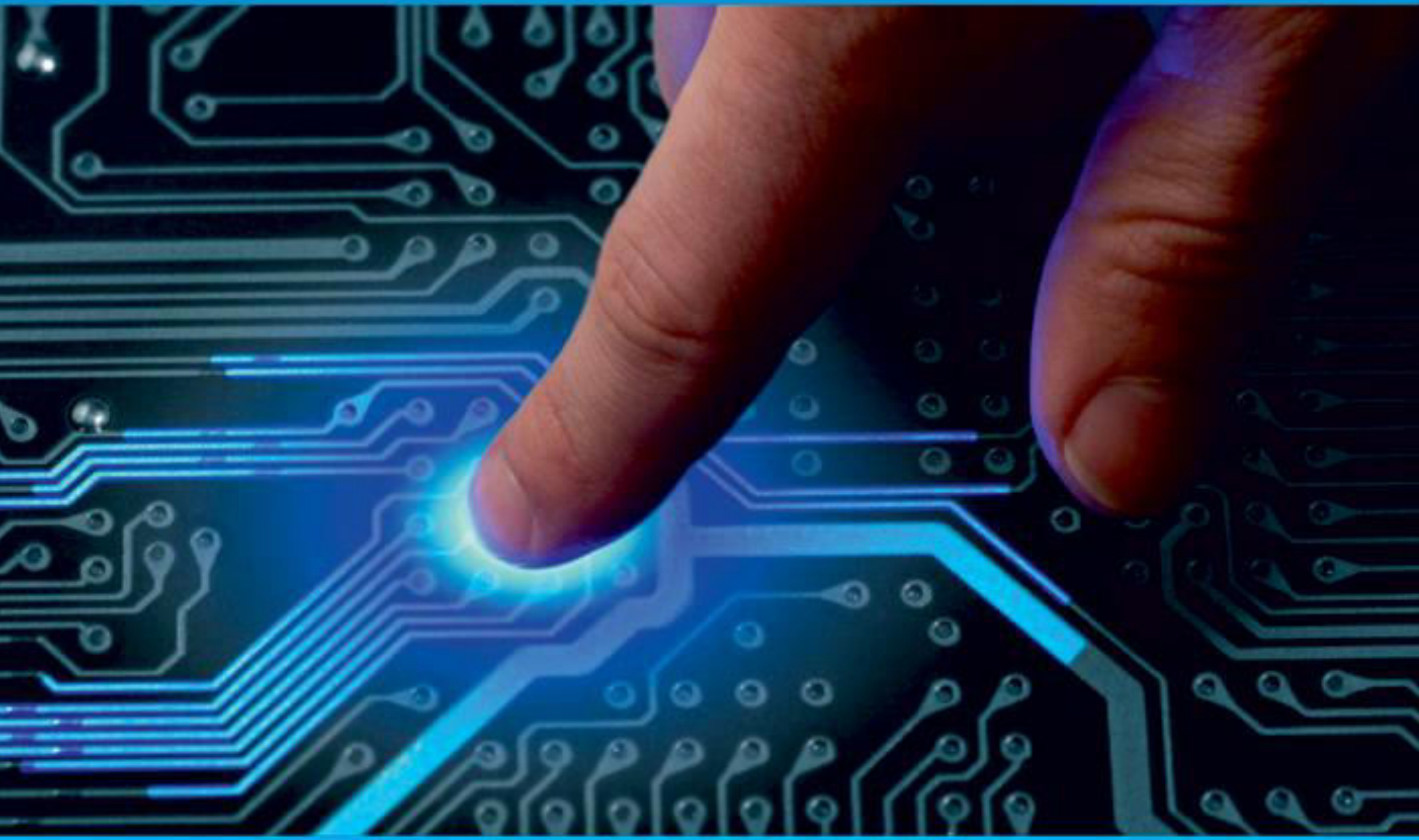
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 10, Issue 9, September 2022

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.165

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165

|| Volume 10, Issue 9, September 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1009007 |

Enhanced Security Features of ATM through Face Recognition

Prof. Md. Irshad Hussain B[1], Chandan Nimbalkar B R[2]

Professor, Department of Master of Computer Application, UBDTCE, Davangere, India[1]

PG Student, Department of Master of Computer Application, UBDTCE, Davangere, India[2]

ABSTRACT*:* Currently, ATMs have widespread popularity among customers. However, people often forget their ATM cards or their PIN numbers because they find them cumbersome to carry around. It's possible for the ATM card to get broken, leaving consumers without access to their funds. Instead of using a PIN and an ATM card, we propose using biometric identifiers for authentication. Because of the success of combining various biometrics, Face ID is given top billing in this context. There is a risk that unauthorised individuals will be able to access ATMs by using a valid PIN. Images captured in front of the ATM are compared to those stored in a database to ensure the identities of the users. If the user can be verified, the updated image is utilised to fine-tune the model's predictions. The acquired image is processed by openCV, and then the faces are identified with the help of the Haar Cascade Classifier. Local Binary Pattern is used for the facial recognition.

I.INTRODUCTION

A computerised machine that allows customers to withdraw cash from their own bank accounts is called an Automatic Teller Machine (ATM). In light of the fact that ATMs are widely used in the financial industry, banks are placing a strong emphasis on safeguarding these machines. Therefore, adequate safety measures should be taken to prevent theft or damage to ATMs.

Future technologies are being constructed with robust safety measures because of the rapid progress in science and technology. However, there are various dangers that could compromise this safety. A number of financial organisations, including banks, and apps, including ATMs, are still vulnerable to theft and fraud, despite improvements in automation. Existing ATM models rely on cards and PINs, which opens the door to theft, poorly chosen PINs, card duplication, and other security risks. And then there's the even bigger issue of PIN hacking. Fraudulent attacks such as eavesdropping, spoofing,abuse of system resources; a form of blackmail against the user. Thefts from automated teller machines are also a possibility. The 'ATM Security system based on Facial recognition, PIN and OTP' project uses a combination of traditional features, such as the Personal Identification Number (PIN), and innovative features, such as face recognition and a one-time password (OTP), to solve these issues. Users' account information, including photos of their faces and mobile phone numbers, is stored in a database, which significantly increases security.

At the outset, the customer visits the ATM, where a live image of them is recorded through Web Camera.

system definition interface, such as an automated teller machine, whose images are checked against those in a database. Upon facial recognition, the user is prompted to enter their PIN. A one-time password (OTP) will be sent to the user's verified cellphone number if the PIN is a match. With a correct OTP entry, the transaction can be finalised. Thus, a face recognition algorithm, personal identification number (PIN), and one-time password (OTP) greatly lessen the likelihood of fraud. A linear discriminate classification algorithm based on deep learning is used to improve accuracy. And I ran the same command in OS.

II.LITERATURE SURVEY

Face recognition and tracking [1-2] have been used for a variety of purposes, including surveillance, security, human-computer collaboration, etc. Various face recognition methods are discussed in the literature, such as the Viola Jones method, the Haris corner method, the Principal Component Analysis method, and the Haar classifier. In this analysis, we use a face-recognition system based on a Haar classifier derived from the Viola Jones algorithm. Using MATLAB and a Raspberry pi, we are able to identify the Eigen features of a person's face in order to track its whereabouts. The motivations behind criminal distinguishing proof and affirmation are typically based on computational models of face area and face affirmation. Various fields, including perception, security, human-computer interaction, and others, have looked to the popularity and surface area of faces for ideas. This paper uses a Raspberry PI modified with image processing software to demonstrate the situation by activating an LED upon detection of a face[2]. In the future, signals may be used to operate various devices. In addition, this programme can only be used for "single-person face following," for obvious reasons. We may decide to expand it into a multi-user system in the near future.

In this article, authorization to access the system might be granted solely by a selected client speaking into an amplifier connected to the framework. The proposed framework will then decide whether the word is "On" or "Off" in that situation. We'll use the selected voice to trigger Arduino's automatic transfer and, from there, the motor's starter motor. The suggested framework utilises a grouping framework based on Support Vector Machines in order to differentiate between acceptable and unacceptable terms .[1]

Programming solutions that make use of optimised OpenCV executions can achieve 1.78 FPS(Frames Per Second) on VGA image sizes [6]. An alternative is to use a machinery method, which expedites the calculating estimation by making use of an application-specific programme. For relatively small images, it can reach frame rates of up to 15 FPS. Using a Microblaze delicate core processor from Xilinx, Nair et al. [8] fostered a group identification inserted framework that achieved around 2.5 FPS for 216 x 288 pixel images. Gao et al. [7] suggested an FPGA setup tailored specifically for computing highlight classifiers.

Mobile phone featuring Bluetooth accessory, SMS, and camera [9, 10]. So that users can make their mobile devices function as personal computers, it has been built into and made available on a number of popular chip sets. Short Message Service (SMS) is an interchanges standard facilitating the exchanged of short instant messages between cell phone gadgets. The framework might start the engine by sending an SMS from the phone. In this case, an external BJT circuit is used to activate the motor. The plan is for the user to activate the motor with their mobile device .[10]

Automobile owners are increasingly opting for remote ignition systems. In the hands of precise timekeepers, such as another boss who is always late for work, time takes on new significance and value. Auto hardware plays an important role in the automobile industry, providing luxurious extras and addressing safety and security issues [3]. Our goal in this paper is to provide a workable solution to the problem of designing and developing an event information recorder, a request that has come mostly from the aviation sector in light of the corresponding benefits.

Biometrics, seeing humans in videos, and communicating with computers all benefit greatly from face recognition. We demonstrate the fastest known FPGA implementation of the Viola-Jones face identification calculation executed on a cluster of graphics processing units. While the GPU architecture provides significantly cheaper development, the FPGA implementation has reduced power requirements .[6]

III. TECHNOLOGY OVERVIEW

The Facial Recognition Based Car Ignition and Security System could have face recognition as one of its primary functions. The verified customer's essence has been picked out using a Haar-like feature in order to provide a risk-free environment for starting and entering the car.

It's possible that highlighting extraction as part of a face recognition and identification approach is a fundamental human facial characteristic. Ada's computational assistance allows for the identification of individual faces.

In order to determine whether or not a picture contains a face, Ada-Boost learning is used to select a small number of weak classifiers and combine them into a strong classifier. Next, the Haar Classifier calculation is used to recognise the selected faces by comparing the current face's HaarClassifer to a database of previously identified faces. The Haar Cascade is a mathematical formula used by artificial intelligence for object recognition in still images and moving video.

In order to achieve a risk-free environment for starting and entering the vehicle, a haar-like component has been used to identify and sense the essence of the confirmed client, and a typical rectangular haar-like element can be seen to look like this:

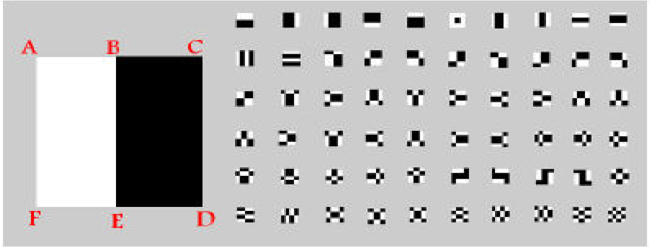
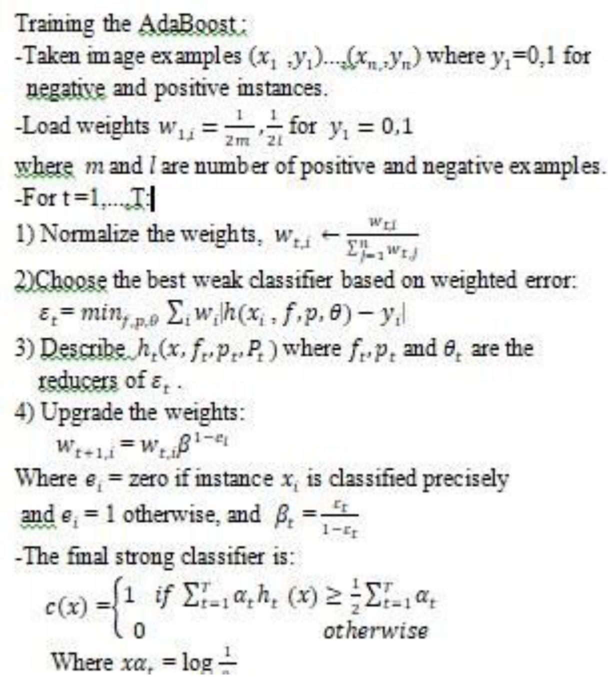


Fig.1.Haar-like Features

The first step is to identify the face, after which the grayscale image will be annotated with a rectangle indicating the location of the identified face. Training on a large dataset of photos, which should be saved as ayml file, is required before a face recognition process can begin. When a face is identified in real time through a webcam, it is compared to the trained photographs saved in ayml file, and only those that are an exact match are displayed. A signal is sent to the microcontroller once the face has been confirmed to belong to a certain person.



Training the AdaBoost:

-Taken image examples $(x_1, y_1)\ldots(x_n, y_n)$ where y_1=0,1 for negative and positive instances.

-Load weights $w_{1,i} = \frac{1}{2m}, \frac{1}{2l}$ for $y_1 = 0,1$

where m and l are number of positive and negative examples.

-For t=1,...,T:

1) Normalize the weights, $w_{t,i} \leftarrow \frac{w_{t,i}}{\sum_{j=1}^{n} w_{t,j}}$

2)Choose the best weak classifier based on weighted error:

$\varepsilon_t = min_{f,p,\theta} \sum_i w_i |h(x_i, f, p, \theta) - y_i|$

3) Describe $h_t(x, f_t, p_t, P_t)$ where f_t, p_t and θ_t are the reducers of ε_t .

4) Upgrade the weights:

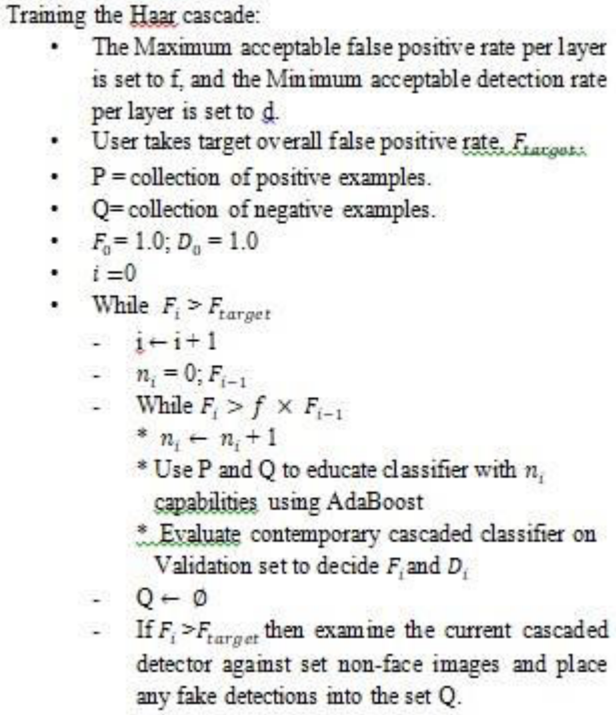
$w_{t+1,i} = w_{t,i}\beta^{1-e_i}$

Where e_i = zero if instance x_i is classified precisely and e_i = 1 otherwise, and $\beta_t = \frac{\varepsilon_t}{1-\varepsilon_t}$

-The final strong classifier is:

$$c(x) = \begin{cases} 1 & if \sum_{t=1}^{T} \alpha_t h_t(x) \geq \frac{1}{2}\sum_{t=1}^{T} \alpha_t \\ 0 & otherwise \end{cases}$$

Where $x\alpha_t = \log \frac{1}{}$



```
Training the Haar cascade:
  • The Maximum acceptable false positive rate per layer
    is set to f, and the Minimum acceptable detection rate
    per layer is set to d.
  • User takes target overall false positive rate, $F_{target}$.
  • P = collection of positive examples.
  • Q= collection of negative examples.
  • $F_0$= 1.0; $D_0$ = 1.0
  • $i$ =0
  • While $F_i > F_{target}$
    -  $i \leftarrow i + 1$
    -  $n_i = 0; F_{i-1}$
    -  While $F_i > f \times F_{i-1}$
         * $n_i \leftarrow n_i + 1$
         * Use P and Q to educate classifier with $n_i$
           capabilities using AdaBoost
         * Evaluate contemporary cascaded classifier on
           Validation set to decide $F_i$ and $D_i$
    -  Q ← ∅
    -  If $F_i > F_{target}$ then examine the current cascaded
       detector against set non-face images and place
       any fake detections into the set Q.
```

Webcams are used to take pictures of people at the present moment, and those pictures are compared to those already stored in a folder. Once a user's face has been verified, the API is contacted to have a One-Time Password (OTP) sent to their registered mobile number; once this OTP has been validated, the user is free to complete the desired transaction.

To turn on the webcam on the front end, we'll be using the bootstrap framework, which has several pre-defined classes that can be used to create simple, responsive web pages. To get a picture of their own faces, users will use JavaScript that can be called upon by a webcam. After users take a photo of their faces, they must transmit it to a server running Python's Flask ajax framework, where it will be read and compared against a previously trained model; if a match is detected, users will be prompted to input an OTP. After the OTP has been verified, the transaction page is displayed.

The python face recognition module, which uses dlib to predict facial features, will be utilised during the face recognition procedure. Given its reliance on deep learning, a 92% success rate seems reasonable. Ansms gateway will be utilised to send out one-time-passcodes to customers.

Flask webserver:

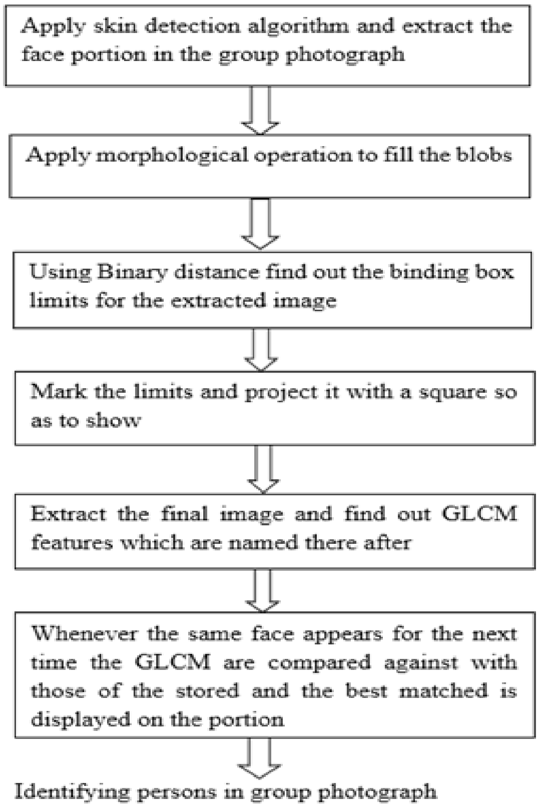
Python's Flask is a tiny web framework. It is considered a micro framework because it does not need any other libraries or tools to function. None of the standard features such as a layer for abstracting databases or validating user input are included. Flask, on the other hand, allows for the use of extensions to add functionality to an app as though it were built into Flask itself. Common framework-related tools like as ORMs, form validators, upload managers, and a wide range of open authentication systems all have extensions..

Data storage:

MySQL stores all data and is great for decentralised applications. The suggested system's ability to perform database transactions without the use of any additional drivers or features is a major plus.

Based on the client-server paradigm, this system necessitates no supplemental client-side software for proper operation. MySQL is utilised for all truncations, with no other applications involved in the user-system exchange.

IV. METHODOLOGY


Apply skin detection algorithm and extract the face portion in the group photograph
Apply morphological operation to fill the blobs
Using Binary distance find out the binding box limits for the extracted image
Mark the limits and project it with a square so as to show
Extract the final image and find out GLCM features which are named there after
Whenever the same face appears for the next time the GLCM are compared against with those of the stored and the best matched is displayed on the portion
Identifying persons in group photograph

Skin Detection Algorithm

The face in a digital photograph is located using an algorithm designed to identify skin. The higher the quality of the photograph, the more accurate the recognition will be. Extracting the face from a photograph can be done in a number of different ways, some of which are simpler than others. We take one of these methods and use it to pull out the faces from the supplied input image. One can infer the following from the illustration: A non-color-specific input image can contain a wide range of colours. In this method, colour data will be utilised heavily during the image extraction process. This strategy is getting a lot of attention these days. At the point where segmentation of images reveals the diseased area for further study. The image has a wealth of information that can be mined for insights. The process of dimensionality reduction is essential. For the sake of avoiding model-related conflicts and misunderstandings It is also crucial to think about all that is required and not forget anything. One of the most important phases of machine learning is feature extraction. Identifying and removing superfluous details is crucial. The choice of features is crucial in preventing either overfitting or underfitting. Randomness, mean, entropy, and the standard deviation of the colour image are just few of the properties recovered in this research.

Morphological Operations

To complete the input image, morphological operations must be performed to fill in the blanks. The most common morphological transformations are dilation and erosion8. The pixels will be processed in both procedures. Maximum values are the focus of dilation, whereas minimum values are the focus of erosion. When we apply the binary distance method to an input image, we get a bounding box that places restrictions on where we can look for the image's edges. Using the bounds, a square representing the tracked face is superimposed on the original image.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165

|| Volume 10, Issue 9, September 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1009007 |

Grey Level Co-occurrences Matrix for Face Detection

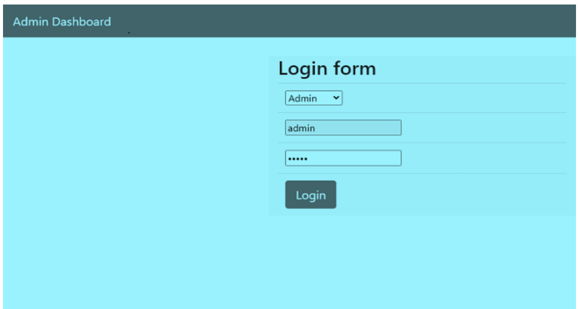
Next, we need to figure out how to get the face out of the picture so we can identify the person. GLCM was one of the first methods developed for extracting texture features9. We will use the facial attributes that were extracted from the faces. As soon as the detected attributes have been retrieved, a square projection of them is superimposed on the group photo

V. CONCLUSION

With each new advancement in ATM technology, criminals have come up with more ingenious ways to steal money. The fact that anyone who learns the PIN can access the funds is the system's biggest drawback. Face-id serves as a solution to this problem. The main value of biometrics lies in the fact that they are truly individual. The suggested improvement is not a substitute for the current method of protecting ATMs. The new idea is seen as a supplement to the standard procedure.

The proposed system is an effort to leverage AI and Computer Vision to create a practical product for the banking industry. It involves maintaining a database of customers along with photographs of their faces, then using those photos to train a model to recognise their faces at ATMs.

VI. RESULTS



Admin Dashboard

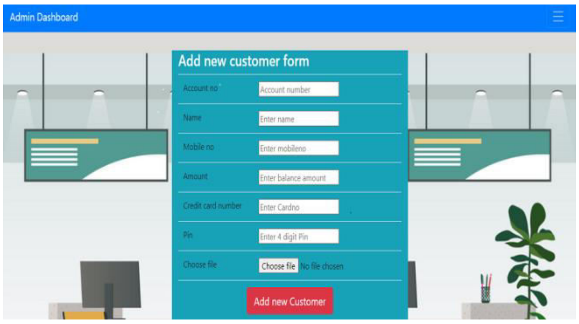
Login form

Admin

admin

•••••

Figure 2: Admin login form



Admin Dashboard

Add new customer form

Account no: Account number

Name: Enter name

Mobile no: Enter mobileno

Amount: Enter balance amount

Credit card number: Enter Cardno

Pin: Enter 4 digit Pin

Choose file: Choose file No file chosen

Figure 3: Form used to create customers

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165

|| Volume 10, Issue 9, September 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1009007 |

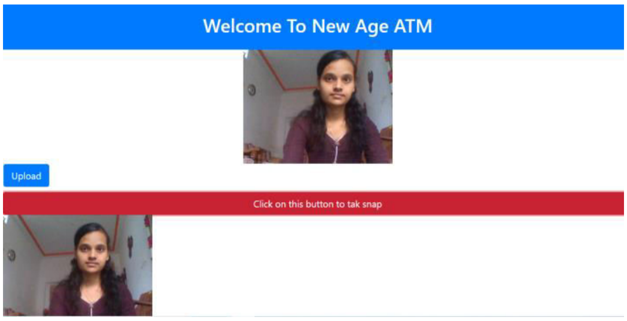
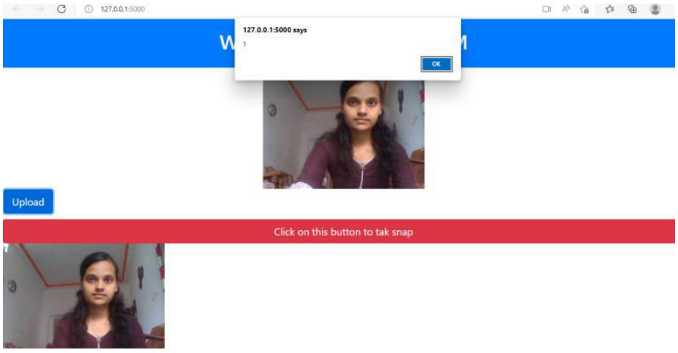


Figure 4: Form used to verify face


127.0.0.1:5000 says

1

Figure 4: Form showing result of face verification

REFERENCES

[1] W. Astuti and E. B. WahyuRiyandwita, "Intelligent automatic starting engine based on voice recognition system," 2016 IEEE Student Conference on Research and Development (SCOReD),2016,pp.1-5,doi:10.1109/SCORED.2016.7810061.

[2] Shah, Z. A. Zaidi, B. S. Chowdhry and J. Daudpoto, "Real time face detection/monitor using raspberry pi and MATLAB," 2016 IEEE 10th International Conference on Application of Information and Communication Technologies (AICT), 2016, pp. 1-4, doi: 10.1109/ICAICT.2016.7991743.

[3] C. Patil, Y. Marathe, K. Amoghimath and S. S. David, "Low Cost Black Box for Cars," 2013 Texas Instruments India Educators' Conference, 2013, pp. 49-55, doi: 10.1109/TIIEC.2013.16.

[4] S. Chaklader, J. Alam, M. Islam and A. S. Sabbir, "Black Box: An emergency rescue dispatch system for road vehicles for instant notification of road accidents and post crash analysis," 2014 International Conference on Informatics, Electronics & Vision (ICIEV), 2014, pp. 1-6, doi: 10.1109/ICIEV.2014.6850749.

[5] J. A. Lopez Leyva and V. D. AjasTerriquez, "Car Black Box System (CBBS) Using FPGA for Determine the Car orientation: Preliminary Results," 2014 International Conference on Mechatronics, Electronics and Automotive Engineering, 2014, pp. 125-128, doi: 10.1109/ICMEAE.2014.20.

[6] Daniel Hefenbrock, “Accelerating Viola-Jones face detection to FPGA-level using GPUs,” Proceedings of the 2010 IEEE, 18th Annual International Symposium on Field-Programmable Custom Computing Machines, 2010, pp.11-18.

[7] C. Gao and S.-L. Lu, “Novel fpga based haar classifier face detection algorithm acceleration,” in Field Programmable Logic and Applications, 2008. FPL 2008. International Conference on, Sept. 2008, pp. 373–378.

[8] V. Nair, P.-O.Laprise, and J. J. Clark, “An fpga-based people detection system,” EURASIP J. Appl. Signal Process., vol. 2005, pp. 1047–1061, 2005.

[9] H. H. B. Aziz, N. H. A. Aziz and K. A. Othman, "Mobile phone car ignition system using EmbededBlue 506 Bluetooth technology," 2011 IEEE Control and System Graduate Research Colloquium, 2011, pp. 70-76, doi: 10.1109/ICSGRC.2011.5991832.

[10] J. Karim, W. M. A. B. W. Amat and A. H. A. Razak, "Car Ignition System via Mobile Phone," 2009 International Conference on Future Computer and Communication, 2009, pp. 474-476, doi: 10.1109/ICFCC.2009.116.

[11] 11. J.J.Patoliya, M.M. Desai, "Face Detection based ATM Security System using Embedded Linux Platform ", 2nd International Conference for Convergence in Technology (I2CT), 2017.

[12] 12. M.Karovaliyaa, S.Karediab, S.Ozac, Dr.D.R.Kalbande,"Enhanced security for ATM machine with OTP and Facial recognition features", International Conference onAdvanced Computing Tech- nologies and Applications(ICACTA), 2015.

13. Sivakumar T. 1 , G. Askok 2 , k. S. Venuprathap, "Design and Implementation of Security Based ATM theft Monitoring system", International Journal of Engineering Inventions, Volume 3, Issue 1, 2013.

14C. Bhosale, P. Dere, C. Jadhav, "ATM security using face and fingerprint recognition", Interna- tional Journal of Research in Engineering, Technology and Science, Volume VII, Special Issue, Feb 2017.

15. Manoj V , M. Sankar R , Sasipriya S , U. Devi E, Devika T ,"Multi Authentication ATM Theft Prevention Using iBeacon", International Research Journal of Engineering and Technology (IRJET).

16. L. Wang,H. Ji, Y. Shi, " Face recognition using maximum local fisher discriminant analysis",18th IEEE International Conference on Image Processing, 2011.

17. K.Shailaja and Dr.B.Anuradha, "Effective Face Recognition using Deep Learning based Linear Discriminant Classification ", IEEE International Conference on Computational Intelligence and Computing Research, 2016.

18. H. R. Babaei, O. Molalapata and A.H.Y Akbar Pandor, "Face Recognition Application for Au- tomatic Teller Machines (ATM)", International Conference on Information and Knowledge Manage- ment (ICIKM), 2012.

19. https://docs.opencv.org/2.4/modules/contrib/doc/facerec/facerec-tutorial.htmlface- recognition

20.https://www.superdatascience.com/opencv-face-recognition/

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

☎ 9940 572 462 6381 907 438 ✉ ijircce@gmail.com

www.ijircce.com

Scan to save the contact details