two preprocessing techniques [37]. All images resized 224 × 224 pixels to be suitable for the VGG16 model and augmentation techniques used to rotate the face images [38].

3.3. Computational complexity

The computational complexity of the optimal value is mainly determined by the solution process. Consider the multi-agent model architecture shown in Fig. 5 for the negotiation process. The cost of a message communication can be calculated as follows:

$$Com_{\ i} = \delta \ \ \mathrm{x(p)} \ \ \mathrm{x} \ \ (\ \ \mathrm{Ttrasm}) + \beta \tag{2}$$

where δ: number of identification messages; p: punishment; Ttrasm: transmission time to send a data, β: message latency in the etwork.

Maximum Q value select as follows.

$$a_{\ i} \ = \mathrm{argmax} Q(si, ai) \tag{3}$$

$$s_{\ i} \ = [M, p1, p2, p3, \ldots\ldots] \tag{4}$$

Set Q-learning parameters α, λ, w, r_{ref}

Set MAS motion model parameters r_c, c^{α}, c^{γ}

Set other parameters r_s, m, n, N, etc.

Create state space, behavior space and Q-value.

Set the maximum training times for training data set N_T.

Initialize the value of each agent and state s, action selected by random agents.

While (Q maximum update after punishment) do.

For each agent i.

Calculate the value of last state-action r(si, ai).

Calculate state s′ i.

Update the p-value 3).

Calculate and Select action a′i using (4).

Update the state and action: si = s′i, ai = a′

End For.

End WhileThe Q-Traversal algorithm has a computational complexity of querying a list and finding the maximum Q-value in action space. In fact, many comparison operations are used in list queries and maximum searches after punishment applies. The length of the list and

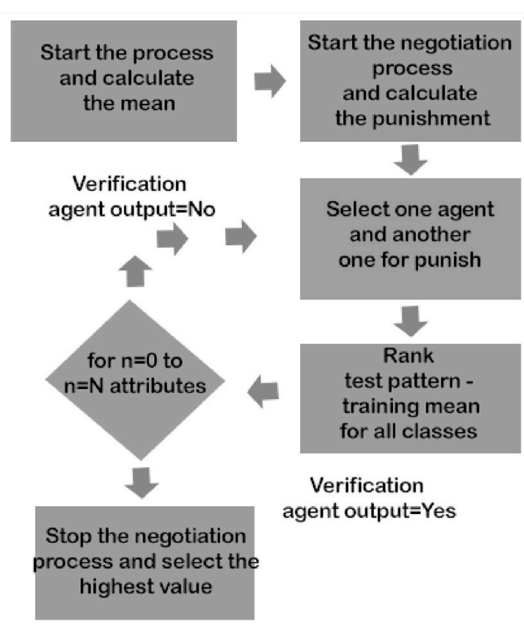

Fig. 5. The negotiation process of the proposed multi-agent-based method.

Fig. 6. VGG16 layer structure.

the type of comparison data define the number of comparisons.

4. Experiments

This section describes the main component of experimental analysis such as experimental data, protocol, result, and comparison of the proposed method. There are two experiments done: Experiment 1: to measure the accuracy of the proposed model with a large dataset and compare with other fusion methods, Experiment 2: to compare with previous ABC systems using the private dataset (D). The preprocessed has been done before the experiment to maintain the guidelines of the ABC process [1].

4.1. Experimental data

Dataset A, Dataset B, Dataset C, and Dataset D represent as National Institute of Standard Technology (NIST) multimodal dataset [2], SDUMLA-HMT multimodal database [18], BANCA database [42] and PRIVATE database respectively in our discussion section. Data preprocessing has been done to maintain the ICAO standards [1]. Therefore, data augmentation and resizing have been applied for images. 224 × 224 pixels images are most suitable for VGG16 and augmentation methods (rotation and flipping) used for face images.

- Dataset A: National Institute of Standard Technology (NIST) released BSSR1 multimodal dataset for research purposes. In this dataset fingerprint, iris, and face images are linked together to identify the individuals. All individuals are formally consented to use their biometrics to advance research purposes [2]. This data gathered during Nail to Nail Fingerprint Challenge [8] from several hundreds of people. Front angle face images and fingerprints (lift and right) have been selected.
- Dataset B: SDUMLA-HMT Shandong University released a multimodal trait database including face images in seven angles, fingerprint, finger vein, and iris from 106 individuals [18].
- Dataset C: BANCA is multimodal biometric database [42].
- Dataset D: PRIVATE dataset that we created for our last biometric-based authorization research which updated with fingerprint and face from 450 students in the university. This dataset uses for practical test the authorization process in our laboratory.

These three databases (A, B, and C) and different classifiers engaging with a multi-agent paradigm show absorbing results for the proposed automated multimodal biometric system. In the next section, we will discuss the experimental protocol. The four multimodal datasets include 88,430 individuals' traits and divided into training, testing, and validation as shown in Table 3.

4.2. Experimental evaluation protocol

To make the evaluation process, four datasets have been divided into tearing, testing, and validation as shown in Table 4. The performance accuracy measure with the following Equation (3). Sensitivity and specificity represented in Equations (4) and (5) respectively. True positive (TP) is correctly recognized that authorized person, the true negative (TN) is not correctly recognized authorized person, False positive (FP) is unauthorized recognized and false-negative (FN) is an unauthorized person not recognized over the total number of tests. The accuracy rate of the classification rate used to compare the two classifiers [18] and datasets was implemented in alphabetical order.

Table 3
Multimodal datasets (fingerprint and face).

	Dataset A (NIST BSSR1)	Dataset B (SDUMLA-HMT)	Dataset C (BANCA)	Dataset D (PRIVATE)
No. of Images	45,990	33,540	8450	450

Table 4
Multimodal datasets (fingerprint and face).

$$Accureccy = \frac{True\ Positive + True\ Negative}{True\ Positive + True\ Negative + False\ Positive + False\ Negative} \tag{3a}$$

$$Sensitivity = \frac{True\ Positive}{True\ Positive + False\ Negative} \tag{4a}$$

$$Specificity = \frac{True\ Negative}{True\ Negative + False\ Positive} \tag{5}$$

	Dataset A (NIST BSSR1)	Dataset B (SDUMLA-HMT)	Dataset C (BANCA)	Dataset D (PRIVATE)
No. of Images	45,990	33,540	8450	450
Training	30,792	26,832	5070	270
Validation	4599	3354	1690	90
Test	4599	3354	1690	90

4.3. Experimental results (Experiment 1)

Before engaged with multi-agent, we tested other classifiers individually (face and fingerprint) with four datasets. Table 5 shows the different classifier results with the CNN model. Fingerprint trait shows the highest accuracy of 99.66% engaging with SoftMax classifier and SVM is the highest accuracy classifier for face biometric engage with CNN base model.

The next step is finding the result of fusion and negotiation-based strategy with multimodal. Table 6 shows the standard deviation of four classifiers at recognition and verification stages using four datasets. Verification classifiers deliver good results than recognition classifies as we expected. Results showing SoftMax and SVM classifiers make better outcomes than others. Results show more similar comparing to different classifiers.

However, after applying the multi-agent negotiation method and other fusions techniques results shows in Table 7. It shows a significant improvement of the negotiation method than sum and vote based technique for all datasets.

As we already mentioned unimodal systems are vulnerable to attackers, therefore our aim is a fusion method, not individual biometric accuracy. Receiver Operating Characteristic curve (ROC) used to compare different classifiers in general with each dataset [43]. The shape of the curve contains useful information. Figs. 7 and 8 represents the ROC curves of different classifiers with four datasets respectively. Ideal classifier should go through the origin (0, 0), the top-left corner (0, 1) and the top-right corner (1, 1). The proposed method shows in the red curve and it very close to ideal with dataset A and another significant improvement with other datasets as well.

4.4. Comparison with previous fusion methods

The following part is a very important result of our proposed system. The majority of researchers are done biometric authorization systems using iris and other highest-level traits [15]. However, we unable to use some biometric traits as already mentioned in this paper (ICAO Standard). Therefore, we compare our proposed method with face and fingerprint authorization systems other researchers have done. The accuracy of the proposed system compared and revived with other multimodal systems in our literature [13,15,16] in Table 8. Accuracy is more similar to three multimodal (fingerprint, finger vein, and face) that have been proposed by El Mehdi Cherrat et al. [15]. However, finger vein traits are not recommended to use for passenger flow control due to privacy and cost [1]. Computational time is a very important

Table 5
Different classifier accuracy (%) results with unimodal biometrics.

	Dataset A		Dataset B		Dataset C		Dataset D	
Classifiers	Face	Fprint	Face	Fprint	Face	Fprint	Face	Fprint
CNN & SoftMax	99.36	99.66	98.57	98.99	97.45	99.45	99.58	99.47
CNN & SVM	99.56	99.45	99.11	99.12	98.45	98.55	99.50	99.44
CNN & LR	99.25	99.47	99.47	99.24	98.41	98.74	98.98	98.77
CNN & RF	99.35	99.55	98.47	98.66	98.66	97.66	99.45	98.66

Table 6
Error results of individual classifiers.

Classifiers	Dataset A		Dataset B	
	Recognition	Verification	Recognition	Verification
CNN & SoftMax	10.12% ∓ 2.41	09.62% ∓ 3.41	10.77% ∓ 2.89	09.22% ∓ 3.41
CNN & SVM	11.12% ∓ 2.58	09.12% ∓ 2.96	12.12% ∓ 2.36	09.12% ∓ 3.55
CNN & LR	12.12% ∓ 2.63	09.10% ∓ 2.81	13.52% ∓ 2.58	09.12% ∓ 3.41
CNN & RF	13.12% ∓ 2.44	09.02% ∓ 2.51	12.72% ∓ 2.62	09.12% ∓ 3.21
	Dataset C		**Dataset D**	
Classifiers	Recognition	Verification	Recognition	Verification
CNN & SoftMax	11.52% ∓ 2.41	09.22% ∓ 2.47	11.18% ∓ 3.91	09.55% ∓ 3.42
CNN & SVM	10.12% ∓ 2.51	08.52% ∓ 2.54	11.42% ∓ 3.47	09.98% ∓ 2.49
CNN & LR	11.12% ∓ 3.71	09.82% ∓ 2.25	12.62% ∓ 3.81	09.25% ∓ 3.61
CNN & RF	12.12% ∓ 3.41	09.57% ∓ 3.41	12.12% ∓ 3.21	09.82% ∓ 2.33

Table 7
Fusion technique results.

Fusion Technique	Dataset A	Dataset B
Proposed Multi-agent	4.42% ∓ 2.41	4.77% ∓ 2.41
Sum Based	9.22% ∓ 2.56	08.12% ∓ 2.41
Majority Vote	11.12% ∓ 2.61	10.52% ∓ 2.41
	Dataset C	**Dataset D**
Proposed Multi-agent	4.18% ∓ 3.99	3.55% ∓ 3.42
Sum Based	9.42% ∓ 3.45	8.98% ∓ 2.49
Majority Vote	12.62% ∓ 3.71	11.25% ∓ 3.61

measurement of passenger flow control systems [2]. Furthermore, Table 8 shows the comparison of time consumption with different fusion methods [15,45]. The proposed method shows less computational time than other fusion methods with all datasets.

4.5. Comparison with existing ABC systems (Experiment 2)

In our research, comparing with fusion methods is not enough therefore in this section describes the comparison with few available ABC systems to measure the overall performance. Experiment 2 carried out with two stages, the first stage collects the face and fingerprint

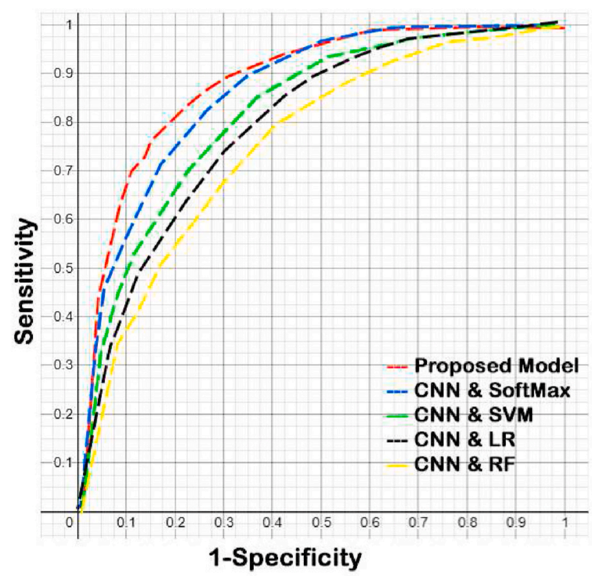

Fig. 8. ROC curves different classifiers dataset C.

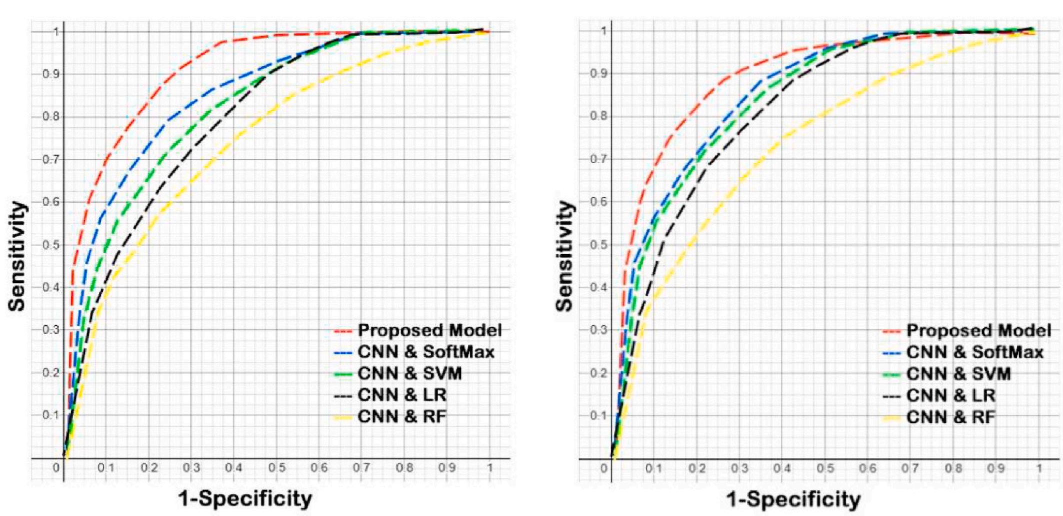

Fig. 7. ROC curve different classifiers dataset A (left) and dataset B (right).

Table 8
Accuracy and computational time compared with proposed system.

Algorithms	Dataset A		Dataset B	
	Accuracy (%)	Time (ms)	Accuracy (%)	Time (ms)
ALGO1	99.49	79	91.34	97
ALGO2	99.31	480	93.33	345
ALGO3	99.40	560	92.33	456
ALGO4	96.00	78	91.04	88
ALGO5	99.62	62	95.52	67
	Dataset C		**Dataset D**	
Classifiers	Accuracy (%)	Time (ms)	Accuracy (%)	Time (ms)
ALGO1	89.49	79	89.25	79
ALGO2	78.37	450	78.36	580
ALGO3	77.44	480	77.41	340
ALGO4	89.55	88	90.00	77
ALGO5	90.12	90	90.62	70

ALGO1 - Fingerprint $_{ANN}$ & Fingervein $_{ANN}$ & Face $_{ANN}$ [15].
ALGO2 - Fingerprint $_{CNN}$ & face $_{CNN}$ [15].
ALGO3 - Multimodal Asymmetric Agg Operators [16].
ALGO4 - Our Previous Research Thenuwara SS [13].
ALGO5- Proposed Multi-agent-based fingerprint $_{CNN}$ & face $_{CNN}$.

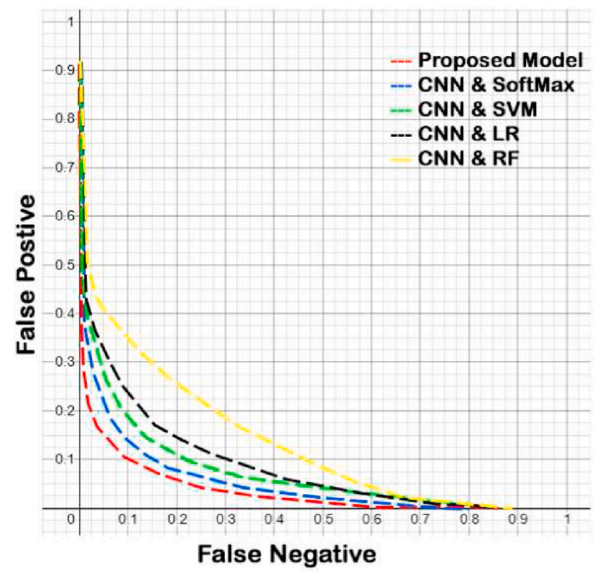

Fig. 9. ROC curves FP and FN rates with different classifiers using dataset D.

biometrics using 450 students and authorization done by the second stage. This experiment was done with Intel Corei7 Processor, 8 GB Ram, and Nvidia GeForce GTX 880 CPU in 64 Bit Ubuntu 16 Environment. Logitech HD QuickCam and AFS 510 USB scanner used for capturing face image and fingerprint respectively. Table 9 shows the comparison of ABC systems with the proposed model by examining the computational cost, security, and accuracy proposed model exceedingly applicable for the ABC system. Purpose of the dataset D is to measure the FN and FP rates in real-time border control like the environment in our laboratory.

The balance between false negative and false positive is very important and Fig. 9 shows significant improvement of the proposed method. Table 9 shows an application-wise comparison with other ABC systems. The final comparison was done with selected ABC systems (accuracy more than 96%) by considering the major components in the system [1] from their research paper. Accuracy refers the ability of correctly identify the live sample, applicability refers to how overall system capacity of using biometric recognition task, cost refers to implementation and sensor costs by capturing and identification phases, authorization time refers to average system time taken for identifying the biometric traits, security refers to use lower-level unimodal biometrics which already identified vulnerable to spoofing attacks and usability refers to how the flexibility of the overall ABC system. In 2012 BIOMET [33] has been developed for passenger flow control with 98% accuracy. They used to face and fingerprint fusion and applicability is low as they already mention that capacity of the system is low. Cost, time, and security very low due to cost-effective biometrics [7]. Security can be considerably low as feature level fusions already vulnerable to attackers and overall medium usability of the system. BOPPASSII [27] and Spreeuwers et al. [28] showed a higher accuracy of 99.45% and 99% with information about SmartGate ABC systems already implemented in Australia and Portugal. Both systems have a lot of user comments regarding the flexibility and recognition time on survey results [4]. Furthermore, Spreeuwers et al [28] system commonly known as Frontex, and it was acquiring high costs at the implementing stage as well as higher time delay at authorization [1]. El Mehdi Cherrat et al. [15] and Nada Alay et al. [18] are presented a research-level ABC system with an accuracy of 99% and 98.72% respectively. Both systems have higher accuracy with lower applicability for ABC systems hence they used finger-vein as modalities [1]. Therefore, both types of research are not significantly useable as automated passenger flow control. Spanish ABC [6] system inaugurated in late May 2010 and implemented in Barajas and El Prat airports. The main disadvantage of the system is if either facial or fingerprint fail to recognize, the system considered the traveler authentication process unsuccessful. Therefore, applicability and usability can be considered as lower than other systems as it already outdated [29,41]. We have done two previous research engage with unimodal biometrics with and without a multi-agent approach [13,44] which encourage us to do a multimodal multi-agent approach. Both types of research are accurate and security-wise lower than others. however, our target is to achieve low cost and high applicable ABC system. Finally, we decided to use multimodal traits that capable of higher security as well as a considerable cost-effective model. The proposed system capable of handling large datasets as well as higher accuracy range compares to BIOMET and BIOPASS II.

Finally, we can conclude that our multimodal multi-agent system is more appropriate and reliable for real-world passenger flow control with maintaining the standards because:

Table 9
Comparison with other ABC systems.

	Accuracy %	Applicability	Cost	Authorization Time	Security	Usability
BIOMET [14]	98.74	Low	Low	Low	Low	Medium
BIOPASS II [27]	99.45	Medium	High	High	Low	High
Spreeuwers et al. [28]	99.00	High	High	High	High	High
El Mehdi Cherrat et al. [15]	99.49	Low	High	Medium	High	Very Low
Nada Alay et al. [18]	98.72	Low	Medium	High	Low	Medium
Spanish ABC [6]	96.61	Low	High	High	Low	Low
Our Previous Research 1 [13]	96.00	Medium	Low	High	Low	Medium
Our Previous Research 2 [44]	98.00	Medium	Low	High	Low	Low
Proposed Multi-Agent	99.62	High	Low	Medium	High	High

- The proposed enhanced method recognition rate higher than other latest multimodal authorization systems especially face and fingerprints.
- The proposed method shows the less computational time for fusion as it used the negotiation paradigm. Time is a very important factor in border control matters.
- The balance between FPR and FNR are favorable.
- CNN is a deep learning method and it could handle a large number of passenger databases who register with the e-Gate system.
- The sensor device cost is relatively lower than other higher-level biometric capturing devices. And also capturing time is lesser than others.
- We can address the distributed level biometric authorization system as well as task-related agents that can be adaptable.

5. Conclusion

A system for passenger flow control using multimodal biometrics with the enhancement of an intelligent agent-based paradigm has been introduced in this paper. The negotiation strategy is the principal concept of the proposed method and it is relatively similar to a human-based decision-making task. The individual agent responsible for the recognition task is a novel concept of an automated biometric authorization domain. The agent-based system improves the quality of the decision-making process than other fusion methods as shown in the results. The experimental result of the proposed method has shown overall accuracy, performance and computational time are preferable than other multimodal authorization systems. Furthermore, the proposed method improved, acceptable and reliable results than other ABC systems. It implies that protentional benefits can be harvest from allowing a negotiation strategy among intelligent agents. Furthermore, the proposed method used ICAO standard biometrics (face and fingerprint) which relatively cost-effective than others. For future study, enhance the proposed passenger flow control system with engaging the robotic operating system (ROS) and against spoofing attack is a task worth investigating.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] Sanchez del Rio Jose, Moctezuma Daniela, Conde Cristina, Martin de Diegoa Isaac, Cabelloa Enrique. Automated border control e-gates and facial recognition systems. Comput Secur J 2016;62:49–72.

[2] Yang Xin, Kong Lingshuang, Liu Zhi, Wang Chunhua, Zhu Hongliang, Gao Mingcheng, Zhao Chensu. Multimodal feature-level fusion for biometrics identification system on IoMT platform. IEEE Access 2018;6.

[3] Gomez-Barrero Marta, Rathgeb Christian, Ulrich Scherhag, Busch Christoph. Predicting the vulnerability of biometric systems to attacks based on morphed biometric information. IEEE IET Biometr J 2018;7.

[4] Orteg David, Fernández-IsabelIsa Alberto, de Diego Martín, Conde Cristina, Cabello Enrique. Dynamic facial presentation attack detection for automated border control systems. Comput Secur J 2020;92.

[5] Gorodnichy D, Yanushkevich S, Shmerko V. Automated border control: problem formalization, IEEE symposium series in computational intelligence (SSCI 2011). 2015.

[6] Daniel Cuesta Cantarero; David Antonio Pérez Herrero; Fernando Martín Méndez, A multi-modal biometric fusion implementation for ABC systems, **2013** *European Intelligence and security informatics conference*.

[7] Robertson Joshua J, Guest Richard M, Elliott Stephen J, O'Connor Kevin. A framework for biometric and interaction performance assessment of automated border control processes. IEEE Trans Human Machine Syst J 2017;47(6).

[8] Tsutomu M, Hiroyuki M, Koji Y, Satoshi H. Impact of artificial gummy fingers on fingerprint systems. Int J Opt Secur Count Deter Technol 2002;4677(IV):275–89.

[9] Kwon Taekyoung, Moon Hyeonjoon. Biometric authentication for border control applications. IEEE Trans Knowl Data Eng J 2008;20(Issue 5).

[10] Eastwood Shawn C, Shmerko VP, Yanushkevich SN, Dr M, ahansky, Gorodnichy DO. Biometric-enabled authentication machines: a survey of open-set real-world applications. IEEE Trans Human Machine Syst J 07 May 2015;46(Issue): 2.

[11] Dmitry O. Gorodnichy, multi-order biometric score analysis framework and its application to designing and evaluating biometric systems for access and border control, IEEE *symposium Series in computational intelligence (SSCI 2011)*, workshop on computational intelligence in biometrics and identity management (CIBIM). Paris – France; 11-15 April 2011.

[12] Labati Ruggero Donida, Genovese Angelo, Muñoz Enrique, Piuri Vincenzo, Scotti Fabio, Sforza Gianluca. Automated border control systems: biometric challenges and research trends. International Conference on Information Systems Security; 2015.

[13] SS Thenuwara and AS Karunananda Department of Computational Mathematics, University of Moratuwa. Sri Lanka. Multi-agent approach to face recognition in border control. General Sir John Kotelawala Defence University; 2013. *to 2017 International Research Conference*. http://ir.kdu.ac.lk/handle/345/2282.

[14] Hiren D. Joshi phd, dept. Of computer science. BIOMET: a multimodal biometric authentication system for person identification and verification using fingerprint and face recognition. 0975 –8887 Int J Comput Appl 2012;51. No.17.

[15] Cherrat El, Alaoui R, Bouzahir H. Convolutional neural networks approach for multimodal biometric identification system using the fusion of fingerprint, finger-vein and face images. PeerJ Comput Sci J 2020;6. e248 , 2020.

[16] Herbadji A, Akhtar Z, Siddique K, Guermat N, Ziet L, Cheniti M, Muhammad K. Combining multiple biometric traits using asymmetric aggregation operators for improved person recognition. Symmetry 2020;12:444.

[17] Sun Yunlian, Zhang Man, Sun Zhenan, Tan Tieniu. Demographic analysis from biometric data: achievements, challenges, and new frontiers. IEEE Trans Pattern Anal Mach Intell 2017;40(Issue):2.

[18] Nada Alay, Heyam H, Al-Baity. A multimodal biometric system for personal verification based on different level fusion of Iris and face traits. Bioscience Biotechnology Research Communications Journal 2019;12. Number 3.

[19] White David, Kemp Richard I, Jenkins Rob, Matheson Michael, Mike Burton A. Passport officers' errors in face matching. Sydney, Australia: School of Psychology, The University of New South Wales; 2014.

[20] Waldemar Wójcik, Konrad gromaszek and muhtar junisbekov **2016** face recognition: issues, methods, and alternative applications Institute of electronics and information technology, Lublin University of Technology, Lublin, Poland.

[21] Girija chett and dharmendra sharma **2006** distributed face recognition: a multi-agent approach. School of Information Sciences and Engineering, University of Canberra, *Australia IJCSNS International Journal of Computer Science and Network Security*; 2006. OL.6 No.8A.

[22] Gupta Rajeev. Multi-agent approach towards face recognition. M.M. Institute of Computer Technology & Business Management Maharishi Markandeshwar University; 2011.

[23] Shaikh Wasim, Shinde Hemant, Sharma Grishma. Face recognition using multi-agent system. Int J Comput Sci Eng 2016;4(4).

[24] Zhu 1 Yanfei, Ruan Qiuqi. Face Feature Extraction Based on Agents with Multi-camera System International Journal of Information and Computer Science 2012; (2):34–8. 2012, IJICS Volume 1PP.

[25] Kapczyński Adrian, Owczarek Tomasz. Simulation model of biometric authentication using multiagent approach. J Telecommun Inf Technol 2010;6.

[26] Deng Zhang, Mabu Shingo, Hirasawa Kotaro. A robust intelligent face recognition framework using GNP-based multi-agent system. SICE Annual Conference 2011; 13–18:2011. 2011, September.

[27] BIOPASS II Automated biometric border crossing systems based on electronic passports and facial recognition: RAPID and SmartGate, Tech. rep., agency, European cooperation, operational borders, external states, Member Union, European.

[28] Spreeuwers LJ, Hendrikse AJ, Gerritsen KJ. Evaluation of automatic face recognition for automatic border control on actual data recorded of travelers at Schiphol Airport. Proceedings of the international conference of the Biometrics Special Interest Group (BIOSIG), 2012 BIOSIG 2012:1–6.

[29] Kosmerlj M, Fladsrud T, Hjelm E. Face recognition issues in a border control environment. In: David Ahang AKJ, editor. Advances in biometrics lecture notes in computer science. Hong Kong: Springer Berlin Heidelberg; 2006. p. 33–9.

[30] Kwon T, Moon H. Biometric authentication for border control applications. IEEE Trans Knowl Data Eng 2008;20:1091–6.

[31] D.C. Cantarero, D.A.P. Herrero, F.M. MendezA Multi-modal biometric fusion implementation for ABC systems, **2013** *European Intelligence and security informatics conference* 277–280.

[32] Conde C, Martin de Diego I, Cabello E. Face recognition in uncontrolled environments, experiments in an airport, e-business and telecommunications. Commun Comput Inform Sci 2011;314:20–32.

[33] Garcia-Salicetti S, et al. BIOMET: a multimodal person authentication database including face, voice, fingerprint, hand and signature modalities. In: Kittler J, Nixon MS, editors. Audio- and video-based biometric person authentication. AVBPA 2003. Lecture notes in computer science, vol. 2688. Berlin, Heidelberg: Springer; 2003.

[34] Marjory Cristiany Da Costa Abreu. Analyzing the benefits of a novel multiagent approach in a multimodal biometrics identification task. IEEE Syst J 2009;3(4).

[35] Stephen Knoxa, MeierJimYoon Philipp, Harou cJulien J. A python framework for multi-agent simulation of networked resource systems. ScienceDirect Journal 2018;103:16–28.

[36] Malcolm Reida Elhadi M.Shakshukia. Implementing a multi-agent system for recording and transmitting biometric information of elderly citizens **2017**. The 7th International Conference on Current and Future Trends of Information and

Communication Technologies in Healthcare (ICTH 2017), Volume 113, Pages 334-343.
[37] Gunasekaran K, Raja J, Pitchai R. Deep multimodal biometric recognition using contourlet derivative weighted rank fusion with human face, fingerprint and iris images. Automatika Science Direct Journal 2019;60(3):253–65.
[38] Mohite Ayusha, Gamare Shruti, Karan, Patil Nita. International Research Journal of Engineering and Technology (IRJET) 2019;(6 Issue).
[39] Patil Abhijit, Kruthi R, Gornale Shivanand. Analysis of multi-modal biometrics system for gender classification using face, Iris and fingerprint images. J. Image, Graphics and Signal Processing 2019;5:34–43.
[40] Park Eunsoo, Kim Weonjin, Li Qiongxiu, Kim Jungmin, Kim Hakil. Fingerprint liveness detection using CNN features of random sample patches. International Conference of the Biometrics Special Interest Group (BIOSIG) 2016:321–8.
[41] Cockell R, Halak B. On the design and analysis of a biometric authentication system using keystroke dynamics. Cryptography 2020;4:12.
[42] Rane M, Latne T, Bhadade U. Biometric recognition using fusion. In: Kumar A, Paprzycki M, Gunjan V, editors. ICDSMLA 2019. Lecture notes in electrical engineering, vol. 601. Singapore: Springer; 2020.
[43] Walia GS, Rishi S, Asthana R, Kumar A, Gupta A. Robust secure multimodal biometric system based on diffused graphs and optimal score fusion. IET Biom 2019;8(4):231–42.
[44] Thenuwara SS, Premachandra C, Sumathipala S. "Hybrid approach to face recognition system using PCA & LDA in border control," 2019 national information technology conference (NITC), colombo. Sri Lanka; 2019. p. 9–15. https://doi.org/10.1109/NITC48475.2019.9114426.
[45] Nguyen HM, Rattani A, Derakhshani R. Biometrics fusion with applications in passenger Re-authentication for automated border control systems. Woburn, MA, USA: 2019 IEEE International Symposium on Technologies for Homeland Security (HST); 2019. p. 1–7. https://doi.org/10.1109/HST47167.2019.9032968.
[46] Clabian Markus, FastPass - Automated Border Control as Challenging Combination of Various Security Technologies. IH&MMSec '14: *Proceedings of the 2nd ACM workshop on Information hiding and multimedia security*. 2014.
[47] Zhang X, Chang Z, Wang Y. Multi-model method decentralized adaptive control for a class of discrete-time multi-agent systems. IEEE Access 2020;8:193717–27. https://doi.org/10.1109/ACCESS.2020.3030635.
[48] Palanca J, Terrasa A, Julian V, Carrascosa C. SPADE 3: supporting the new generation of multi-agent systems. IEEE Access 2020;8:182537–49. https://doi.org/10.1109/ACCESS.2020.3027357.
[49] Bei X, Liu S, Poon CK, et al. Candidate selections with proportional fairness constraints. Auton Agent Multi-Agent Syst 2022;36:5. https://doi.org/10.1007/s10458-021-09533-7.