

User Access Control Technique through Smart Device Authentication using Bluetooth Communication with the Aid of Face Recognition

Samir Uprety¹, Padmini M²

M.Tech Student, Dept. of Electronics, East Point College of Engineering & Technology, Bangalore, India¹

Associate Professor, Dept. of ECE, East Point College of Engineering & Technology, Bangalore, India²

Abstract: The new experience of this work is to provide a simple and low cost solution for users' access in a secured protected place. Large scale adoption of smart devices like smart mobile phones for personal usage has opened up an opportunity to identify people via their smart device identities. This paper aims to (accomplish or gain with effort) very simple way of doing things of users' access control through device (verifying someone's identity) using a microcontroller board such as nuvoTon W78E052D 8-Bit Microcontroller that interacts with the smart device using Bluetooth technology (HC-05 Bluetooth Module) which is almost available in every smart device. Further, the proposed (verifying someone's identity) and (machines/methods/ways) are (intelligent/obvious) and require minimum effort. As a way(s) of doing things of secured communication is used in the mobile apps. The putting into use procedure is discussed through the AdaBoost algorithm for face recognition system using mat lab and java. Some possible application areas are discussed in which the proposed way(s) of doing things may be applied to enable appropriate services.

Keywords: Bluetooth Technology, Face Recognition System, Client-Socket Communication, Android Mobile Device.

I. INTRODUCTION

According to the work presented by Limi Kalita., shows that elements of network programming and concepts involved in creating network applications using sockets. And they spread like wildfire with the Internet. The client and server can communicate with each other by writing to or reading from these sockets. Sockets play a vital role in client server applications. The aim of the paper is to introduce sockets, its deployment pertaining to network programming. One of the most basic network programming tasks likely to be faced as a java programmer is performing the socket functions/methods because java has been preferred mostly for establishing client server communications using sockets. They were invented in Berkeley as part of the BSD flavor of UNIX operating systems [01].

The work carried out by Savithri G and K.L.Sudha., shows that a Chaotic systems are known for its randomness, it can be made utilized in achieving the encryption. In this paper chaos-based encryption algorithm for images is used. This algorithm is based on pixel scrambling where in the randomness of the chaos is made utilized to scramble the position of the pixels. This Application is developed using the Java programming language in Android Software Development Kit. This application created for the Android operating system can be used in smart mobile phones for sending any image in a secrete manner by hiding it in another larger image. Random pixel insertion method is used for hiding the secrete image in cover image. Information hiding is an art which has been used since long back for covert

communication. Steganography is the art of hiding secret message within a larger image or a secret image in another cover image, such that the hidden message or an image is undetectable [02].

The author Archana Jadhav and Vipul Oswal., explained that a conditions that must be followed are that a VNC server must be installed on the person's computer which will be monitored and it must be connected to a Wi-Fi network. Current key assignments can be viewed using guidance function. This process will be carried out using Virtual Network Computing based architecture. In this paper, we will enlist the process to access the desktops of remote computer systems with the use of a android based cellular phone. There is shortcut function that can be used to quickly access the frequently used area. The user can access and manipulate the desktop within the Wi-Fi range irrespective of various platforms like windows, mac or linux. The image of the desktop is compressed before it is transmitted to the cellular phone. A user will be able to access and manipulate the desktops of remote computers through a VNC viewer that will be provided on the user's cell-phone. A user can view two areas simultaneously using a twin view function. The prototype is already implemented using java and tested on a java based cellular phone. There are several functions provided so as to ease the viewing on cell-phones [03].

The author Nateq Be-Nazir Ibn Minar and Mohammed Tarique., conclude that it also presents some tips that end-users can implement immediately to become more cautious about their private information. Finally, the paper

concludes with some recommendations for future security enhancements that can be implemented in the Bluetooth standard. The availability of mobile phones, game controllers, Personal Digital Assistant (PDA) and personal computers has made Bluetooth a popular technology for short range wireless communication. However, as the Bluetooth technology becomes widespread, vulnerabilities in its security protocols are increasing which can be potentially dangerous to the privacy of a user's personal information. This paper presents the vulnerabilities in the security protocols of this technology along with some past security threats and possible countermeasures as reported in the literatures which have been surveyed and summarized in this paper. Bluetooth technology has become an integral part of this modern society. The security issues of Bluetooth have been an active area of research for the last few years [04].

According to the work proposed by Jaya Bharathi chintalapati and Srinivasa Rao et.al., explained that to work on this, we must install VNC server on our computer connected with Wi-Fi network. There is shortcut function that can be used to quickly access the frequently used area. The user can access & perform operation through the range of Wi-Fi platforms like Linux, Mac, windows etc. The image of the desktop is compressed before it is transmitted to the cellular phone. There are several functions provided so as to ease the viewing on cell-phones. This process is based on VNC (virtual network computing) technique. In this paper, we will present the process to access the computers with the help of android mobile phones. Current key assignments can be viewed using guidance function. A user can view two areas simultaneously using a twin view function. The prototype is already implemented using java and tested on a java based cellular phone [05].

According to the work presented by M.Gopi Krishna and A. Srinivasulu., shows that the proposed architecture for face detection has been designed using Verilog HDL and implemented in Modelsim. We describe here design techniques including image scaling, integral image generation, pipelined processing as well as classifier, and parallel processing multiple classifiers to accelerate the processing speed of the face detection system. Also we discuss the optimization of the proposed architecture which can be scalable for configurable devices with variable resources. We show about 35 time's increase of system performance over the equivalent hardware implementation. This work presents architecture for face detection based system on AdaBoost algorithm using Haar features. Its performance has been measured and compared with an equivalent hardware implementation [06].

The author Sharon Panth and Mahesh Jivani., explained that a HAS system for Android users is a step towards the ease of the tasks by controlling one to twenty four different appliances in any home environment. This paper presents the automated approach of controlling the devices in a household that could ease the tasks of using the traditional method of the switch. Hence with the help of his companion – a mobile phone, some daily household tasks can be accomplished by personifying the use of the mobile phone. Analyzing the current smart phone market, novice

mobile users are opting for Android based phones. Home Automation System (HAS) has been designed for mobile phones having Android platform to automate an 8 bit Bluetooth interfaced microcontroller which controls a number of home appliances like lights, fans, bulbs and many more using on/off relay. In the present times, we can find most of the people clinging to their mobile phones and smart devices throughout the day. Automation of the surrounding environment of a modern human being allows increasing his work efficiency and comfort. The most famous and efficient technology for short range wireless communication- Bluetooth is used here to automate the system. It has become a second name for a mobile phone in layman terms. There has been a significant development in the area of an individual's routine tasks and those can be automated [07].

According to the work proposed by Yasaman Heydarzadeh and bolfazl Toroghi Haghghat et.al., explained that one of the fastest and most successful approaches in this field was presented by Viola. In this work, Viola approach is used as the basis algorithm in order to propose a new efficient face detection system. Moreover, some preprocessing techniques are also used to limit the candidate places which make final algorithm runs faster. Using Haar-like features for facial parts and learning these features by AdaBoost algorithm make proposed approach possible to detect occluded faces and increase the detection rate. In order to build a fully automated system that analyzes the information in face image, there is a need for robust and efficient face detection algorithms. The experimental results represent that, the proposed approach has the capability of achieving a detection rate of 94.7% while false positive rate is just 2% .Furthermore, this system can detect faces in image, averagely four times faster than Viola approach [08].

The work carried out by Erina Ferro and Francesco Potort., shows that Bluetooth and IEEE 802.11 (Wi-Fi) are two correspondence convention norms that characterize a physical layer and a MAC layer for remote interchanges inside of a short range (from a few meters up to 100 m) with low power utilization (from under 1 mW up to 100 mW). Bluetooth is situated to joining close gadgets, serving as a substitute for links, while Wi-Fi is situated toward PC to-PC associations, as an augmentation of or substitution for cabled LANs. In this article we offer a diagram of these prevalent remote correspondence benchmarks, contrasting their primary components and practices regarding different measurements, including limit, system topology, security, nature of administration bolster, and force utilization [09].

II. PROPOSED SYSTEM

The current system is designed to provide better authentication for institutions, companies, schools, industries, etc. The proposed system is a two-fold solution for existing authentication problem.

Examples for existing systems include:

1. Consider an institution, where the attendance of the students has to be taken manually, and the count of students present in the class may not be correct due to proxy attendance. And

also few times, the chances of someone from other section/class being present in class may also happen.

So to avoid these kinds of problems, the existing system was designed using RFID (Radio Frequency Identification), where each individual is provided with RFID card with unique ID to take the count as well attendance of the person.

But the disadvantage here is nobody knows whether the person using RFID is the valid owner of the card or not.

2. Consider the case in companies, where every employee has to swipe/tap their ID card, basically designed on RF technology.

The disadvantage is that if the employee forgets his/her ID card, then the security personnel don't allow the person inside the premises until and unless he/she provides a valid proof of authentication.

Considering the disadvantages in the existing system, we have proposed a two-fold security system, where the person entering into institution/company must be recognized as Authenticated user by utilization of Face Recognition system and after face recognition, the person has to enter a valid unique ID which is assigned to every authenticated individual. So thus an efficient and reliable authentication system is designed in this current work.

The architecture design of the proposed system is shown in Figure 1. This system includes the implementation in MATLAB® 7.10.0 (R2010a) for Face Recognition, Java® Eclipse Galileo for establishing communication between an Android mobile device and Java system, finally Bluetooth authentication is done using nuvoTon W78E052D 8-bit Microcontroller which is programmed in Keil µVision IDE using Embedded C programming. The block diagram of proposed system is shown in Figure 1.

The software system included is shown on top of the Figure 1, which consists of Training and Testing Phase. Main components of software module are composed of methods required to detect and recognize face region using Image Processing concepts. The steps involved in detecting and recognizing (training and testing) faces are acquiring face image, pre-processing the acquired image, extracting the facial features using AdaBoost (Adaptive Boosting) algorithm with the aid of Haar cascade classifiers, storing these features in Knowledge Base and later comparing the test facial image features with features stored in Knowledge Base. Efficiency and accuracy of the system proves to be promising.

A. Software Module

Java eclipse GALILEO software (Integrated Development Environment) is used as tool for establishing communication medium between Android mobile device and Java module. The connection will be established on validating IP (Internet Protocol) Address, and Port number entered in Android mobile device as shown in Figure 3.1. Android mobile device and PC (Personal Computer) in which Java module is running must be connected to the

same network. IP address numerical label assigned to every device connected to a network with the aid of IP for communication. Main purposes of IP address include host or network interface identification and location addressing. IPv4 addressing includes 32 bits of data separated by dot, which is called as dotted-decimal notation. For example: IPv4 dotted-decimal notation address looks like 173.16.244.1. In Windows® platform - to find the IP address, user has to type the command "ipconfig" in Command Prompt.

A computer port is a type of software-, electronic- or programming-related docking point through which information will be transmitted from a program on one computer to another computer from the Internet in a network. Usually port numbers are used to establish a communication within a network. The range of port numbers can be classified as 0-1023, 1024-49151 and 49152-65536. In our proposed system the port number used is 8080. Port number 8080 is commonly used for caching port and as well for proxy.

The proposed system validates the IP address and Port number entered from user Android mobile. The first field shown is to enter IP address and the second field is to enter Port number. After providing these details, the user has to press "Register" button to establish a connection. If the person is identified as unauthenticated, that person's face is displayed on the mobile screen.

B. Hardware Module

1. Microcontroller board

nuvoTon W78E052D 8-bit microcontroller is used with RS232 89V51RD2 flasher project board. This development board has 40 general purpose input output (GPIO) pins with on board power supply circuit, RS232 port for serial interface with computer and other serial devices, reset switch, power status LED and a general purpose switch and LED. This board is compatible with P89V51RD2 microcontroller, which allows serial programming and can be programmed directly with this board through a serial communication (COM) port to a PC without the need for an external programmer. Developing the code for microcontroller is done in Keil µVision IDE Version 4.0. This board has MAX232 interface circuit for easy communication with computer and other serial devices. The schematic connections to development board with Magnetic door lock, LCD display, and relay board is shown in Fig. 2.

2. LCD Display

16×2 Liquid Crystal Display (LCD) can display 16 characters per line and there are 2 lines. Each character is displayed in 5×7 pixel matrix. There are two kinds of registers namely Command and Data. The data register stores the data which is to be displayed on the LCD. The data will be ASCII value of the character. The command register stores command instructions such as initializing LCD, setting the cursor position, clearing the LCD display, etc. In our project LCD display has been used to view the current status of the system, for e.g. whether person is authenticated or unauthenticated.

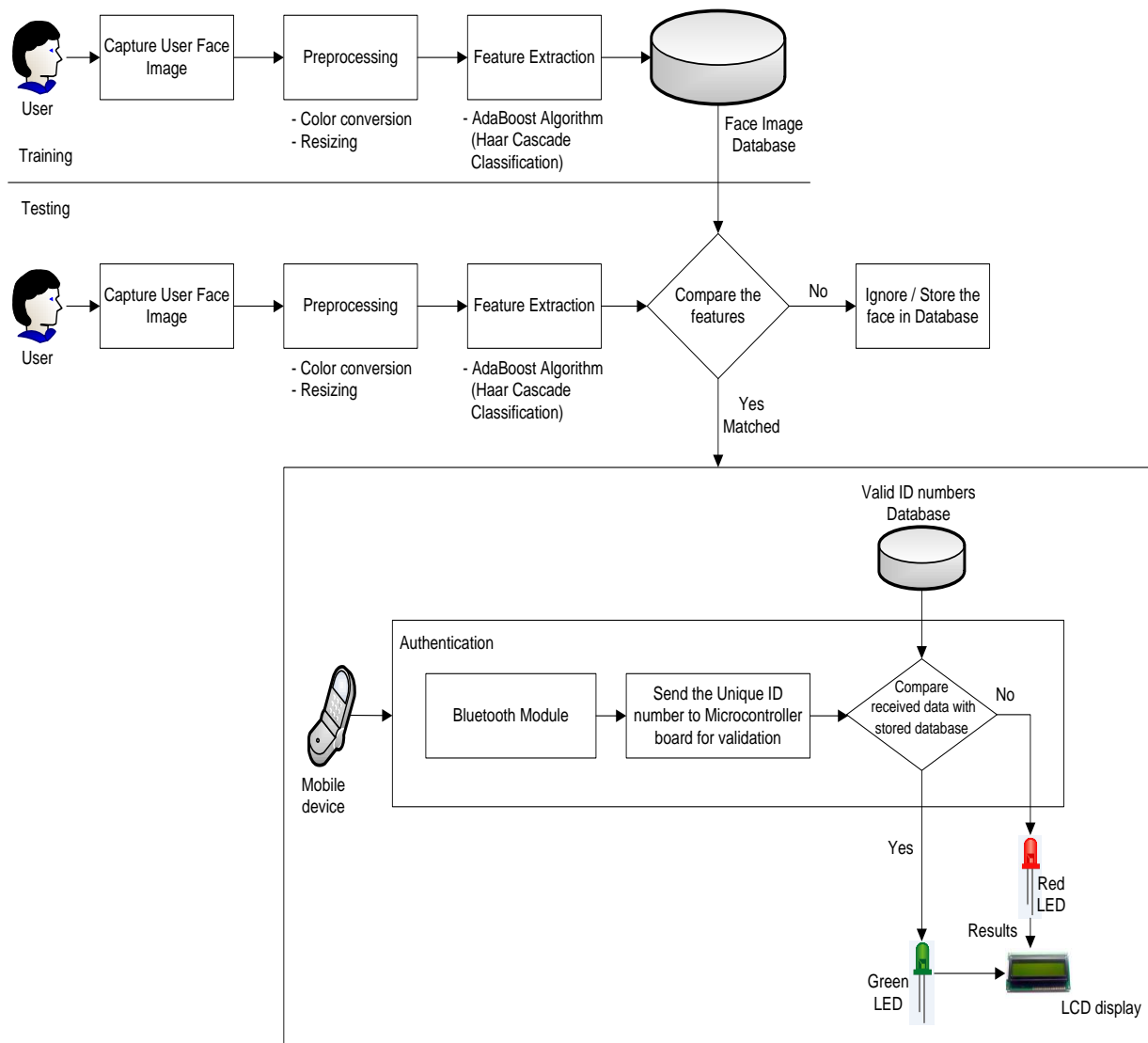


Figure 1: Architecture Design of the proposed system.

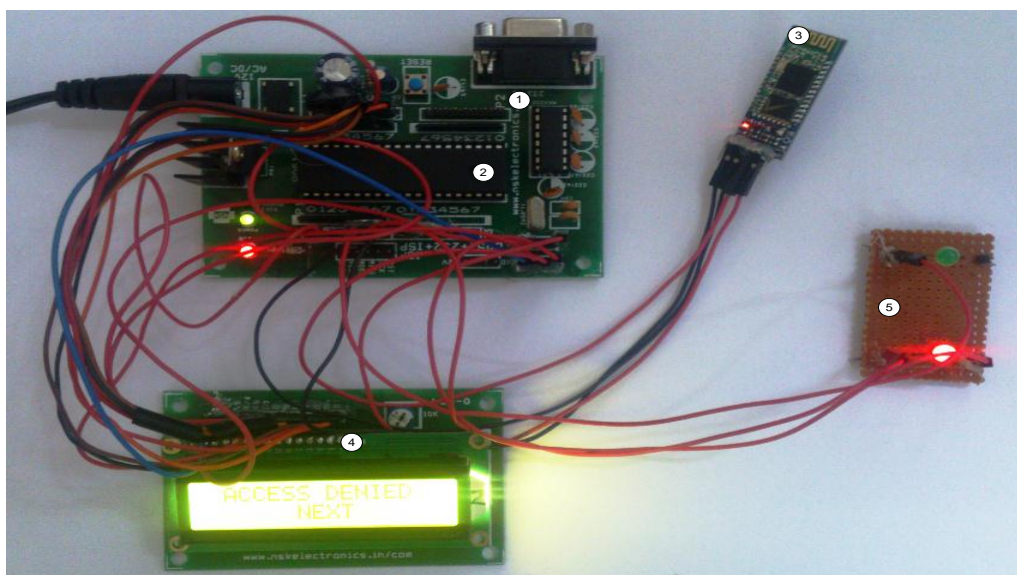


Figure 2 : Hardware connections, 1. Project Board, 2. nuvoTon W78E052D 8-Bit Microcontroller, 3. HC-05 Bluetooth Module, 4. 16x2 LCD Display, and 5. Green and Red LED connected to 5V and Ground

III. RESULTS

The hardware implementation is shown in Fig. 2. The hardware system consists of a Project Board, nuvoTon W78E052D 8-Bit Microcontroller and 16×2 LCD Display, Green and Red LED connected to 5V and Ground.

LCD displaying “ACCESS GRANTED” after the unique ID number entered by user is confirmed as valid number, and “NEXT” is being displayed for allowing next person to enter his/her unique ID number, as shown in Fig. 4.

If not, LCD displaying “ACCESS DENIED” after the unique ID number entered by user is confirmed as not a valid number, and “NEXT” is being displayed for allowing next person to enter his/her unique ID number” will be displayed on LCD as shown in Fig. 3.

RTFR abbreviates for Real Time Face Recognition. After pressing Start Video button, the camera continues to capture video and if any face is detected in that window, the detected with bounding box is displayed in side window.

Then the image processing will be done in MATLAB software.



Figure 3: LCD displaying “ACCESS GRANTED” after the unique ID number entered by user is confirmed as valid number, and “NEXT” is being displayed for allowing next person to enter his/her unique ID number.



Figure 4: LCD displaying “ACCESS DENIED” after the unique ID number entered by user is confirmed as not a valid number, and “NEXT” is being displayed for allowing next person to enter his/her unique ID number.

Figure 5: (a) RTFR_Toolbox GUI (Graphical User Interface), RTFR abbreviates for Real Time Face Recognition. After pressing Start Video button, the camera continues to capture video and if any face is detected in that window, the detected with bounding box is displayed in side window.

Figure 5: (b) Since the face shown in Figure 5(a) is trained, hence the message box showing “Authenticated Person”.

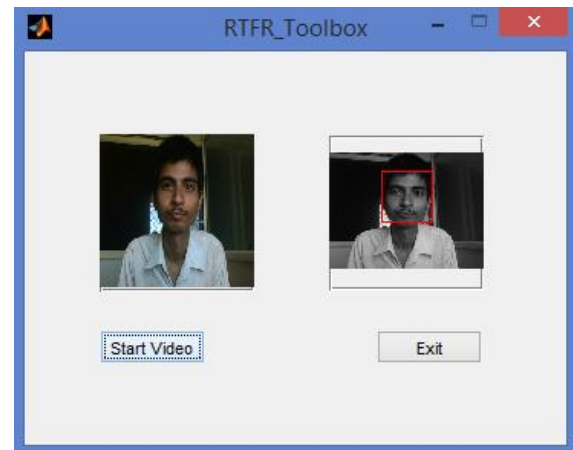


Figure 5:(a) RTFR_Toolbox GUI (Graphical User Interface)

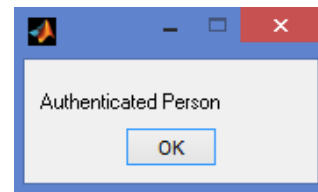


Figure 5: (b) Authenticated Person Alert Box

Figure 6: (a) RTFR_Toolbox GUI (Graphical User Interface), RTFR abbreviates for Real Time Face Recognition. After pressing Start Video button, the camera continues to capture video and if any face is detected in that window, the detected with bounding box is displayed in side window.

Figure 6: (b) Since the face shown in Figure 6(a) is not trained, hence the message box showing “Unauthenticated Person”.

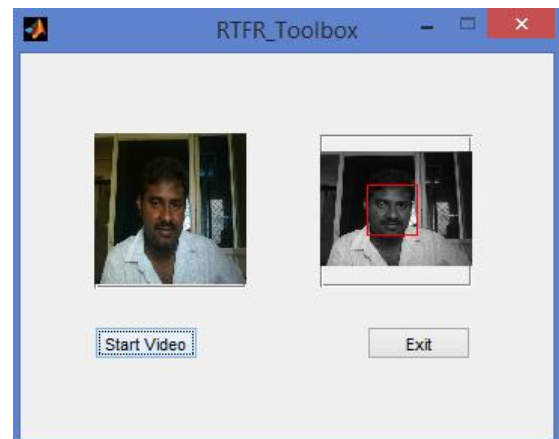


Figure 6: (a) RTFR_Toolbox GUI (Graphical User Interface)

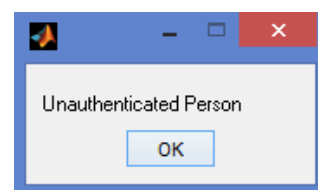


Figure 6: (b) Unauthenticated Person Alert Box

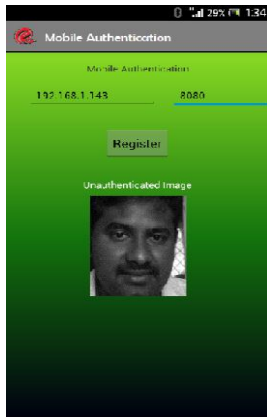


Figure 7: Image of unauthenticated Person on Android Mobile & Shows that the unauthenticated person image after recognition stage from matlab process.

- [9] Erina Ferro and Francesco Potort," Bluetooth and Wi-Fi Wireless Protocols:A Survey and a Comparison," IEEE Wireless Communications, 2001.

IV. CONCLUSION

In this project, a very simple mechanism of users' access control via smart mobile device authentication is discussed. A model has been implemented using Bluetooth communication and microcontroller board. The important aspect of this work is the concept of using smart phone instead of electronic identity cards or other instruments as access control device, and smart phones are carried by every person nowadays. This is a low cost yet effective solution for access control. We proposed a user access control technique through smart device authentication using Bluetooth communication with the aid of human face recognition system. The embedded actions based on the posture of human face in the captured image by using Adaboost algorithm. For further investigating the face recognition and authenticated via android mobile and socket programming is implemented for client-server communication.

REFERENCES

- [1] Limi Kalita, "Socket Programming," International Journal of Computer Science and Information Technologies, Volume 5, Issue 3, 2014.
- [2] Savithri G and K.L.Sudha, "Android Application for Secret Image Transmission and Reception Using Chaotic Steganography," International Journal of Innovative Research in Computer and Communication Engineering, Volume 2, Issue 7, 2014.
- [3] Archana Jadhav and Vipul Oswal, "VNC Architecture Based Remote Desktop Access Through Android Mobile Phones," International Journal of Advanced Research in Computer and Communication Engineering, Volume 1, Issue 2, 2012.
- [4] Nateq Be-Nazir Ibn Minar and Mohammed Tarique, "Bluetooth Security Threats and Solutions: A Survey," International Journal of Distributed and Parallel Systems (IJDPS), Volume 3, Issue 1, 2012.
- [5] Jaya Bharathi chintalapati and Srinivasa Rao, "Remote computer access through Android mobiles," IJCSI International Journal of Computer Science Issues, Volume 9, Issue 5, 2012.
- [6] M.Gopi Krishna and A. Srinivasulu, "Face Detection System On AdaBoost Algorithm Using Haar Classifiers," International Journal of Modern Engineering Research (IJMER), Volume 2, Issue 5, 2012.
- [7] Sharon Panth and Mahesh Jivani,"Home Automation System (HAS) using Android for Mobile Phone International Journal of Electronics and Computer Science Engineering, India, 2011.
- [8] Yasaman Heydarzadeh and bolfazl Toroghi Haghight,"An Efficient Face Detection Method Using Adaboost and Facial Parts," Electronic department Azad University of Qazvin Tehran, Iran, 2011.