

Authentication Security System Based on Multimodal Biometric Features

Pooja J. Hajare ¹, Mrs. S. S. Patil ²

¹ Dept of E&TC

²Professor, Dept of E&TC

^{1,2} Ashokrao Mane Group of Institutions, Vathar tarf Vadgaon, Kolhapur Maharashtra, India,

Abstract- *Biometrics is used to authenticate the person's identity. As we all know, many security systems are available which consumes high power. Given paper helps to prevent or provide security in highly restricted area with less power consumption. In this multimodal biometric security system consists of many locking steps are available.. This proposed system provides security by using different biometric features like face recognition, signature verification and through fingerprint. In this proposed system database that is data to be verified is already registered. The register data consist of name, photo, signature, fingerprint etc. and having unique number. Matlab software is used for programming of face identification signature identification and verification of signature.*

Keywords- Biometric features ,Authentication system, Dynamic face recognition, Signature module ,Finger print module, Matlab, Arduino platform.

I. INTRODUCTION

Nowadays, security system is an important role, and in the future it may also be used in homes, healthcare centers, banks etc. As the world is not getting safer plays to feel secure that is to avoid thievery. Using this our proposed security system we can avoid thefts and can provide security to the place as well as we can provide security to confidential data or information. This biometric security system can also play the role of key to cryptography. Biometrics is a technology used to verify human characteristics. There are different characteristics like palm print, fingerprint, retina, DNA, Iris, gait movement, smell, signature and voice too. In this multimodal biometric security system, we use of combination of minimum two biometrics feature. Here we can make many grouping like of face and eye iris, combination of signature and palm print combination of retina and face etc. Use of multimodal that is combination of two biometric features, is always better than single one, as it acts a powerful lock to the system. This proceeding system is combination of face identification, signature verification and fingerprint verification.

II. EXISTING SYSTEM

In the existing security system face recognition, signature verification or fingerprint verification from only single feature is considered and provides security to the system. Here this all security verification is used. We have proposed managing the security of the authentication system based on multimodal Biometric features that provide high security to the system.

III. PROPOSED WORK

The mostly use of this proposed system can be done in banks for locker system. In the proposed system, initially user has to register in the system via face, signature and fingerprint. The information of all the registered users is saved into the database. The database will contain person's photo, signature, fingerprint which will be stored permanently. Arduino platform performs very crucial task tasks like controlling the different devices. Here face identification and signature verification done by using MATLAB software. For fingerprint verification the system uses arduino software for controlling. For security management, from face recognition and signature image verification at least one case should be passed then only user is allowed for second verification i.e. fingerprints verification. If face recognition or signature image verification test will not be done successfully then system will not move for second verification. Now second verification test is done successfully then user will be allowed to enter the restricted area. If second verification test fails then user will not be allowed to enter the restricted area. From three cases fingerprint verification should be compulsorily passed if this case is not passed then person will not be allowed to enter the restricted area.

At first verification, camera will take either the image of a person's face or signature which is to be verified. Use eigenface algorithm is used to verify the captured image of a person's face or signature and image already present in database. If a match occurs then first verification test of either face recognition or signature verification will be passed by authorized person. After that second step, verification of authorized person through finger print module will be done.

The person's are verified by comparing the stored finger characters and scanned finger characters. If a match found then person will be successfully authorized. These two verifications done successfully, then relay driver circuit will turn on and a person will be allowed to enter the restricted area e.g. bank locker room.

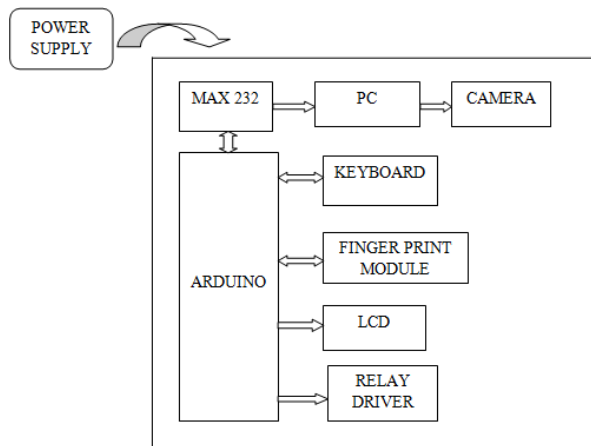


Fig 1: Block Diagram

The block diagram of design Security Management of Authentication System based on multimodal Biometric Features. In this system requires power supply, Arduino platform, MATLAB software, Finger print module, LCD display, relay driver. In which location higher security is required in that place this system can be used. The use of this system can be done in banks for locker system.

IV. METHODOLOGY

A. Registration of Biometric information

In the proposed system, initially user has to register in the system via face and/or signature and fingerprint. This database is used and it contains a person's photo, signature, fingerprint which will be stored permanently. Here arduino platform handles the devices. Here MATLAB software is used which identifies face and signature. For fingerprint verification the system uses arduino software for controlling.

(i) Face Registration

Initially if user is not registered or not found in the system, we have to register the user in to the system by turning on the camera and stored in the database.

(ii) Signature Registration

After registration of user face signature registration should be carried out by capturing image of signature so that it can be registered in the database.

(iii) Fingerprint Registration

After registration of face and signature, the next step is to register fingerprint scanning module is ready to scan the user's fingerprint. Arduino software helps to assign memory location of that user. Then user should put his/her finger on that fingerprint screen. After taking finger pressed against the scanner and storing it on the image buffer. Then convert into an array and then stores in arduino memory. Arduino grants unique identification number to each user after registration.

B. Implementation

After successfully registration of users information now user can enter into restricted area after verification of user's information.

For entering into restricted area user has to go through verification process. Here from face recognition and signature verification at least one case should be passed then only user is allowed for second verification i.e. fingerprints verification. If face recognition or signature verification test will not done successfully then system will not move for second verification. Now second verification test is done successfully then user will be allowed to enter the restricted area. If second verification test fails then user will not be allowed to enter the restricted area. From three cases fingerprint verification should be compulsorily passed if this case is not passed then person will not be allowed to enter the restricted area.

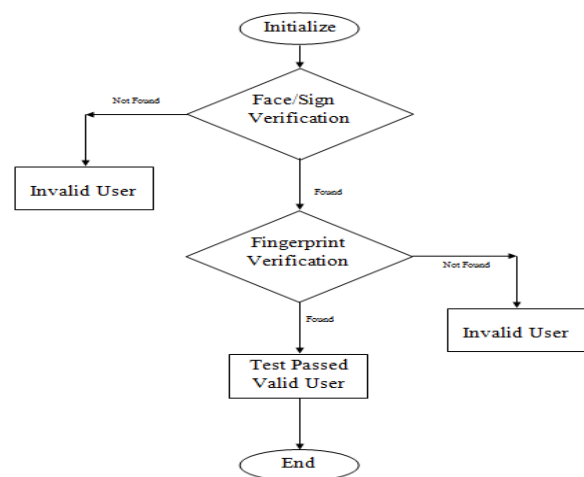


Fig 2: Flow Chart of system

These two verifications done successfully, then relay driver circuit will turn on and a person will be allowed to enter the restricted area e.g. bank locker room.

(i) Face / Signature image Verification

Initially recognition of face / Signature from the input image is important. For detecting face / Signature, we need an existing database of faces / Signature. Compare the result of input image of a face / Signature flatten it into a vector and calculate the Euclidean distance between it and all of the other flattened image in our database.

Steps:

- Resize all M faces to $N*N$.
- Remove average.
- Create matrix A of faces each row $N * N$, total size of A is $(N * N) * M$.
- Calculate average face.
- Remove average face from A.
- Calculate $[C * A' * A]$, covariance matrix, where C size is $M * M$.
- Calculate eigenvalues and eigenvectors, to Calculate the eignefaces need to go back to higher dimension.
- Calculate each original face's linear combination.
- Given new face project it to eigenface and compute distance to each eigenface this is the recognition.

(ii) Fingerprint Verification

The user needs to scan his finger by scanner and the system detects that person is registered or not. In the system used R305 fingerprint scanning module. Also 16X2 LCD display is need to display the information.

(a) Fingerprint Enrolling

- Initially, take the image of fingerprint and save into image buffer and then convert it into an array.
- Then convert it into 256 bytes and each stored into character buffer.
- Make template file of 512 bytes and store with assigning an ID to each of the template stored.



Fig 3: Scanned image

(b) Fingerprint Matching

- Initially, take the image of finger pressed against the scanner and then store into image buffer and then convert it into an array.
- Then matching it against the templates stored onto the device.
- When match found then it returns the template ID otherwise it returns the error that presents match not found.

After preceding the results of fingerprint module relay driver indicated weather user can enter into restricted area.

V. RESULTS

A. Face Recognition

The implemented system makes use of non moveable camera, which helps to avoid false user for verification. Most important factor in face recognition is accuracy or clarity of picture image, if the picture quality or clarity is good the calculating time required is less. Implemented system captures image from front view as this algorithm mainly focuses on nose, eyes of user. Only Eigenface algorithm is used for matching of image. Figure 4 shows the result of face recognition.



Fig 4: Verify User

B. Signature Recognition

Implemented system uses multimodal biometric system which helps to get accurate results. Signature image

used can be of any ink color. Implemented system uses Euclidean distance with Eigenface algorithm for matching. Figure 5. shows the result of signature verification.



Fig 5: Verify User's Signature

C. Fingerprint Recognition

Before fingerprint recognition only one verification of face or signature is required and then fingerprint verification will be started. Here arduino platform used to recognize the input fingerprint is registered or not. Figure 6 shows the result of fingerprint recognition.

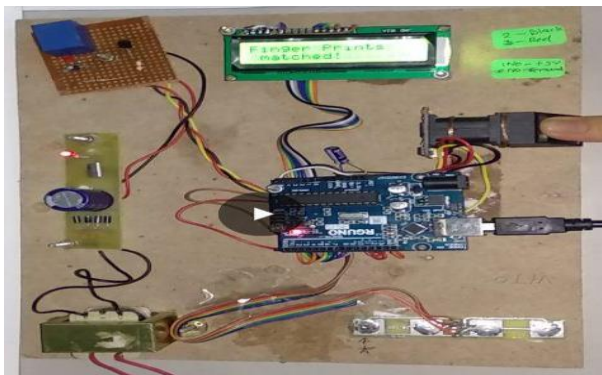


Fig 6: Fingerprint Matched

D. Performance Analysis

In the Figure 7 column represents each user distance is measured against view angle respectively. It is observed that the user got the smallest value than the others for all viewing direction from the distance varies and the threshold of the authentication system is set. Our experimental results describes that we can successfully use this system to unlock image verification of face or signature and fingerprint.

user/angle	45 degree	90 degree	135 degree
USER 1	1.00e+06	3.10e+07	2.30e+07
USER 2	2.20e+07	4.60e+07	3.90e+07
USER 3	3.60e+07	3.10e+07	2.30e+07
USER 4	2.70e+07	4.70e+07	3.30e+07
USER 5	3.66e+07	3.50e+07	3.12e+07
USER 6	9.20e+06	9.80e+06	9.60e+06
USER 7	3.04e+07	4.00e+07	3.50e+07
USER 8	2.9e0+07	3.30e+07	3.20e+07
USER 9	1.70e+06	2.20e+06	1.90e+06
USER10	2.90e+07	3.90e+07	3.35e+07

Fig 7: Experimental results

F. Experimental Setup



Fig 8: Experimental Setup

VI. CONCLUSION

Biometric identification management systems other higher security, convenience, accountability, and accurate audit trails all attributes that motivate businesses to research and implement the technology for their own use. Implemented system provides higher security due to multimodal biometric verifications. The working environment for implemented system is MATLAB software for face and signature verification and fingerprint verification by arduino. Arduino handles the systems devices. Here face or signature and fingerprint verification is available so no any unauthorized user can enter into the restricted area. As time goes forward, biometric technology implementation will grow and be used in different security areas.

VII. FUTURE SCOPE

In future system will grow with new different and high security technologies and memory capacity of fingerprint module will be increased. Flash memory of 1MB can be used for fingerprint module for increasing the capacity. External memory can be provided for storing the fingerprint image, which can be later accessed for comparison Unique Identification Numbers (Aadhar cards) have already been introduced in India that contains Security management of authentication system based on multimodal biometric features an individual's fingerprints and an iris scan.

REFERENCES

[1] Pooja J. Hajare, Mrs.S. S. Patil "Security Management of Authentication System based on multimodal Biometric Features", International Journal of Scientific & Engineering Research Volume 8, Issue 11, November-2017 ,ISSN 2229-5518.

- [2] Anandaraj S, Anish R, Devakumar P.V, “Secured Electronic Voting Machine using Biometric” IEEE Sponsored 2nd International Conference on Innovations in Information, Embedded and Communication systems (ICIIECS) 2015.
- [3] Shashikumar D. R1, K. B. Raja, R. K. Chhotaray, Sabyasachi Pattanaik, “Biometric Security System Based on Signature Verification Using Neural Networks” 978-1-4244-5967-4/10/\$26.00 ©2010 IEEE.
- [4] Yao-Hong Tsai, Hsiao-Ping Huang, HuiRong Wu “Security Management of Authentication System Based on Dynamic Biometric Features” 2014 International Conference on Trustworthy Systems and their Applications 978-1-4799-6566-3/14 \$31.00 © 2014 IEEE, DOI 10.1109/TSA.2014.19.
- [5] Alaguvel. R 1, Gnanavel. G 2, Jagadhambal. K 3 , “Biometrics using Electronic Voting System with Embedded Security” International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 2, Issue 3, March 2013.
- [6] George Chellin Chandran . J 1 Dr. Rajesh. R.S 2, “Performance Analysis of Multimodal Biometric System Authentication.” IJCSNS 290 International Journal of Computer Science and Network Security, VOL.9 No.3, March 2009.
- [7] M.Sudhakar, 2B.Divya Soundarya Sai, “Biometric System Based Electronic Voting Machine Using Arm9 Microcontroller” IOSR Journal of Electronics and Communication Engineering (IOSR-JECE) e-ISSN: 2278-2834,p- ISSN: 2278-8735.Volume 10, Issue 1, Ver. II (Jan - Feb. 2015).
- [8] Shankar Kartik1, K. Ram Kumar2 and V.S. Srimadhavan3, “Security system with face recognition, sms alert and embedded network video monitoring terminal” International Journal of Security, Privacy and Trust Management (IJSPTM) Vol 2, No 5, October 2013.