IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 6, June 2016

Hardware Integrated Trio Security System

Ria Mathews[1], Nisha Mariam Jacob[2],Sruthymol TA[3],Tobin PC[4],Varghese Chacko[5]

Assistant Professor, Computer Science, Saintgits, Kottayam, India [1]

Student, Computer Science, Saintgits, Kottayam, India [2,3,4,5]

Abstract: security assurance is an inevitable factor required for online voting system. The proposed system is an authenticated system that provides integration of trio security features such as QR code scanning, face recognition, cryptography. The existing voting system is based on ballot machine where when we press the button corresponding to the symbol, the voting is done. Here there is a security risk, the person who votes may be fake person voting. The people there might not know that a person is using fake voting card, this may cause problem. The proposed system is an integrated system that provides three layers of security. First level of security is that each individual voter is provided with a separate QR code and that code is scanned before entering the room. The second phase security is provided by face recognition. The voter's image is captured and compared with the image stored in the database, if it matches the automated smart room will be opened and can cast their vote and the door can be closed using a sensor and the bulb inside will be illuminated. The third level of security is provided for the voter's details by encryption method. The intended system will provide more security than the existing systems.

Keywords: Cryptography, Face Recognition, QR Code Scanning,

INTRODUCTION

Security is generally a state or feeling of being saved and protected, an assurance that something of value will not be taken. Security is very important feature in many system. Currently security is provided using a variety of logical and physical methods. But all these security methods adopted today are overcome by intruders and hackers in one way or other.

Face recognition is an important method for biometric verification .Face recognition is a type of biometric software application that can identify a specific individual in a digital image by analysing and comparing patterns .Face recognition system is a real time computer system that can locate and track a subject's head and then recognize the person by comparing characteristics of the face to those of known individuals. One of the ways to do this is by comparing selected facial features from the image and a facial database. Security systems have been developed over the years with different discrete access codes being employed, but also in the recent past, with the ability of face recognition principles or ideas being applied to a wide range of problems like criminal identification and crowd surveillance. Images/film processing can also be applied to the development of a security system.

This can be used in different environments where high degrees of security are required which include places like banks, military research areas, areas of national security, production areas of multinational companies, big private investment companies, etc. This prompted the pursuit of research into how this could be achieved and the implementation of how facial recognition can be used in developing a security system. QR code is the Quick Response code. Before the QR code there are some authentication methods are available that are-User name and password, Barcode, Finger prints, Face identity etc. QR code is the trademark for the type of matrixbarcode which was invented by the Japanese corporation Denso Wave. QR Code has a number of features such as large capacity data encoding, dirt and damage resistant, high speed reading, small printout size, 360 degree reading and structural flexibility of application. In cryptography, encryption is theprocess of obscuring information to make it unreadablewithout special knowledge. This is usually done for secrecy, andtypically for confidential communications. Encryption can also be used for authentication, digital signatures, digital cash etc... Voters details are encrypted using cryptography. We are using AES algorithm for data encryption.

Trio Security system is an efficient system which emphasis on different security features. In this system we provide layers of security such as QR code scanning, face recognition and cryptography etc...QR code scanning is considered as an authentication criteria to activate the system. Biometric authentication such as face recognition technique is used to control the door of the room. In this cryptography is used as an encryption technique to keep the data's more secure .

The main characteristics of the system is that here the comprehensive integration of different security features are amalgamated together .Since we are using the mechanism of QR code scanning ,face recognition and cryptography together the security become more substantial. The system mainly aims at avoiding the problem of security attacks in the existing system by the comprehensive integration of different security features. This system is fully automated and thereby reduce the manual labour required for the different processes.

DOI 10.17148/IJARCCE.2016.5621

RELATED WORKS

In the existing system there were chances of high security attacks and the manual labour required to control the system is very high. The different processes in the existing system is very time consuming. So we ensure a feasible system ensuring all sorts of security which is economical and reliable. Biometric features such as face recognition alone is not sufficient enough to provide security for the existing system. So that, we have implemented an assimilated system that provides more security than the existing one.

In the existing system we are providing the security features such as face recognition, QR code scanning separately, but the proposed system is an authenticated system that provides integration of Face recognition, QR code scanning etc. on an automated smart room. This system is fully automated and thereby reduce the manual labour required for the different processesIn addition to face-recognition algorithms, a ternary authorization such as eye lid recognition or finger print recognition can be implemented to make the areas even more secure .The consequences of web application vulnerabilities is overlooked and in most cases adequate importance is not given during product development phase. The advantages of the proposed system are scalability ,low power consumption ,highly secure ,reduce manual labour ,relatively fast approach ,simple to use ,highly reliable ,low maintenance cost .The existing system includes online banking using QR code[1],Online voting system using biometric measures such as finger printing[2].In our project we develop a security system which uses QR code for security.

Issues in the existing biometric authentication methods is that ,Certain physical characteristics such as voice, gait and fingerprints may vary with time. So, it is judicious to not have authentication merely based on biometrics. Besides, the physical and behavioral characteristics of an individual are non-revocable, non-secret and thus pose a physical threat to the user. Since biometrics is currently in its nascent stages, the technology is expensive and not mature yet.

If we consider the secure authentication of online banking system using QR Code[1], the security methods are like password ,username ,fingerprints , and face detection .It is a security system which use QR code for security and provide two way authentications such as online and offline authentication system .It consists offour modules ,which includes QR code generation ,online authentication system ,offline authentication system and QR code generation But in these security is not more, so we need to ensure high security using the proposed system .

The existing system for online voting system using fingerprint scanning is inefficient and vulnerable to outer threats .There will be a great chance of fraudulent attempts. Fingerprint recognition or fingerprint authentication refers to the automated method of verifying a match between two human fingerprints. Fingerprints are one of many forms of biometrics used to identify individuals and verify their identity. A fingerprint looks at the patterns found on a fingertip. There are a variety of approaches to fingerprint endorsement.

In the proposed system we are amalgamating three levels of security features .In the first level security is implemented by QR code scanning and in the second phase security is ensured by face recognition. The third level of security is provided by cryptographic method. Authorization using various security features enables the right person to vote and makes it a fully automated and secure system We can implement this trio security for various systems such as online voting system, online banking system etc.. .

In our project we are implementing the trio security for an online voting system ,so that voters can cast their votes at the right time for the intended person without any delay .So that the human effort is reduced to a great extent and can be performed faster than the existing systems.

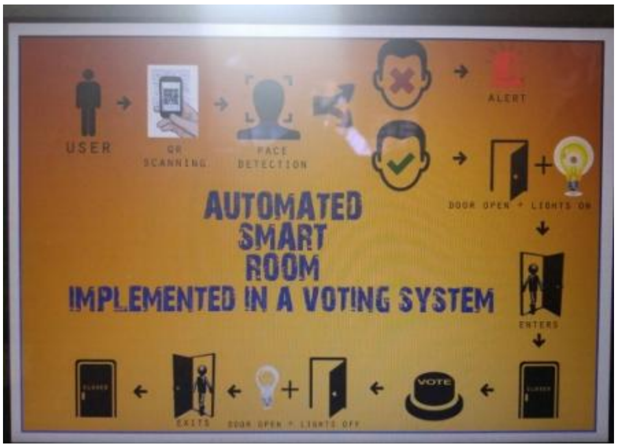
EXPERIMENTAL RESULTS

The input of the system is designed in such a way that they are satisfying two algorithms based on encryption standards .Eigen face detection algorithm uses voters faces as input and comparison of captured image and stored image are done in order to produce an output in the form of an electrical impulse that trigger open the door of the smart room with an accuracy rate of 70 %(approx. up to 92%) and a standard delay of 2e+9 nanoseconds.ccryptographic encryption using AES algorithm uses the details of the voters as input and produces a cipher text as output such that it provides maximum security to the voters We have implemented the trio security system in a voting system.

Voting is an universal right for all adults .To ensure fair and safe voting and to avoid discrepancies we need to recognize the identity of the voter completely,in every possible way.It is easy to fake identities and break through voting premises these days .Also,the mark made on the index finger can be removed by some special reagents. So here comes the need for security .Trio biometrics ie, face recognition and also a QR code is also provided to each voters in order to make the voting system active. This will allow only valid voters and therefore chances of false votes and violence are almost nil.

In the trio security system we are also using the encryption techniques like cryptography to keep the data more secure so nobody can know who voted for which party. Nobody can harm or pressurize the voter. Also it allows only one person in the voting room at a time. This avoids confusion at the booth.It is a blessing to both the voters as well as the authorities conducting election.Security system not only provides a safe environment but verifies the voter's identity with a high level of accuracy.

DOI 10.17148/IJARCCE.2016.5621



BIOMETRIC AUTHENTICATION

Biometric mechanism is considered as a method of verification.It includes face recognition,finger image, hand geometry,iris recognition,retinal scanning,signature verification and speaker verification.All biometric mechanisms share an underlying methodology involving enrolment and verification or identification.

When biometrics are used for verification the captured biometric record is matched against one biometric template in the data stored to determine a match.

When biometrics are used for identification,the biometric capture and conversion are the same, but no separate identifier is acquired,and therefore the verifier matches the biometric record against all biometric records in the datastored.

Face recognition is a type of biometric software application that can identify a specific individual in a digital image by analyzing and comparing patterns.Stages of Face Recognition includes face location detection, feature extraction and facial image classification.The approaches to feature extraction includes local features like eyes ,nose,mouth etc. sometimes we consider the global feature which extract feature from the whole image.

A.FACE RECOGNITION USING EIGENFACES

Face Images are projected into a feature space ("Face Space") that best encodes the variation among known face images. The face space is defined by the "Eigenfaces", which are the eigenvectors of the set of faces.

APPLICATIONS

There exist many application for our system, it can be implemented in an online banking system, where high rate of security is required and also can be implemented for a secure systems in shopping malls. In overall our project provides a system which is more user friendly, reliable and secure .Usefulness of this project are ,reasonable, accuracy,personalization,privacy preserving and platform independent.

FEATURES AND BENEFITS

- Comprehensive integration of security systems.
- It can be used to reduce fraudulent attempts.
- Energy saving.
- Improved face recognition algorithms can be used which will give better results even with varying environments making the system portable
- In addition to face-recognition algorithms, a ternary authorization such as eye lid recognition or finger print recognition can be implemented to make the areas even more secure.
- System is easily updateable since all the modules work individually.
- security is more powerful because of the QR code and encryption algorithm
- The QR codes are only readable by the machine so untrusted person cannot understand what is inside the QR code.
- QR code can readable when it is partially damage
- There is no way for any attack because the file is not easily accessible and it is encrypted

FUTURE SCOPE

In addition to face-recognition algorithms, a ternary authorization such as eye lid recognition or finger print recognition can be implemented to make the areas even more secure.Rather than just using simple IR sensors, other motion detection modules can be included to make the place more secure.

Utilizing a more sophisticated camera to enhance image quality and improve recognition capability.There can be a combination of biometric applications being used such as combining facial recognition withfinger print identification for each user.Providing a backup power source for the whole system when implemented in order to avoid system failure as a result of power failure.

CONCLUSION

Security is a salient feature required for many systems. Now we have different security systems with distinct security features .The trio security system is a well-organized system in which different security features are integrated together to make the system more powerful and secure.

REFERENCES

[1] S. M. Metev and V. P. Veiko, Laser Assisted Microtechnology, 2nd ed., R. M. Osgood, Jr., Ed. Berlin, Germany: Springer-Verlag, 1998. J. Breckling, Ed., The Analysis of Directional Time Series: Applications to Wind Speed and Direction, ser. Lecture Notes in Statistics. Berlin, Germany: Springer, 1989, vol. 61.M. Wegmuller, J. P. von der Weid, P. Oberson, and N. Gisin, "High resolution fiber distributed measurements with coherent OFDR," in Proc. ECOC'00, 2000, paper 11.3.4, p. 109.

[2] R. E. Sorace, V. S. Reinhardt, and S. A. Vaughn, "High-speed digital-to-RF converter," U.S. Patent 5 668 842, Sept. 16, 1997.

DOI 10.17148/IJARCCE.2016.5621

(2002) The IEEE website. [Online]

[3] M. Shell. (2002) IEEEtran homepage on CTAN. [Online]. Available: http://www.ctan.org/tex-archive/macros/latex/ contrib. /supported/IEEEtran/

[4] FLEXChip Signal Processor (MC68175/D), Motorola, 1996.
"PDCA12-70 data sheet," Opto Speed SA, Mezzovico, Switzerland.

[5] A. Karnik, "Performance of TCP congestion control with rate feedback: TCP/ABR and rate adaptive TCP/IP," M. Eng. thesis, Indian Institute of Science, Bangalore, India, Jan. 1999.

[6] J. Padhye, V. Firoiu, and D. Towsley, "A stochastic model of TCP Reno congestion avoidance and control," Univ. of Massachusetts, Amherst, MA, CMPSCI Tech. Rep. 99-02, 1999.

[7] Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specification, IEEE Std. 802.11, 1997.

[9] S. Zhang, C. Zhu, J. K. O. Sin, and P. K. T. Mok, "A novel ultrathinelevated channel low-temperature poly-Si TFT," IEEE Electron Device Lett., vol. 20, pp. 569–571, Nov. 1999.

DOI 10.17148/IJARCCE.2016.5621