Face Recognition for Smart Door Lock System using Hierarchical Network

Muhammad Waseem[1], Sundar Ali Khowaja[2]
Faculty of Engineering and Technology
University of Sindh Jamshoro, Pakistan
aliaafaque@gmail.com[1] ,
sandar.ali@usindh.edu.pk[2]

Ramesh Kumar Ayyasamy[3], Farhan Bashir[4]
Faculty of Information & Communication Technology
Universiti Tunku Abdul Rahman Kampar
rameshkumar@utar.edu.my[3],
Farhan.shaikh@usindh.edu.pk[4]

Abstract— **Face recognition system is broadly used for human identification because of its capacity to measure the facial points and recognize the identity in an unobtrusive way. The application of face recognition systems can be applied to surveillance at home, workplaces, and campuses, accordingly. The problem with existing face recognition systems is that they either rely on the facial key points and landmarks or the face embeddings from FaceNet for the recognition process. In this paper, we propose a hierarchical network (HN) framework which uses pre-trained architecture for recognizing faces followed by the validation from face embeddings using FaceNet. We also designed a real-time face recognition security door lock system connected with raspberry pi as an implication of the proposed method. The evaluation of the proposed work has been conducted on the dataset collected from 12 students from Faculty of Engineering and Technology, University of Sindh. The experimental results show that the proposed method achieves better results over existing works. We also carried out a comparison on random faces acquired from the Internet to perform face recognition and results shows that the proposed HN framework is resilient to the randomly acquired faces.**

Keywords— Face Recognition, Deep Machine learning, Security Door, Raspberry pi, Smart home

I. INTRODUCTION

With the evolution of systems getting smarter through the integration of artificial intelligence technologies, the ways to sabotage those systems are also gauging, simultaneously. Specifically, in the security and surveillance applications, relying on a uni-modal system for reliable monitoring is not recommended [1]. Security problems are given high priority because every business owner strives to keep their organizations, assets, and workplace as sheltered as could and same goes for homes [2]. In this way, the security does matter in everyday life. One of the main reasons for compromise of security is the unauthorized access to strangers [3]. The old door security systems made use of keys, locks and chains. However, the locks can be easily broken. The use of keys to unlock the doors is not efficient sometimes, because the keys may be sometimes used by the wrong person or keys can get stolen or can be duplicated [4]. Then came the era of shallow learning algorithms with uni-modal systems which could accommodate a single biometric trait at a time to ensure the authorized access [1]. The most significant aspect of any door security framework is recognizing accurately the people who want to access the entryway; however, uni-modal systems fail to achieve that benchmark [5]. With the evolution of devices, the one thing which needs to be adapted is the pervasiveness and unobtrusive nature of acquiring biometric trait suggesting that the user should not be fatigued when requesting the authorization. Using iris recognition, and complicated traits such as Gait and signature, require the user to perform some tasks which are specific to the authorization system. Even with fingerprint recognition one has to place the finger on the device to request the access. The face modality is the only trait which can be used for a security system that complies with ubiquitous characteristics [6]. Another aspect which needs to be explored is the single-tier recognition system which results in false positives and can be spoofed with the evolutionary methods [7]. Such as deep fakes [8], however, these methods are designed to fool the single-tier systems which does not comprehend to the diversified information. A hierarchical multi-tier system needs to be proposed which is trained on diversified data to cope with the aforementioned issue [7,9,10,11,12].

There have been a lot of face recognition studies using deep learning techniques which can be considered as state-of-the-art methods. However, these methods heavily rely on a single-tier of recognition using the features projected in embedding space. Randomly obtained faces from Internet sometimes are able to make the networks believe that they reside in the pool of authorized users. It is therefore, necessary, to add a second-tier of authorization to improve the performance and add resilience to the recognition system. In this regard, we propose a two-tier hierarchical network (HN) architecture which uses a discriminative learning method followed by FaceNet to perform the face recognition. Furthermore, we also built a prototype which takes into account the multi-mode of recognition, i.e. recognition from embedded system followed by the authorization from the home owner via e-mail. In this way, our system reduces the probability of false positives, accordingly. Moreover, the implemented embedded system provides a realization to the proposed study. The contribution of our proposed work are as follows:

1. We propose a hierarchical network (HN) framework to improve the face recognition performance.
2. We built a prototype to show the implication of proposed work.
3. We show that the HN framework is resilient to the randomly acquired facial images from the Internet.

The remaining paper is structured as follows: Section 2 provides a consolidated analysis of the works related to face recognition. Section 3 presents the proposed methodology for

978-1-7281-8408-1/20/$31.00 ©2020 IEEE

HN framework. Section 4 provides the details of the prototype. Section 5 gives quantitative and qualitative results and Section 6 concludes this work.

II. LITERATURE REVIEW

Hassan, Harnani. et al [13] proposed security framework utilizing face acknowledgment in which programmed magnetic lock associated with microcontroller is utilized. GUI based face acknowledgment framework is created in MATLABA2009A that orders to microcontroller utilizing sequential correspondence to open or close the magnetic door lock.

J. Shankar Kartik et al. [14] have proposed system in which system uses a webcam to recognize the interloper that was working by program introduced on the computer and it utilizes web for correspondence, if camera detect movement of any gatecrasher the recognition software will communicate to home owner via Internet and simultaneously it gives sound caution and also system will send SMS to the house holder.

G. Senthilkumar.et al [15] proposed system that was taking images from camera Using RaspberryPi and compared it from accessible database however the confinement was his model could not work appropriately in the poor lighting.

H. Lwin.et al. [16] introduced an entryway lock system which comprises of three subsystems: face recognition, face identification and last is door entry. The recognition is done by using PCA algorithm. The entrance gate will open automatically for the authorized person and caution will ring for the unapproved individual. Restriction of this framework was taking pictures using webcam consistently until stop button is pressed.

CA. Athira.et al. [17] proposed a security framework which uses face as the biometric trait. Authors used PCA provided with MATLAB package. At the point when the face was perceived, a SMS ready will be given to approved individual using GSM. The precision of the framework was simply 85%. The execution time was higher in light of the fact that the program was executed in MATLAB.

Meera Mathew.et al. [18] proposed secure gateway locking system with multi-factor confirmation also used various method for encryption by using RFID, which can authorize the user. his main target was to structure and deploy an advanced security system that can be used in critical place where simply authorized persons can be entered.

Ibrahim Mohammad Sayem.et al. [19] presented face recognition security system using IOT in which raspberry pi is used with camera module for input taking image and compared to dataset, OpenCV library were used in python for feature extraction. His proposed system was able to recognize person from poor image quality.

Ketan J. Bhojane. et al. [20] introduced face recognition security framework for car in which face detection and face tracking system algorithm were developed using OpenCV, Haar Classifier and eigenface in MATLAB, and whole system was connected with Raspberry pi to command the car.

Awais, Muhammad. et al [21] proposed continuous monitoring security system through face acknowledgment by using HOG and neural system in which data obtain through video dataset. Face, foreground and background extracted from captured video data and compared to available database in case of no face is found the alarm will ring for action alert.

Sajjad, Muhammad. et al [22] introduced recognition for smart security in law enforcement services in which suspicious behavior recognition can be detect based on the facial expression and behavior of person, camera connected with raspberry pi will capture the video. SVM and Gabor algorithm is used to extract the features from face which will predict the emptions like angry, fear, happy etc. based on the collective emotion action will be take.

Mamoon Tahnoon. et al [23] proposed face recognition security system using deep neural network which uses histogram equalization for enhancing image quality, a wavelet transforms for compress image size and multi neural network for extract main features from face and results compared to present database for classification.

Jaiswal, Arvind. et al [24] presented real time security surveillance system due to public security concerns in this system IP CCTV Camera is used, for extracting features from every person's face LBPH algorithm is used and Haar Case Cade for face detection.

The existing methods mostly employ shallow learning algorithms which have been proven to not perform as good as deep learning methods [11,12]. Moreover, the studies employing deep learning strategies mostly focus on a single-tier recognition system. We prove in our ablation study that the single-tier recognition system fails to generalize the recognition performance when fake images or spoofed images from the Internet are used to gain the authorization access. In this work, we add another tier of security check in the form of discriminative learning strategy so that the diversified representation is learnt which has the ability to distinguish between the authorized and unauthorized users while dealing with spoofed images.

III. HIERARCHICAL NETWORK FRAMEWORK

As mentioned in the former section that a single-tier does not generalize the performance when dealt with spoofed images from the Internet which has been shown in our ablation study. Existing studies have proved that the networks trained in hierarchical structure provide better recognition rates as well as generalize the performance across diversified data [7,9,10,11,12]. Following the success of hierarchical networks in array of applications supporting automation [7,9,10,11,12] we designed our framework to leverage those characteristics. In this section, we present the proposed framework for real-time face recognition system as shown in figure 1. The first step is to acquire the image from any acquisition device such as camera, webcam. Once the facial image is acquired, we detect the face and crop it for further processing. Our recognition framework is based on two-tier authentication suggesting that the first tier uses our proposed deep learning architecture (ResNet101) to recognize the face. The idea of branching off the ResNet101 network at specific layer was leveraged by the study [11,12]. The second tier will use face embedding from (FaceNet) to authorize the individual. The recursive nature of using two discriminative learning strategies for face recognition is termed as hierarchical network in this study. We will cover the details of our training and testing datasets, face detection, proposed pre-trained model ResNet101 and the use of FaceNet embedding in the subsequent subsections.

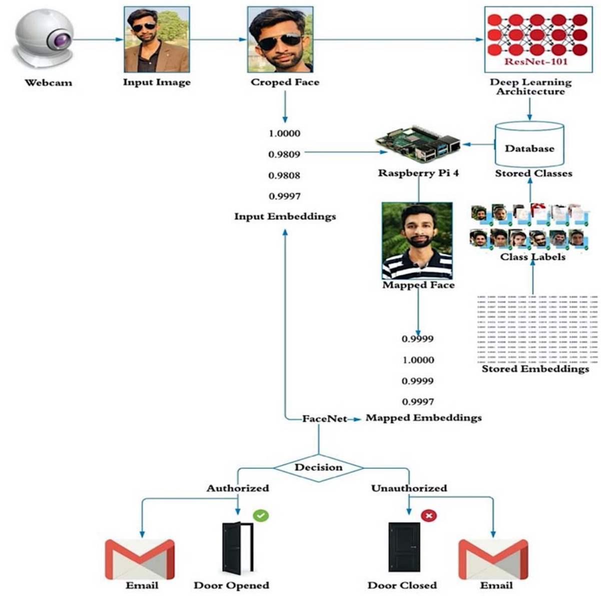


Fig 1: Proposed HN Framework

A) Dataset

We collected dataset from 12 students from Faculty of Engineering & Technology, University of Sindh in which each class contains 35 images for training and 15 images for testing purpose. The dimesons of each image were 3024×4032 JPEG format and images were taken with different poses at different places under the different lighting conditions to ensure more accuracy for recognition. Most of the existing studies evaluate their method on benchmark datasets which are collected in a scripted and controlled environment. It has been shown in existing studies that when experimenting with the faces in the wild, the recognition accuracy drops significantly [25,26]. Our work here uses a small amount of collected images to prove that the proposed network is able to deal with small volume of that as in the case with real applications. Secondly, it will be helpful to compare the performance with the existing works when we add some spoofed images from the Internet in testing scenarios which has not been performed in the existing studies to prove the applicability of their method in real-world setting.

B) Face Detection

Our face detection module is based on the ResNet as a base detector in single-shot detector (SSD) framework. We fine-tuned the ResNet with face detection dataset and benchmark (FDDB) [27] and Wider Face [28] datasets. We trained the network for 5000 iterations with stochastic gradient optimization (SGD) optimizer, a learning rate of 0.02, and a decay rate of 0.04, accordingly. The pre-trained model, i.e. (.caffemodel and .ptototxt.txt) is uploaded on [29]. The detected face using the fine-tuned network is cropped for further processing.

C) ResNet101

As discussed earlier, our recognition is based on two-tier strategy where to reduce the ambiguity we perform recognition using ResNet101 and based on the obtained results we only use the resultant user images for further authentication. ResNet101 pre-trained on Image-Net is a popular network and has been used widely for image recognition and analysis studies. In this work, we modify the ResNet101 network such that we break off the network at 210th layer, i.e. res4b12 and use two fully connected layers to fine-tune the network. We fine-tune the network with the learning rate of 0.02 in the first phase and 0.9 in the second so that the scaling of residuals during the training process could be stabilized. figure 2 shows the training result of ResNet101 model. We trained the network with 300 iterations, ADAM optimizer with default values and a batch size of 32.

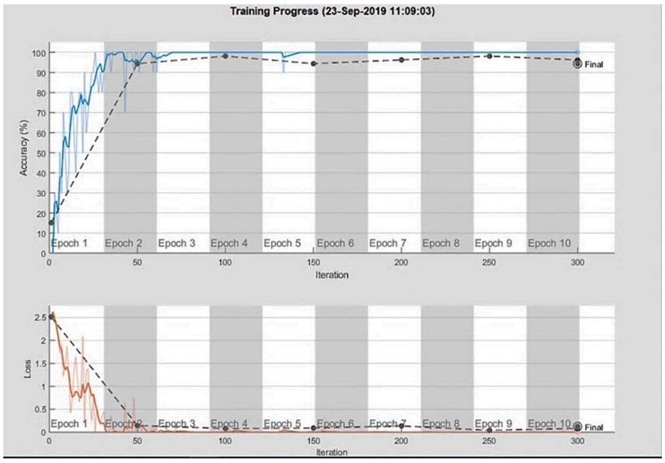


Fig 2: Training Result of ResNet101

D) Face Embeddings

The second tier involves the use of face embedding using FaceNet. It is used for obtaining main features from a person's face and give a result in 128 dimensional vectors that represent the most significant features of a human face called embedding [30]. To verify person's image whether it belongs to same person is present in database or not we have to compute face embeddings by using Euclidean distance formula. Euclidean distance is the distance between two points [31], in order to calculate input embeddings with present embeddings in database the formula will be,

$$d\,(q,p) = \sqrt{(q_1 - p_1)^2 + (q_{2} - p_2)^2 + \cdots + (q_n - p_n)^2}$$

$$= \sum_{i=1}^{n} (q_1 - p_1)^2$$

IV. Hardware and Software

E) Raspberry pi

The developed application of face recognition is installed in raspberry Pi 4, it is single board computer made by the Raspberry Pi Foundation in UK [32], It's GPIO interaction between the software and hardware. figure 3 shows raspberry pi 4 Model 2GB.

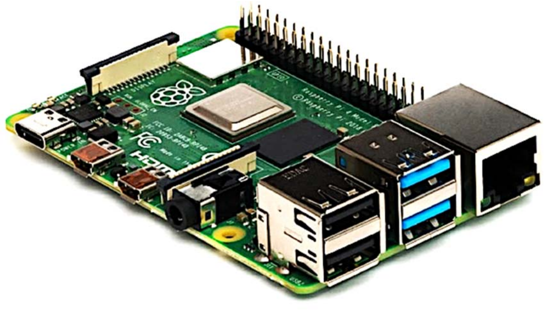


Fig 3: Raspberry Pi 4 Model (Source: Google Images)

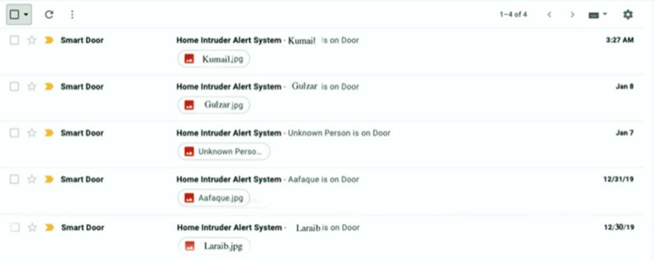
F) Servo Motor

Servo motor is rotating electric device used to control speed, torque and position it has an encoder which changes mechanical movement into the digital signals decrypted by a movement controller [33]. it uses closed loop system that uses position feedback to control its motion at any angle, here we have set an angle from 0 to 180 degree for sliding door. figure 4 shows picture of servo motor.

Fig 4: Servo Motor SG90 (Source: Pinterest Images)

G) Notification E-mail

When system become aware of individual either authorized or unauthorized standing infront of camera it will send an email alert to home owner with picture and name of the person who is trying to get in the home if standing person is known system will send an email with his name i.e "Aafaque" else it will send as "Unknown Person" with subject of "Home Intruder Alarm". following figure 5 shows emails received on home owner ID.


1–4 of 4

Smart Door	Home Intruder Alert System - Kumail is on Door Kumail.jpg	3:27 AM
Smart Door	Home Intruder Alert System - Gulzar is on Door Gulzar.jpg	Jan 8
Smart Door	Home Intruder Alert System - Unknown Person is on Door Unknown Perso...	Jan 7
Smart Door	Home Intruder Alert System - Aafaque is on Door Aafaque.jpg	12/31/19
Smart Door	Home Intruder Alert System - Laraib is on Door Laraib.jpg	12/30/19

Fig 5: Received Email on Owner ID

In this paper we have used Gmail for email service devolped by Google in which SMTP protocol has been used for transferring and receiving messages with port number 587.

V. RESULTS

In this section, we present the quantitative results of our proposed hierarchical network architecture for face recognition. We present the ablation results in table 1. The quantitative results show the face recognition accuracy using FaceNet as the baseline. We then use multiple pre-trained networks in our proposed framework to select the best one for further comparison. The testing has been conducted on the testing set of the collected dataset along with 50 random face images from the Internet assumed to be non-authorized users. We evaluate the FaceNet pipeline for developing a baseline to see whether the proposed work contributes to the better performance or not. The results show that the proposed framework is able to increase the performance of the baseline by ~15%.

Model	Recognition Accuracy
HN (ResNet101 + FaceNet)	87.36%
HN (DenseNet201 + FaceNet)	86.97%
HN (DarkNet19 + FaceNet)	83.62%
HN (GoogleNet + FaceNet)	82.29%
HN (ShuffleNet + FaceNet)	79.66%
HN (VGG19 + FaceNet)	74.85%
FaceNet (Baseline)	72.43%

TABLE 1: Ablation Results for Comparing Baseline with The Pre-Trained Architectures in The Proposed Framework

The enhancement in the recognition accuracy show the resilience of the proposed network to the random faces being used from the Internet. We further compare our results with existing works on the collected dataset and the results are shown in table 2. The reason for choosing the said studies for comparison is their availability of codes which ensures that the comparison would be fair enough to evaluate the recognition performance. It can be observed that the proposed work not only outperforms the shallow learning methods such as eigenfaces [34], HoG [35], laplacianfaces [36], and LBP [37] but also performs well in comparison to state-of-the-art methods.

Method	Recognition Accuracy
Eigenfaces [34]	63.19%
HOG [35]	66.45%
Laplacianfaces [36]	65.07%
LBP [37]	67.36%
Openface [38]	75.72%
Dense U-Nets [39]	81.43%
RetinaFace [40]	83.87%
HN (ResNet101+FaceNet)	87.36%

TABLE I: Comparison of Face Recognition Accuracy with Existing Works

We have developed user interface for recognition in which there is two portions as show in figure 6, left portion contains main three things, first is profile picture of authorized person with name and also have checkbox which gives an advantage to block or ban the person for period of time, second is cropped picture after recognition and last is 'Add New Person' button for that person who is not in authentication list and want to be authorized hence system will ask for his/her name and will take images training and testing purpose. While right side portion contains only real time view of webcam and when person as authorized system will show the authorized person on screen and also will speech the name.

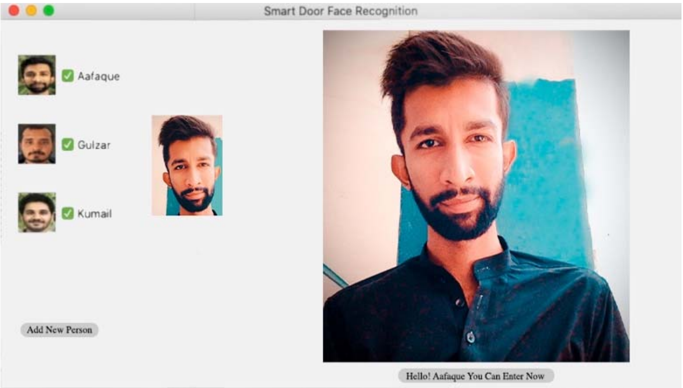


Fig 6: Face Recognition Interface

As we mentioned above, we have built a prototype to show the proposed work, final prototype is shown in figure 7.

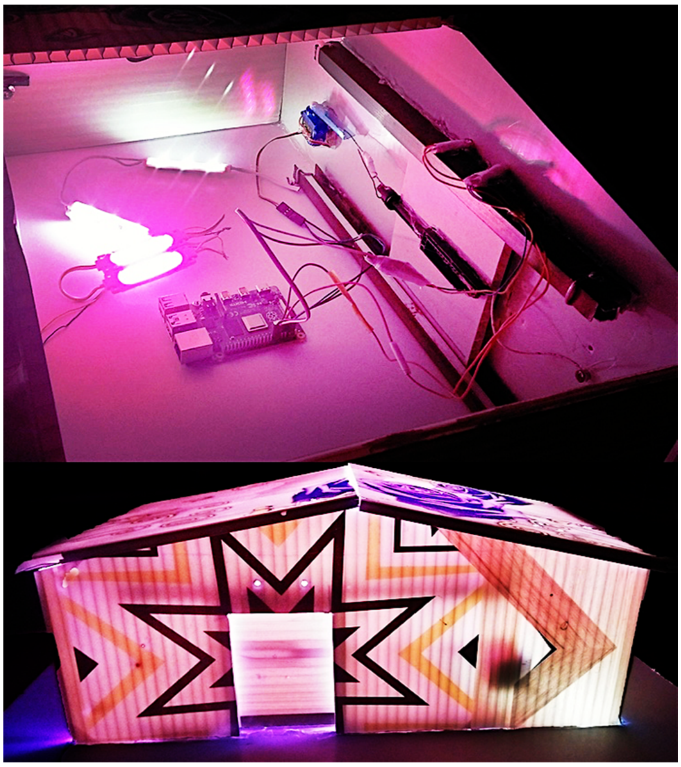


Fig 7: Final View of Prototype

VI. CONCLUSION

In this paper, we proposed a hierarchical classification network based on two-tier recognition systems. The first tier uses deep machine architecture ResNet101 for recognition and second tier uses FaceNet for authorization. We have also developed a prototype of a security system for home or offices to show the applicability of the proposed work in real-world settings. The equipment used in prototype was Raspberry Pi which is main hardware that have Debian OS is installed where developed recognition software is running over on it, servo motor is connected with raspberry pi to slide the gate for opening and closing purpose. The results show that when using the FaceNet alone, we achieve 72.43% accuracy and when transforming the FaceNet embedding in our proposed hierarchical classification framework the accuracy improves by 14.93%, respectively which supports our assumption of two-tier classification. Furthermore, we compared our proposed approach with the existing works when the spoofed images are added from the Internet. It is revealed that the existing works have lower resilience to the spoofing in comparison to the proposed approach which also proves our intuition to use two-tier classification approach. The results also comply with the existing studies using hierarchical network structure for improving the recognition performance.

VII. REFERENCES

[1] Khowaja, S., Shah, S., Shah, R. And Shah, A., “Dc Coefficients Comparison Based Approach For Fingerprint Identification System”, Sindh University Research Journal-Surj (Science Series), 47(1).

[2] Anuj, “The Importance of Security Systems.” Omkar Group India, omkargroupindia.com/importance-security-systems/, 4 May 2018

[3] Mdnasimuzzaman Chowdhury , “Access Control of Door and Home Security by Raspberry Pi Through Internet.”, projects-raspberry.com/access-control-of-door-and-home-security-by-raspberry-pi-through-internet/, 20 May 2015.

[4] Ketki Prasade et al., “Face Recognition Based Door Locking System”, International Research Journal of Engineering and Technology (IRJET), July 2018.

[5] R. Manjunatha et al., “Home Security System and Door Access Control Based on Face Recognition”, International Research Journal of Engineering and Technology (IRJET), March 2017.

[6] Khowaja, S.A., Dahri, K., Kumbhar, M.A. and Soomro, A.M., 2015, December. Facial expression recognition using two-tier classification and its application to smart home automation system. In 2015 International Conference on Emerging Technologies (ICET) (pp. 1-6). IEEE.

[7] Khowaja, S.A., Yahya, B.N. and Lee, S.L., 2017. Hierarchical classification method based on selective learning of slacked hierarchy for activity recognition systems. Expert Systems with Applications, 88, pp.165-177.

[8] Korshunov, P. and Marcel, S., 2018. Deepfakes: a new threat to face recognition? assessment and detection. arXiv preprint arXiv:1812.08685.

[9] Khowaja, S.A., Prabono, A.G., Setiawan, F., Yahya, B.N. and Lee, S.L., 2018. Contextual activity based Healthcare Internet of Things, Services, and People (HIoTSP): An architectural framework for healthcare monitoring using wearable sensors. Computer Networks, 145, pp.190-206.

[10] Khowaja, S.A., Khuwaja, P. and Ismaili, I.A., 2019. A framework for retinal vessel segmentation from fundus images using hybrid feature set and hierarchical classification. Signal, Image and Video Processing, 13(2), pp.379-387.

[11] Khowaja, S.A. and Lee, S.L., 2020. Semantic image networks for human action recognition. International Journal of Computer Vision, 128(2), pp.393-419.

[12] Khowaja, S.A. and Lee, S.L., 2020. Hybrid and hierarchical fusion networks: a deep cross-modal learning architecture for action recognition. Neural Computing and Applications, 32(14), pp.10423-10434.

[13] Hassan, Harnani, Raudah Abu Bakar, and Ahmad Thaqib Fawwaz Mokhtar. "Face acknowledgment dependent on auto-exchanging attractive entryway lock framework utilizing microcontroller." 2012 (ICSET). IEEE, 2012.

[14] J. Shankar Kartik Et al., "SMS Alert and Embedded Network Video Supervising Terminal", (IJSPTM) , October 2013.

[15] G.Senthikumar et al., “Embedded Image Capturing System Using Raspberry Pi System”, International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), April 2014.

[16] Lwin, H., Khaing, A., Tun, H."Automic door access system using face recognition”, International Journal Of Scientific & Technology Research, July 2015.

[17] C.A. Athira et al., "Security Alert using Face Recognition", International Journal of Advances in Computer Science and Technology, Vol. 5, No. 12, pp. 176-179, 2016.

[18] Mathew Meera, R S Divya, "Extravagantly Security Entryway System For Critical Zones", International Conference on Networks and Advances in Computational Technologies (NetACT), 20–22 July 2017.

[19] Ibrahim Mohammad et al., " Integrating Face Recognition Security System With the Internet of Things ", International Conference on Machine Learning and Data Engineering (ICMLDE). IEEE, 2018.

[20] Bhojane, Ketan J., and S. S. Thorat. "Face Recognition Based Car Ignition and Security System." International Research Journal of Engineering and Technology (IRJET) 5.05: 3565-3668, (2018).

[21] Awais et al., "Constant Observation Through Face Recognition Using HOG And Feedforward Neural Systems." IEEE Access 7 ,121236-121244 (2019).

[22] Sajjad et al. "Raspberry Pi helped outward appearance recognition system for shrewd security in law-authorization administrations." Information Sciences 479,416-431:(2019).

[23] Mamoon Tahnoon et al., "Face Recognition Security System Based on Convolutional Neural Networks", International Journal of Advanced Science and Technology, 2020.

[24] Jaiswal, Arvind, and Sandhya Tarar. "Realtime Biometric System for Security and Surveillance Using Face Recognition.", International Conference on Advances in Computing and Data Sciences Springer Singapore, 2020.

[25] Huang, G.B., Mattar, M., Berg, T. and Learned-Miller, E., 2008, October. Labeled faces in the wild: A database forstudying face recognition in unconstrained environments.

[26] Kushwaha, V., Singh, M., Singh, R., Vatsa, M., Ratha, N. and Chellappa, R., 2018. Disguised faces in the wild. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops (pp. 1-9).

[27] V. Jain and E. Learned-Miller, "Fddb: A benchmark for face detection in unconstrained settings," Tech. Rep.

[28] Sander-Ali. "Sander-Ali/Face_Detect_OpenCV_SSD." GitHub, github.com/sander-ali/Face_Detect_OpenCV_SSD.

[29] S. Yang, P. Luo, C.-C. Loy, and X. Tang, "Wider face: A face detection benchmark," in IEEE Conference on Computer Vision and Pattern Recognition, 2016, pp. 5525–5533.

[30] Ars Futura , "Face Recognition with FaceNet and MTCNN.", arsfutura.com/magazine/face-recognition-with-facenet-and-mtcnn/.

[31] AHDID1, R., 2016. Euclidean & Geodesic Distance Between A Facial Feature Points In Two-Dimensional Face Recognition System.

[32] Opensource, "What Is a Raspberry Pi?", opensource.com/resources/raspberry-pi.

[33] Blog CLR, "What Is a Servo Motor and When Is It Used", clr.es/blog/en/what-is-servo-motor-and-when-is-it-used/.

[34] Turk, M.A. and Pentland, A.P., 1991, January. Face recognition using eigenfaces. In Proceedings. 1991 IEEE computer society conference on computer vision and pattern recognition (pp. 586-587). IEEE Computer Society.

[35] Déniz, O., Bueno, G., Salido, J. and De la Torre, F., 2011. Face recognition using histograms of oriented gradients. Pattern recognition letters, 32(12), pp.1598-1603

[36] He, X., Yan, S., Hu, Y., Niyogi, P. and Zhang, H.J., 2005. Face recognition using laplacianfaces. IEEE transactions on pattern analysis and machine intelligence, 27(3), pp.328-340.

[37] Ahonen, T., Hadid, A. and Pietikainen, M., 2006. Face description with local binary patterns: Application to face recognition. IEEE transactions on pattern analysis and machine intelligence, 28(12), pp.2037-2041.

[38] Amos, B., Ludwiczuk, B. and Satyanarayanan, M., 2016. OpenFace: A general-purpose face recognition library with mobile applications.

[39] Guo, J., Deng, J., Xue, N. and Zafeiriou, S., 2018. Stacked dense u-nets with dual transformers for robust face alignment. arXiv preprint arXiv:1812.01936.

[40] Deng, J., Guo, J., Zhou, Y., Yu, J., Kotsia, I. and Zafeiriou, S., 2019. Retinaface: Single-stage dense face localisation in the wild. arXiv preprint arXiv:1905.00641.