International Journal on
"Technical and Physical Problems of Engineering"
(IJTPE)
Published by International Organization of IOTPE

ISSN 2077-3528
IJTPE Journal
www.iotpe.com
ijtpe@iotpe.com

March 2024 | Issue 58 | Volume 16 | Number 1 | Pages 63-72

ENHANCED SURVEILLANCE SYSTEM: MASKED FACE RE-IDENTFICATION USING CLOUD COMPUTING AND DEEP LEARNING

A.J. Jalil [1] E.A. El Seidy [2] S.S. Dauod [2] N.M. Reda [2]

1. Department of Computer Science, Faculty of Computer Science and Information Technology, University of Basrah, Basrah, Iraq, alyaa.jalil@uobasrah.edu.iq
2. Department of Mathematics, Faculty of Science, University of Ain Shams, Cairo, Egypt
essamelseidy@sci.asu.edu.eg, samehdaoud@sci.asu.edu.eg, naglaa_reda@sci.asu.edu.eg

Abstract- The spread of Covid-19 virus, and the growth of suspicious people existence, raised the difficulty of securing public enterprises and pivotal organizations. In order to limit infection and prevent intruders from entering, the availability of qualified monitoring systems has become necessary. This paper proposes a surveillance system based on Cloud computing that observes people entering public buildings. The system's goal is to employ deep learning to reveal masked passers who have been infected with viruses or recorded as invaders. It considers dealing with images of different accuracy. It focuses on excluding important details from the exposed part since a large amount of information was lost due to the covering part. The system has been tested first offline using MATLAB 2020, then it was implemented online using Python. Both versions use Resnet CNN. This resulted in similarity rates while identifying banned ranges from 75% to 100%. Five computed performance measures reach 100% for men and 99.5% for women, when training to validate percentage was 3:1, except for one person due to image dispersity. However, when the ratio is 2:3, the average score, excluding those of similar people, is around 97%.

Keywords: Cloud Computing, Convolution Neural Networks, Identification System, Image Processing, Masked Faces, Monitoring System.

1. INTRODUCTION

The availability of computing resources provided by InPs and the facility of leasing by reliable SPs are the main cause of Cloud-based applications' spread. The emergence of Cloud monitoring systems helps in taking vital decisions in different essential fields based on the collected information. The success of existing systems proves that Cloud computing is particularly helpful for monitoring, controlling, and optimizing processes. In security, visual surveillance is frequently employed. Emerged automatic systems take advantage of computer vision, technology, and AI algorithms. Cloud-based surveillance systems are in demand for storing and processing large amounts of data, quickly and accurately [1]. Research on using a person's anatomical features demonstrates that biometric recognition automatically verifies their identity. Face recognition has gained significant attention and has become a necessary biological authentication technique, because of the rich structure of face.

Based on modern generations of information technology, an integrated work has been achieved that includes the Cloud computing concept, IOT, and several convolutional neural networks to propose a system that can be applied in the security fields. Modern technology has become an important and indispensable part of societies' life after smart systems entered many devices and made them work like the human mind, which saved people time and effort. It enables solving many problems related to the provision of specialized staff for attendance control and the high income of the individual due to the need to be physically present for a long time for preventing issues such as the admission of unapproved individuals into important locations. In addition to the foregoing, technology is known for its accuracy and the lack of errors that can occur in humans because of exhaustion, fatigue, and sometimes lack of attention [2]. Recently, surveillance system, digital cameras, and modern technologies have supported many institutions and departments, whether governmental (airports, ID issuing institutions, banks), marketing (malls, supermarkets), or educational (universities, institutes). It is expected that the development of Internet applications will increase and become more expanded in people's lives [3].

This work aims to reduce the effort on humans by training the system on faces and the possibility of bringing suspect information in addition to the speed of recognition and data security. The design goal is to achieve better performance for a vital service to a reasonable group of enterprises. It targets people wearing masks due to the presence of the Corona virus. The software was designed to deal with images of people in two types, thermal and RGB. Special surveillance cameras are supposed to capture these photos of citizens when they enter specified public organizations.

Registered: 230618 Article Info: 1700 Accepted: 240221
Reserved: 231031 Available: 240331

It in addition takes snapshots or videos of banned people uploaded by authorized person. For people who show a fever symptom (or intruders), a dataset of their images is exported to the Cloud. The proposed Cloud software should recognize (masked) faces and extract set of features aiming at simplifying the identification processes. Thereafter, when they appear in front of any monitoring camera, they will be identified as suspicious persons, to issue alerts that they should be prevented. The paper illustrates the proposed Cloud-based surveillance system for banned people as follow. Section 2 highlights the most related research to the study. Section 3 presents the methodology of suggested work. Section 4 outlines the used platform, then shows and discusses obtained results from conducted experiments.

2. RELATED WORK

Overpopulation is a major problem that hinders the process of issuing identity or official documents to an individual. So, the need for reliable Cloud authentication has emerged, in addition to the rapid developments in accessing the database and communications. Its purpose is to recognize the face and enable authentication. Researchers [4] proposed a system to solve the recognition problem, achieving an accuracy of 99.9% for the controlled face for the FRGC dataset, and validation accuracy of 88.13% for the hard LFW data set.

It is also known that Cloud computing has the potential to increase resources when processing huge data. In [5], the eigenface concept was applied during data collection. although the REST concept was also used for the training data. The purpose is to save resources, and then the data processing stage for the server to do. As a conclusion from this, the possibility of applying Eigenface and REST in face recognition. By receiving information to use it, in addition, when standardizing the image source, this will increase the possibility of development for the system. The algorithm also intervened in the concept of mobile Cloud computing to detect the face and recognize, because the legal prosecution used the program as a tool to combat crime, and the evolutionary stages of mobile applications helped in that. The results proved that mobile Cloud computing reduced the total processing time.

Mobile devices, Cloud computing components, and mobile Internet make up mobile Cloud computing. It is considered because face recognition is the most important application for mobile phone passers and the most important platform. Given the mobile phone environment, one of the most advantages of interacting between Cloud computing on mobile devices and Cloud computing is the overcomes of limitations of mobile devices such as storage, bandwidth, battery life, processing, and surroundings like heterogeneity, and scalability, in addition to security (privacy, reliability) [6].

The most important applications for the face recognition mechanism in surveillance systems is the intelligent verification of attendance as a biometric method, it created an integrated scheme that uses deep learning algorithms based on CNN. This scheme included three tasks: capturing data from surveillance cameras, stream data to a dedicated server, and view real-time data through android mobile devices. Where photos of workers are taken at certain times and stored in a huge database and pushed to the server, after several preprocessing done on the images, the system training on it, to make the system distinguish employees from others. At last, the system generates a report based on the employee's attendance, and uploaded it to Android devices, so the employer can monitor the employee's attendance from his smartphone [7].

The system can also be applied in order for students to attend lectures or exams, as happened when giving lectures via the Internet due to the Covid19 pandemic, as many countries issued decisions imposing social divergence and not touching anything given that because the virus is rapidly spreading. So, it was necessary to design an attendance monitoring system that depends on face recognition. It issues a warning message when attempts to defraud students and enter with several personalities (fraud), and the acceptance rate reached 95% [8]. Or, the recognition process could be periodic in line with a specified time (fixed or changeable) to ensure that students are paying attention to the material [9].

These systems can be used to organize the entry of visitors, where the process of verifying and authenticating the visitor takes place with recording the time/date of the visit, the name of the visitor, and the name of the person who wishes to visit him. This type of system is called the Face Recognition Visitor Management System (FRVMS), the system aims to secure the place from strangers who try Spying or stealing the building. The system became more efficient because the system enables controlling and managing the processes [10]. In addition, some panels serve as a platform for intrusion detection into the Cloud. Multiple technologies assist in detecting penetration attempts and attacks as they happen and allow for their possible control by working productively while conducting in-depth analyses [11]. To decrease time consumption and lower false-positive rates of intrusion detection systems in Cloud environments, research [12] introduced the Optimized Sine Swarm algorithm (OSS) to select significant features solitary. It gets 98.15 accuracy rate for UNSW-NB15 Dataset.

Also, Monitoring can be used to solve the problem of the traditional methods that many farmers follow in arming, which leads to a decrease in the yield of crops and fruits. Using a variety of Cloud-based voice recognition techniques, automation has been introduced in [13], replacing humans with automated computers. Accuracy for a set of common commands were improved, often ranging from 65% to 95%. In addition, IoT Cloud platform has been used in enhancing the safety of modern agricultural production and management [14]. It makes possible to do tasks like remote control of equipment, uploading and acquiring of sensor data, and motion-based video monitoring.

Recent study suggests an effective idea based on artificial intelligence and computer vision that focuses on automated monitoring through the camera [15]. It aims to detect whether people are wearing a mask or not, as well as checking the body temperature by sensors for the purpose of making a safe environment. Modern deep learning algorithms were mixed with several techniques to detect unmasked faces or high temperatures and send a specific alert for each status. The model had 90% accuracy. Cloud-based lung tumor stage categorization and detection have recently been proposed [16].

The system of deep learning and data collecting strategy utilizing the Cloud are provided to categorize the different stages of pulmonary illness. The average achieved lung tumor stage classification accuracy was 98.6%. In [17], a system for constantly monitors the person's voice activity is presented. In the case that there is an anomaly in the analysis results, it automatically contacts the involved hospital or carer to claim the patient's condition. It achieves a precision of 67.90% with real-time voice input. It might serve as a lifesaving mechanism for those suffering from heart attack, stroke, or hysteria, among other illnesses.

3. PROPOSED SYSTEM

We suggested a strategy that involves four phases in order to achieve our goal. Phase (I) creates a database. containing a collection of photographs for each prohibited (contagious patient or intrusive) individual. Phase (II) recognizes passers by detecting and analyzing their eye-forehead region. Phase (III) identifies those belonging to the uploaded database, when appearing in any monitored section. Phase (IV) takes the necessary alert procedures for prevention. The proposed monitoring system's architecture is illustrated in Figure 1. As well, steps controlling the function flow of the proposed system phases is depicted below, in Algorithm 1.

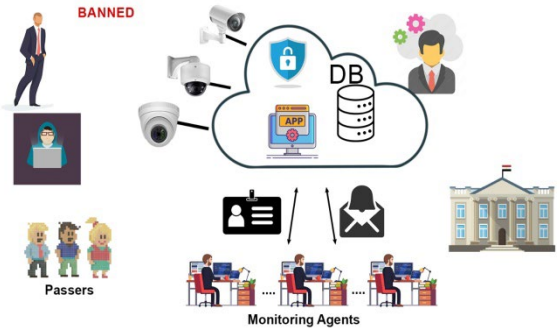


Figure 1. The proposed Cloud-based monitoring system architecture

3.1. Phase I: Image Database Construction

For the recognition stage, we need to prepare the database of banned images that shall be used in training and validation. Our idea is to separate males from females for better and faster matching. The program inputs the images and splits them into two groups (training and testing) to recognize the gender [18]. The flowchart of this phase, showing processes sequence for constructing our database, is given in Figure 2.

Algorithm 1. Proposed monitoring system

```
Input: B1[ ] (Banned snapshots),  B2[ ] (Banned videos), Img[ ] (Passer images), F (Banned Information file)
Output: E_msg (Alert message), M_msg (Monitor notification)
Begin
 Construct (B1, B2, MDB, WDB ) ;
 While ∃ Ph ∈ Img & Permit ( ) do
    Read (Ph) ;
    Preprocess (Ph) ;
    Viola-Jones (Face) ;
    Detect (E-F) ;
    Extract (F, Wt) ;
    Classify (G) ;
    If G  == 'M' then
              Match (Wt, MDB) ;
     Else
              Match (Wt, WDB) ;
    End If;
    Compute (S) ;
    If S  ≠ λ then
               Display ("Unknown person") ;
    Else
              Get (Id) ;
              Readf (F, Id, G, N , B, C, S, E) ;
              E_msg = "Prevent" + N ;
           SendE (E_msg, N, Id, Loc_B, Loc_I,Date ( ), Time ( )) ;
              M_msg = ("We identify this person as banned") ;
              Display (M_msg, Id, Img, G, N, B, C, S, E) ;
    End If;
End while;
End
```

where, *MDB* is men's database, *WDB* is women's database, *Ph* is passer photo, *F* is features, *Loc_B* is Banned location, *Loc_I* is Identify location, *Wt* is weights, *S* is similarity ratio, λ is threshold, *Id* is identity number, *C* is country, *G* is gender, *N* is name, *B* is year of birth, *S* is skin color, *E* is eye color.

The process of extracting features is one of the main tasks for distinguishing between mem and women. Deep learning has been used for the purpose of extracting features in addition to the ability to recognize the face, identify the object and distinguish the pattern. Next, to collect needed data for training the model, we accept both videos and photos of the people we want to prevent from entering specified places. Frames are extracted from videos. Thus, the proposal detects eye-forehead (E-F) regions from images, regarding either who is wearing a mask or not [19]. The output will be a dataset for men (MDB) and another for women (WDB).

Also, each individual is assigned a unique ID, starting with one for males and zero for females, and save banned information. Furthermore, the system is trained on both datasets (MDB and WDB), and weights are saved. As well, gender, eyes and skin colors are detected. Figure 3 displays some cases for different inputs with the resulted cropped part.

3.2. Phase II: Passer Recognition

In the second stage, the system accepts colored images of people of both kinds (with/without masks) that are passing through a gate at another place. Then, to detect gender, the system adopts our deep learning residual network model [19] that use CNNs to categorise people in masked or undercover based on their images. Google Drive, Google Colab, and Gmail are used to carry out classification jobs.

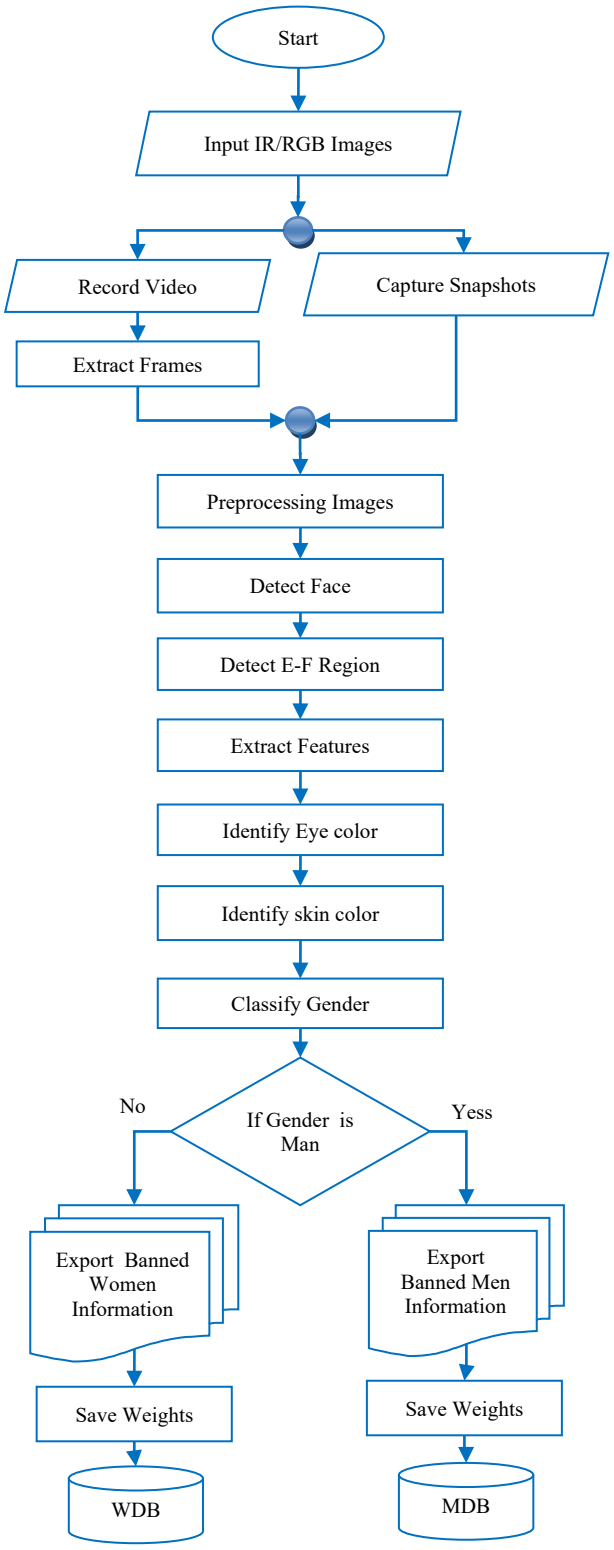


Figure 2. Banned database construction

3.3. Phase III: Banned Identification

When the identification stage starts, each passer image, that has been detected in the previous stage, is compared with the database that was stored for banned of the same gender. For accessing the databases, we get permission. The system matches the weights, calculates the percentage of similarity, and determines his/her identity, according to gender. These processes are depicted according to Figure 4 with steps for alert.

3.4. Phase IV: Alert Management

The last phase of the system comes after the identification phase ended with a conclusion that the passer match one of recorded banned persons, see Figure 4. In this case, the system immediately sends a warning email message (via Gmail), as alert, including the person ID with the location, date, and time. In addition, it displays all needed information on the monitoring agent screen to facilitate finding him easily. It shows banned personal image, the gender, similarity ratio, and other recorded information.

4. PERFORMANCE RESULTS

This section is dedicated to the implementation process. It gives a description of the used platform and the dataset for the proposed system. A brief discussion follows the presentation of the experimental findings. Also, security taken precautions for protecting data are clarified.

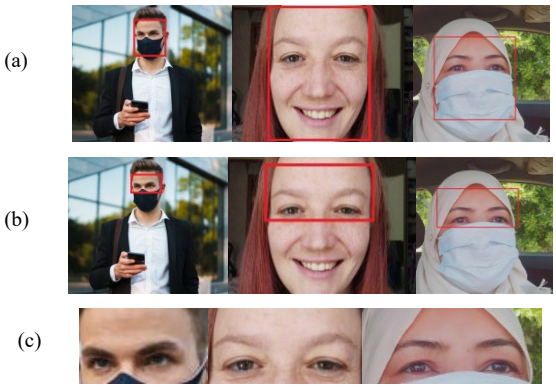


Figure 3. Samples of resulted images during dataset creation
a) Detected face, b) Detected region, c) Cropped image

4.1. Platform

As clarified before, we started the implementation by designing an offline system using Matlab2020 to classify the gender of humans from input facial images, whether it is thermal or RGB.

Then, we implemented our proposed deep learning residual neural network model using Cloud computing. Thereafter, we completed our identification system programmed with Python, using Gmail, Google Drive, and Google Colab. For online and offline training, we needed different requirements, as listed in Table 1.

Table 1. Online vs. Offline requirements

Subject	Offline	Online
Environment	PC and OS	Cloud infrastructure
Program	MATLAB (installed) and libraries	Python (Online) and libraries
Processor	CPU	GPUs
Data usages	On Computer Drives	On google Drive
Internet	No need	Required
Programming language update	Required	No need

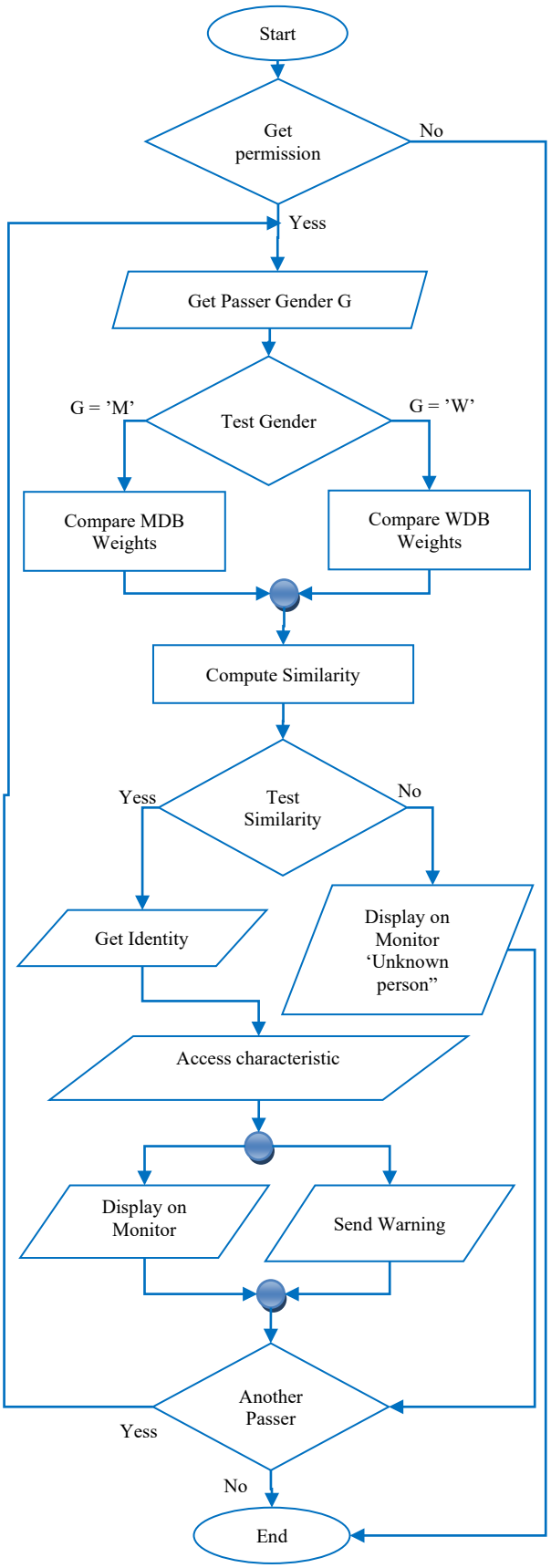


Figure 4. Passer identification as banned and alert

Since GPU (graphics processing unit) nowadays are used in many multimedia tasks, such as image processing, pattern matching, recognition, and others. We combined GPU and CPU strengths and features, to gain higher performance. As known, CPU Architecture is consisting of little cores that are interacting with caches that deal with a few instructions at one time. On the other hand, GPU includes many cores which can deal at the same time with a big number of instructions. Table 2 shows the configuration of used platform for implementing and testing our proposal. The Python program runs on the Colab environment to train our Neural Network (ResNet) on uploaded images. The images were earlier sent using Google Mail and are now kept in a Google Drive folder. The capacity of the drive can be increased as the image database is getting larger.

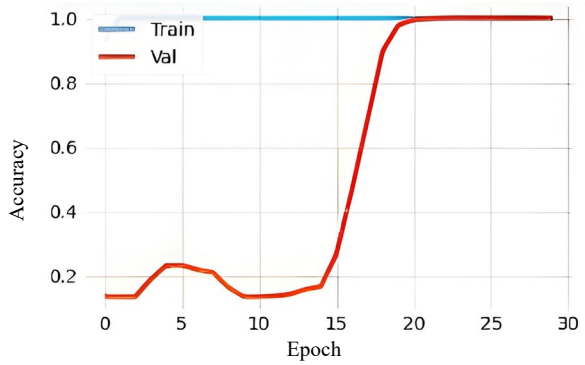
Table 2. Configuration of platform

Configuration	Parameters
Operating system	Edition: Windows 10 Enterprise
	Version: 22H2
	Experience: Windows Feature Experience Pack 120.2212.4190.0
	System type: 64-bit operating system, x64-based processor
CPU	Intel(R) Core (TM) i7-7500U CPU @ 2.70GHz 2.90 GHz
GPU	NVIDIA GeForce 9300MX
Installed RAM	12.0 GB (11.9) Usable
Python	3.8.10 (default, Nov 14, 2022, 12:59:47) [GCC 9.4.0]
Platform processor	x86_64
Tensor flow	2.9.2
Keras	2.9.0
CV2	4.6.0

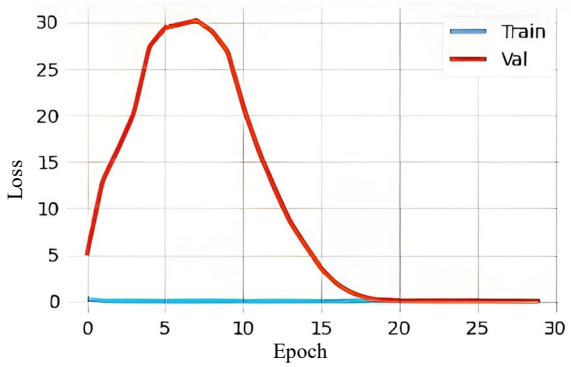
4.2. Dataset

As discussed earlier, our aim was to apply the system in public places such as educational institutions, banks, and health centers, etc. But we faced difficulties in authentication procedures, due to privacy rules. Thus, for image accession, we used existing available public datasets, and added some collected images and videos from our relatives and the Internet. For the purposes of prohibited image collection, we made the assumption that certain persons are sick and that a camera that has detected their high temperature has collected thermal photographs of them. Likewise, some other RGB photos are sent for detected intruders. Different IR and RGB datasets were used. One dataset has a total of 461 photos and the other has around 2907 thermal pictures [20, 21].

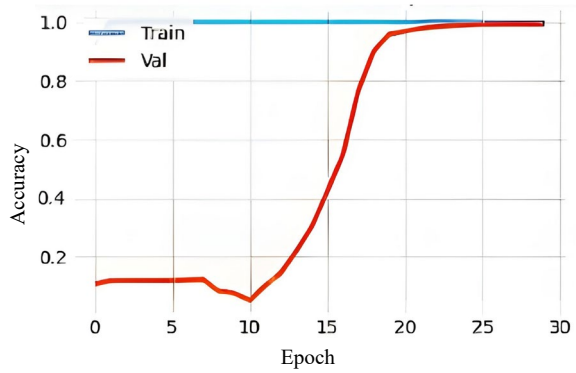
For recognition/identification phases, we have constructed a database for nine men (MDB) including 2176 image, and another for nine women (WDB) having 2358 images. There are also 23 images for identification and additional 300 images of persons of each gender for recognition. The images include only eye-forehead region. To ensure citizen safety and protect data from unauthorized access, we have implemented security measures. An alert is sent by email asking to allow accessing the drive and deal with the files. According to admin response, authorized persons are given permissions, while others are prevented.



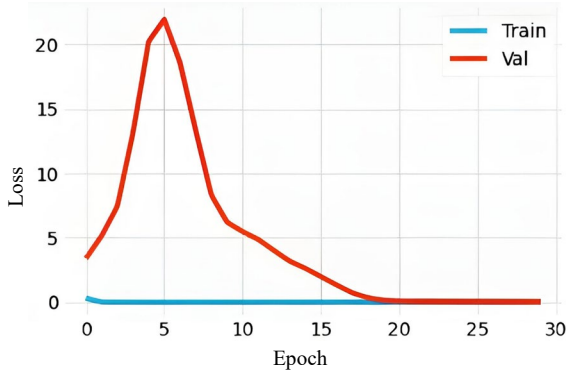
(a)



(b)



(c)



(d)

Figure 5. Accuracy and loss during training and validating, a) Model accuracy for men, b) Model loss for men, c) Model accuracy for women, d) Model loss for women

4.3. Results

Ninety percent of the built-in database, split into ratios of forty to sixty, has been used for training and validating our model. Whereas the other ten percent has been preserved for testing. Figure 5 shows the accuracy vs. loss for classifying men and women. When executing our Python program on Cloud environment, all images, in both types, have been classified. On the contrary, the MATLAB program has classified 99% of IR and 99.2% of RGB images. Finally, similarity has been tested, and recognition rates have been computed, observing the number of images that has been recognized from total 300, as listed in Tables 3 and 4.

Table 3. Similarity and recognition ratio for men

Similarity ratio	Recognition ratio	# Images
75%	59.6%	179
80%	66.6%	200
85%	74%	222
90%	81%	243
95%	88%	264
100%	100%	300

Table 4. Similarity and recognition ratio for women

Similarity ratio	Recognition ratio	# Images
75%	63.6%	191
80%	67%	201
85%	73%	219
90%	80%	241
95%	87.6%	263
100%	100%	300

For more comparison, we have operated our system with different image distribution proportions, once using 40-60, and the other using 75-25. The disproportion of resulted rates has been pictured below for overall accuracy, recall, specificity, precision, and F-score, as shown in Figures 6-15, according to the ratio of correctly classified [18-19] [22]. For True Positive (*TrPo*), True Negative (*TrNe*), False Positive (*FaPo*), False Negative (*FaNe*), formulas are:

$$Recall = \frac{TrPo}{TrPo + FaNe}, \quad Precision = \frac{TrPo}{TrPo + FaPo}$$

$$F - Score = 2 \times \frac{Precision \times Recall}{Precision + Recall}$$

$$Overall\ accuracy = \frac{TrPo + TrNe}{TrPo + TrNe + FaPo + FaNe}$$

$$Specificty = \frac{TrNe}{FaPo + TrNe}$$

For men, labeled ('*A*', '*O*', '*B*', '*M*', '*W*', '*K*', '*J*', '*H*', and '*S*'), the system accuracy and recall ranges were from 99 to 100 except 'A' decreases to 65 (Figures 6 and 8). '*A*' precision was 87.4 and '*M*' was 84.2, when the rest got 100 (Figure 10). Considering F-score measure, '*A*' has 78.9, '*O*' has 93, '*M*' has 91.4, and others have 100 (Figure 12). All record 100 specificity but '*O*' was 98.3 and 'M' was 97.6 (Figure 14). On the other hand, for women labeled ('*D*', '*I*', '*U*', '*N*', '*R*', '*Q*', '*F*', '*K*', and '*L*'), the system accuracy and recall ranges were from 97 to 100 except '*D*' decreases to 88.1, and '*R*' to 94.8 (Figures 7 and 9).

The '*N*' precision was 96 and '*Q*' was 80.5, when the rest almost 100 (Figure 11). Considering F-score measure, '*D*' has 93.7, '*I*' 94.6, and others ranges between 97 and 100 (Figure 13). All record about 100 specificities but '*Q*' was 96.7 (Figure 15). Figures 16 and 17 show that the average performance for men/women identification gets 100% specificity and other measures moves from 95 to 100 percent.

5. CONCLUSION

As perceived, dataset of people who were selected are of different ages and nationalities for the purpose of demonstrating the power of the system and its ability to simulate the heterogeneity of features in real life. Preserving citizens privacy is of our concern. The similarity check demonstrated the proposed system qualification to identify any input image regarding the stored database. Tables 3 and 4 indicates that resulted similarity rates ranging from 75% to 100%. The similarity rate disparity is due to cases of pictures' distortion or missing parts. Proposed NN model achieves very good accuracy percentage in contrast to loss, as Figure 5 proves.

Experimental results infer that the five performance measures reach the highest rate (100%) when training to validating percentage was 3:1 (75-25), except for 'R' that because the resolution of video is low. However, due to their similarity, 'A' and 'M' had worse male values in the 2:3 (40-60) ratio than 'I' and 'D' did for females. Balqes records low precision. Whilst tests for others record exceeds ninety percent. To conclude, proposed system for recognizing the identity of masked persons is essential, as the problem difficulty increased recently, since the start of Covid 19 pandemic. As a consequence, preventing banned infected one in addition to intruders becomes possible.

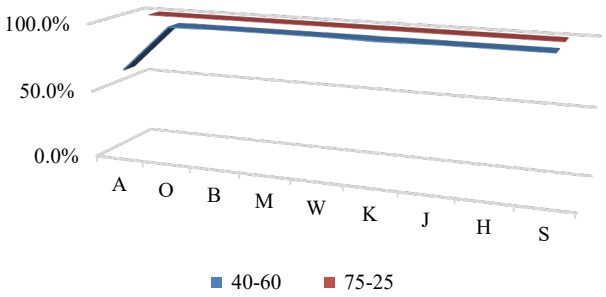


Figure 6. Accuracy for men

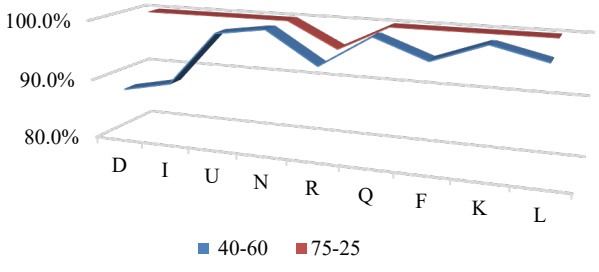


Figure 7. Accuracy for women

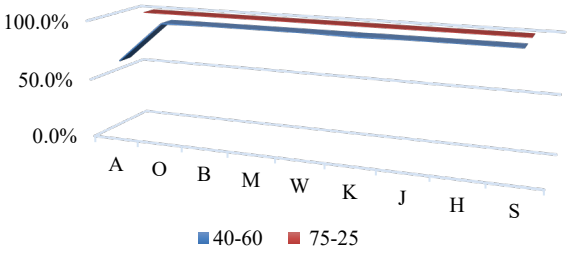


Figure 8. Recall for men

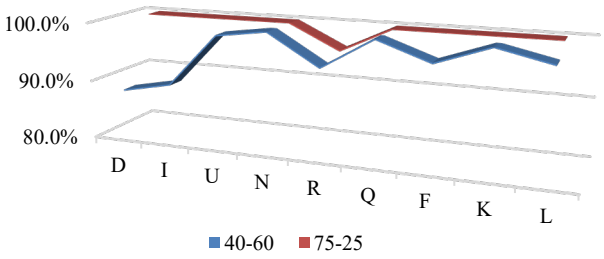


Figure 9. Recall for women

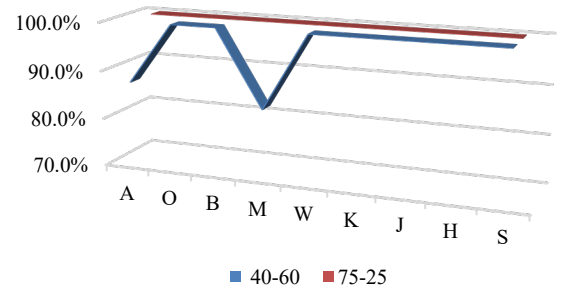


Figure 10. Precision for men

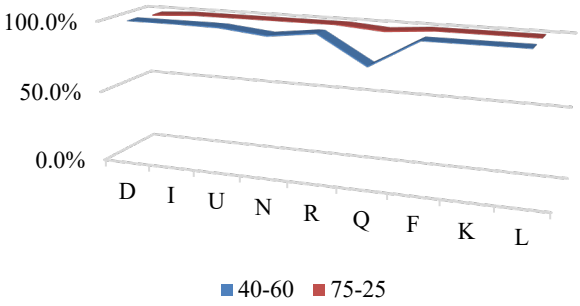


Figure 11. Precision for women

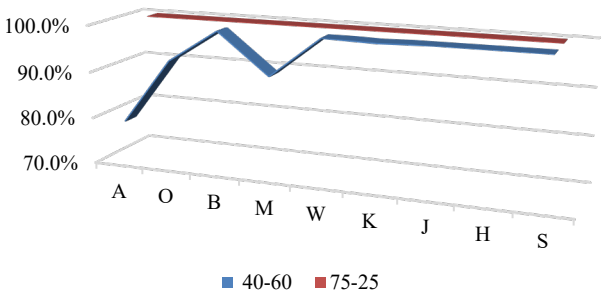


Figure 12. F-Score for men

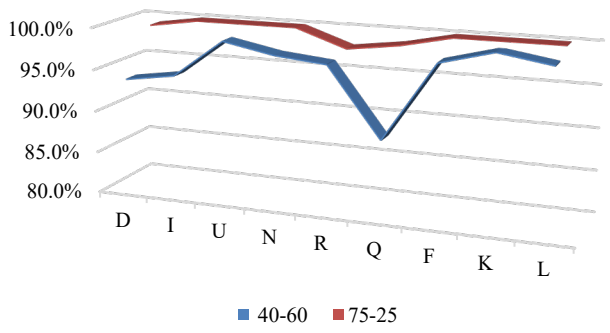


Figure 13. F-Score for women

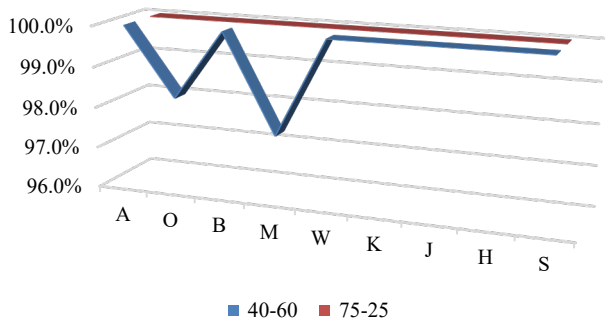


Figure 14. Specificity for men

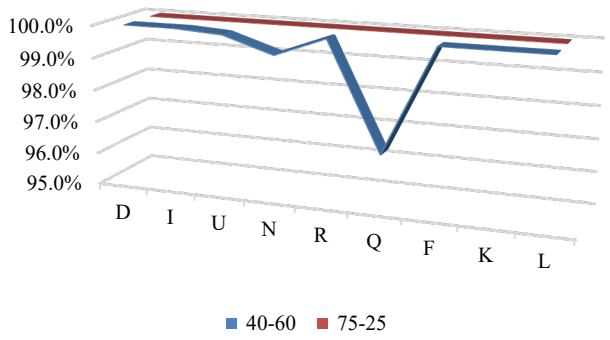


Figure 15. Specificity for women

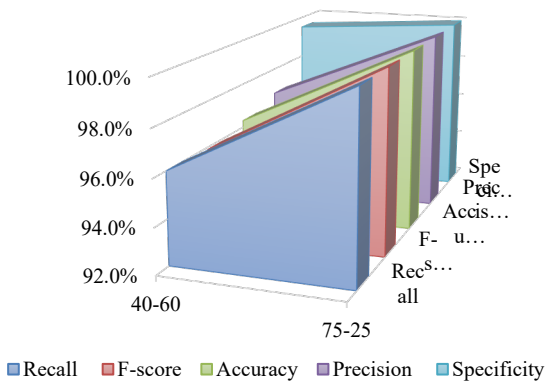


Figure 16. Average performance for men identification

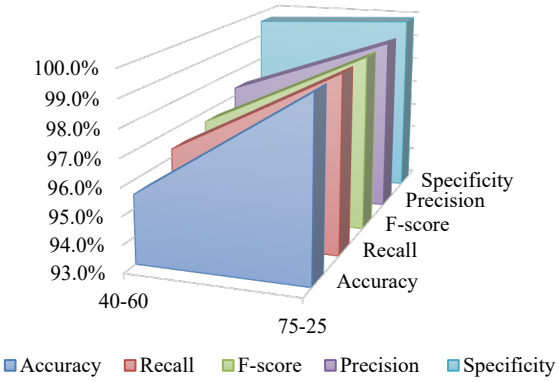


Figure 17. Average performance for women identification

REFERENCES

[1] L. Wang, R. Ranjan, J. Chen, B. Benatallah, "Cloud Computing: Methodology, Systems, and Applications", CRC Press, 2011.

[2] B. Rochwerger, et al., "An Architecture for Federated Cloud Computing", Cloud Computing: Principles and Paradigms, John Wiley and Sons, pp. 393-410. ISBN 9780470887998, 2011.

[3] N. Azzeddine, "An Approach to Monitoring System Based on Cloud for IoT", M.Sc. Thesis, University of Eloued, Algeria, 2018.

[4] S. Kumar, D. Sadhya, D. Singh, S.K. Singh, "Cloud Security Using Face Recognition", Web-Based Services: Concepts, Methodologies, Tools and Applications, pp. 2055-2075, 2016.

[5] S.T.M. Siregar, M.F. Syahputra, R.F. Rahmat, "Human Face Recognition Using Eigenface in Cloud Computing Environment", The 10th International Conference Numerical Analysis in Engineering, IOP Conference Series Materials Science and Engineering, Vol. 308, No. 1, pp. 1-9, Banda Aceh, Indonesia, 2018.

[6] R. Akshata, N. Gireeshbabu, M. Muneshwara, G.N. Anil, "A Survey on Face Recognition through Mobile Cloud Computing Environment", International Journal of Engineering Research and Technology (IJERT) NCRTS, Vol. 3, No. 27, pp. 1-5, 2015.

[7] F. Hamami, I.A. Dahlan, S.W. Prakosa, K.F. Somantri, "Implementation Face Recognition Attendance Monitoring System for Lab Surveillance with Hash Encryption", Journal of Physics: Conference Series, Vol. 1641, No. 1, pp. 1-6, 2020.

[8] A. Jain, R. Gupta, M.S. Ansari, T. Ikram, "Attendance Monitoring System Using Face Recognition", International Journal for Research in Applied Science and Engineering Technology, Vol. 10, No. V, pp. 3024-3029, 2022.

[9] T. Rahman, A.N. Saputra, E.D. Anggara, "Attendance Monitoring System Based on Iot", Multitek Indonesia, Vol. 15, No. 2, pp. 33-43, 2022.

[10] B.S. Satari, N.A. Abd Rahman, Z.M. Zainal Abidin, "Face Recognition for Security Efficiency in Managing and Monitoring Visitors of an Organization", The 2014 International Symposium on Biometrics and Security Technologies, pp. 95-101, Kuala Lumpur, Malaysia, 2014.

[11] Y.H. Alagrash, H.S. Mehdy, R.H. Mahdi, "A Review of Intrusion Detection System Methods and Techniques: Past, Present and Future", International Journal on Technical and Physical Problems of Engineering (IJTPE), Issue 54, Vol. 15, No. 1, pp. 11-17, March 2023.
[12] J. Vimalrosy, S. Brittorameshkumar, "OSS-RF: Intrusion Detection Using Optimized Sine Swarm Based Random Forest Classifier on Unsw-Nb15 Dataset", International Journal on Technical and Physical Problems of Engineering (IJTPE), Issue 51, Vol. 14, No. 2, pp. 275-283, June 2022.
[13] J. Kim, H. Lee, S. Jeong, S. H. Ahn, "Sound-Based Remote Real-Time Multi-Device Operational Monitoring System Using a Convolutional Neural Network (CNN)", Journal of Manufacturing Systems, Vol. 58, No. PA, pp. 431-441, 2021.
[14] S. Liu, L. Guo, H. Webb, X. Ya, X. Chang, "Internet of Things Monitoring System of Modern Eco-Agriculture Based on Cloud Computing", IEEE Access, Vol. 7, pp. 37050-37058, 2019.
[15] C. Lal, S. Aftab, S. Kumar, M. Shaikh, "Smart SOP's Surveillance System Using Deep Neural Network Smart SOP' s Surveillance System Using Deep Neural Network", Vol. 14, No. 7, pp. 6-11, 2022.
[16] G. Kasinathan, "Cloud-Based Lung Tumor Detection and Stage Classification Using Deep Learning Techniques", BioMed Research International, Vol. 2022, Article ID 4185835, pp. 1-17, 2022.
[17] G. Latif, A.H. Khan, M.M. Butt, O. Butt, "IoT Based Real-Time Voice Analysis and Smart Monitoring System for Disabled People", Asia Pacific Institute of Advanced Research, Vol. 3, No.2, pp. 191-199, 2017.
[18] A.J. Jalil, N.M. Reda, "Infrared Thermal Image Gender Classifier Based on the Deep ResNet Model", Advances in Human-Computer Interaction, Vol. 2022, Article ID 3852054, pp. 1-11, 2022.
[19] A.J. Jalil, E. El Seidy, S.S. Daoud, N.M. Reda, "CNN Model for Analyzing Masked Facial RGB Images Using Cloud Computing", International Journal of Intelligent Systems and Applications in Engineering, Vol. 11, No. 2, pp. 648-654, 2023.
[20] "Index of /downloads/TD_IR_E", http://tdface.ece.tufts.edu/downloads/TD_IR_E/, 10 January 2023.
[21] "SCIEBO", https://rwth-aachen.sciebo.de/s/AoSNdkGBRCtWIzX, 10 January 2023.
[22] E. Eidinger, R. Enbar, T. Hassner, "Age and Gender Estimation of Unfiltered Faces", IEEE Transactions on Information Forensics and Security, Vol. 9, No. 12, pp. 2170-2179, December 2014.

BIOGRAPHIES

Name: **Alyaa**
Middle Name: **Jaber**
Surname: **Jalil**
Birthday: 10.03.1983
Birthplace: Basrah, Iraq
Bachelor: Computer Science, Computer Science Department, Faculty of Science, University of Basrah, Basrah, Iraq, 2005
Master: Computer Science, Computer Science Department, Faculty of Science, University of Basrah, Basrah, Iraq, 2011
Doctorate: Student, Computer Science, Mathematics Department, Faculty of Science, University of Ain Shams, Cairo, Egypt, Since 2020
The Last Scientific Position: Lecturer, Computer Science, Computer Science Department, Faculty of Computer Science and Information Technology, University of Basrah, Basrah, Iraq, Since 2011
Research Interests: Cloud Computing, Images Processing, Neural Network
Scientific Publications: 9 Papers

Name: **Essam**
Middle Name: **Ahmed**
Surname: **Al Seidy**
Birthday: 28.11.1961
Birthplace: Cario, Egypt
Bachelor: Pure Mathematics, Mathematics Department, Faculty of Science, University of Ain Shams, Cairo, Egypt, 1983
Master: Pure Mathematics, Mathematics Department, Faculty of Science, University of Ain Shams, Cairo, Egypt, 1988
Doctorate: Pure Mathematics, Mathematics Department, Faculty of Science, University of Ain Shams & University of Vienna, Egypt-Austria, 1994
The Last Scientific Position: Prof., Game Theory, Mathematics Department, Faculty of Science, University of Ain Shams, Cairo, Egypt, Since 2019
Research Interests: Population Game Dynamic, Symmetric and Asymmetric Games, Differential Games, Data Classifications
Scientific Publications: 61 Papers, 2 Books, 35 Theses
Scientific Memberships: The Egyptian Mathematical Society

Name: **Sameh**
Middle Name: **Sami**
Surname: **Daoud**
Birthday: 26.03.1946
Birthplace: Cairo, Egypt
Bachelor: Mathematics Department, Faculty of Science, University of Ain Shams, Cairo, Egypt, 1966
Master: Pure Mathematics, Mathematics Department, Faculty of Science, University of Ain Shams, Cairo, Egypt, 1996
Doctorate: Dynamical System, Probabilities Department, Faculty of Mechanics and Mathematics, Moscow State University, Moscow, Russia, 1975
Last Scientific Position: Assoc. Prof., Computer Science, Mathematics Department, Faculty of Science, University of Ain Shams, Cairo, Egypt, Since 1988
Research Interests: Dynamical Systems, Compiler, Theory of Computation
Scientific Publications: 40 Papers, 30 Theses
Scientific Memberships: The Egyptian Mathematical Society

Name: **Naglaa**
Middle Name: **Mohammed**
Surname: **Reda**
Birthday: 16.04.1969
Birthplace: Cairo, Egypt
Bachelor: Pure Mathematics and Computer Science, Mathematics Department, Faculty of Science, Ain Shams University, Cairo, Egypt, 1990
Master: Computer Science, Mathematics Department, Faculty of Science, Ain Shams University, Cairo, Egypt, 1998
Doctorate: Computer Science, Mathematics Department, Faculty of Science, Ain Shams University, Cairo, Egypt, 2005
The Last Scientific Position: Assoc. Prof., Computer Science, Mathematics Department, Faculty of Science, University of Ain Shams, Cairo, Egypt, Since 2022
Research Interests: Parallel Algorithms, Bioinformatics, Object Recognition, Cloud computing
Scientific Publications: 19 Papers, 2 Books, 5 Theses
Scientific Memberships: The Egyptian Mathematical Society