ResearchGate

See discussions, stats, and author profiles for this publication at: https://www.researchgate.net/publication/299391019

Intelligent Intrusion Prevention System For Households Based on System-On-Chip Computer

CONFERENCE PAPER · MAY 2016

READS
5

5 AUTHORS, INCLUDING:

Md. Tahmid Rashid
BRAC University
8 PUBLICATIONS **0** CITATIONS
SEE PROFILE

Imtiaz Abir
BRAC University
2 PUBLICATIONS **0** CITATIONS
SEE PROFILE

Rakibun Muntaha
BRAC University
1 PUBLICATION **0** CITATIONS
SEE PROFILE

Available from: Md. Tahmid Rashid
Retrieved on: 25 March 2016

Intelligent Intrusion Prevention System For Households Based on System-On-Chip Computer

Md. Tahmid Rashid, Imtiaz Kalam Abir, Niaz Sharif Shourove, Rakibun Muntaha and Dr. Md. Khalilur Rhaman
School of Engineering and Computer Science
BRAC University
Dhaka, Bangladesh
{tahmidrashid, imtiazkalamabir, niazsharifbu} @gmail.com, rakibunmuntaha@yahoo.com and khalilur@bracu.ac.bd

***Abstract*—Over the course of the last few decades, security systems have undergone radical overhauls and have transitioned into such sophisticated devices that some even completely shun any form of human interventions. In spite of its tremendous innovations, however, such setups have not yet made their way into homes and residences, partly owing to the fact that the equipment bear high price tags and lack user friendliness. This paper propositions a unique security system for residences that aims to solve the shortcomings of commercial alternatives. Basically, a Raspberry Pi 2 System-on-Chip (SoC) computer equipped with a camera module and placed outside the entrance of a house would attempt to identify would-be visitors by the means of image processing and voice identification. The system would spontaneously greet known faces with a friendly voice greeting and unlock the main door to allow them to enter the home. In case of unknown faces, the system would initiate a video call to the home's owner through a smartphone application and allow the owner to communicate with the unknown visitor. Upon receiving approval from the owner, the visitor's details would be entered into the system and the main door would be unlocked. If the owner denies access, he or she has the option to verbally ask the unknown visitor to leave or in extreme cases, press a button to call the police.**

Keywords—security systems; Raspberry Pi; System-On-Chip (SoC); image processing; voice identification; smartphone application

I. INTRODUCTION

Up lately, the need for household security has spiraled up significantly. Combined with the fact that home owners of today lead inherently busy lives, the upsurge of premise burglary over the past years has called for a more up-to-date method of dealing with intruders across homes. Many a times, it happens that the residents of a home leave the main door unlocked while going out, which calls for nothing but trouble.

One method to restrict entry to homes that has been widely adopted over the last few years is access control system. Access control system is the selective restriction of access to a place or other resource by the means of passwords, keycards or biometric verifications [1]. When a credential is presented to a secure reader, the reader attempts to verify the authenticity of the credential information, and passes it to a microcomputer [2-3]. The control panel relates the credentials to an access control list, allows or denies the presented request, and sends a transaction log to a database. For cases where access is denied in accordance to the access control list, the door remains locked. If there is a match between the credential and the access control list, the control panel drives a relay that releases a magnetic lock, which in turn unlocks the door [4].

Compared to traditional locking mechanisms, today's access control systems are fairly reliable and have garnered quite a reputation in the security sector. Despite the availability of such sophisticated home entry mechanisms, foolproof residence security is still an unaccomplished chapter today. As mentioned earlier, the occupants of homes tend to leave the entrances open, welcoming intruders or would-be criminals.

It is needless to mention that credentials can be passed around, thus sabotaging the access control system [5]. If someone knows someone else's password or steals his or her keycard, that person can gain access without the latter's consent. To combat this, biometric systems and two-stage verification processes have been introduced. Nevertheless, modern day identity thieves have worked their way around nearly all sorts of biometric fences [5-6]. Fingerprint readers have been tricked with falsely generated finger traces. Retinal scanners have been made to provide access by showing cleverly recreated artificial eyes [7]. One other problem hindering the success rate of these systems is that these come at very high price tags. Commercially available biometric security systems have been designed keeping industry applications in mind and they do not go gentle on consumers' pockets.

Our solution approach aims to develop a complete security solution for homes that would use image processing and voice recognition technology to differentiate between genuine guests and intruders. By discreetly identifying bona fide visitors, only authorized people would be granted access. Upon confirming any unauthorized visitor, the owner of the residence would be notified through a smartphone application and a live camera feed of the visitor would be displayed on the screen. Additionally, a 7" wall mount touchscreen placed on the interior of the home would also provide a similar functionality. By pressing a button, the owner can allow access to the new guest and the application would prompt for a new entry to the database. It would then take a series of photographs and capture the voice of the person for training. In the case when the residence's owner can't identify the visitor, he or she can conduct a video chat with the person and get to know him or her. If the owner is satisfied, he or she can give access to that

person. Alternately, if the owner feels threatened, pressing a button in the application would initiate a call to the police.

II. Background Study

Research in the field of household security is not a novel concept. In fact, over the years that have followed up, there has been a growing trend in the exploration of smart systems that attempts to spontaneously recognize people and allow access. Nguyen et al. came up with a real-time monitoring system that attempts to detect motion and whenever some movement is sensed, it starts to record the video feed for viewing offline later [8]. The real-time video feed can be accessed from smart phones or computers through web browsers. The system does not provide any automatic access control to open or close the main door. The biggest drawback of the system, however, is that it cannot intelligently detect intruders and just rely on the owner's discretion to decide on that. Kumar et.al. proposed a surveillance system which records video upon detecting motion, uploads it to the cloud and sends notifications to the household's owners through text messages [9]. This system also cannot spontaneously identify visitors. Shrikrishna and Mahesh devised a system that would open the door upon recognizing a known face and raise an alarm for unknown faces [10]. The system is very innovative but it skips a pretty big question. What if the unknown person was some genuine guest or a delivery man? It is just not feasible to ring an alarm every time an unknown person comes about. Doi, Sato and Chihara designed a lock control based on face recognition that compensates for fluctuations in size and inclination of face and lighting conditions and allow or deny access based on the preset user database [11]. Again this system does not take into account the scenario when a new visitor arrives.

Our face recognition and voice authentication based security system improves on the solutions already available and aims to curtail all these drawbacks by allowing any allowable newcomer to be enumerated into the system. This way, the system 'learns' about new visitors and prevents false alarms. In addition, the smartphone application we designed would help to remotely inform a landlord or resident about a new visitor, thus eliminating the need to be physically present. The two stage verification procedure of image processing and voice processing would further bolster the security, thus ensuring the system's fault tolerance.

III. System Design and Implementation

Our system is comprised of six key elements:

i) A Raspberry Pi 2 SoC,
ii) A camera module,
iii) An USB microphone,
iv) A switching circuit with a relay operating a magnetic lock on the door,
v) A smartphone application and
vi) A 7" touchscreen LCD display connected to the display connector of the Raspberry Pi.

The diagram in Fig. 1 describes the physical data flow of the components and Fig. 2 illustrates the core functionality of our system.

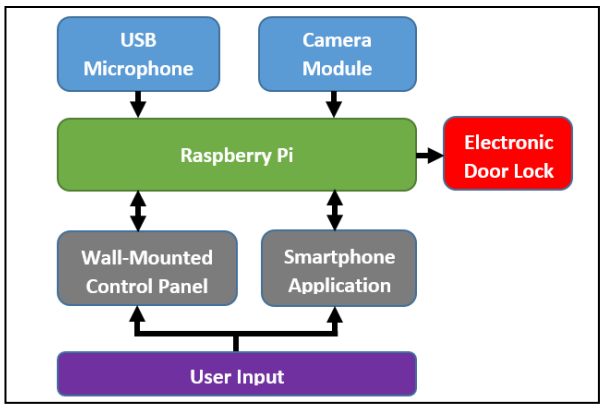

Fig. 1. Physical data flow of the system

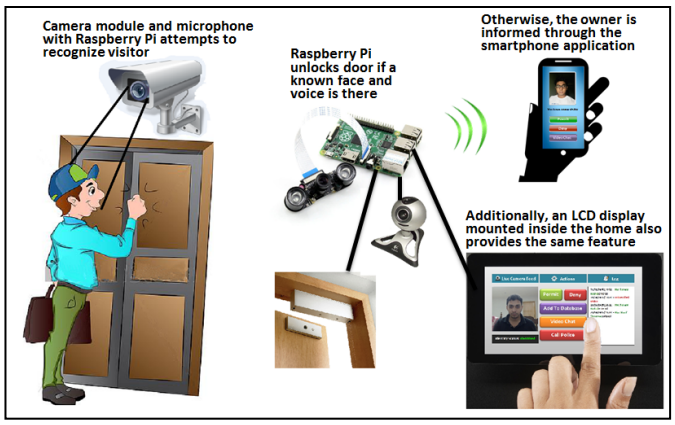

Fig. 2. Core functionality representation of the system

The camera module attached to the Raspberry Pi placed outside the main entrance of the home would look out for any motion. Once the presence of any person is confirmed by motion detection, the Raspberry Pi would capture an image and initialize its face detection process. Upon asserting the person is enlisted in the database, the system would attempt to further verify the person's identity audibly using the USB microphone, by asking him or her to read aloud his or her name. If the verification succeeds, the person would be greeted with a friendly voice greeting. If the visitor's identity cannot be determined at any of the two stages, the visitor would be asked to wait and simultaneously the person associated with the home, typically the home's owner would be notified through the smartphone app. The app would inform the owner that there is a new visitor and present three buttons- "Permit", "Deny" and "Video Chat". If "Permit" is pressed, the visitor waiting outside the door would be asked to speak out his name for voice training and a series of photographs would be taken for face recognition. The owner would be prompted to enter the name of the new entry and this would be recorded into the database along with the voice and photographs obtained earlier. If "Deny" is pressed, the owner would be taken to another screen with two more options- "Ask to Leave" and "Call Police". As their names suggests, these two buttons would offer a mean to deal with the stranger. The third button from the first screen, "Video Chat" would allow the owner to verbally chat with the person and determine his or her identity. Pressing "End Call" on this screen would take the user to the first screen. Screenshots from the app is visualized in Fig. 3.

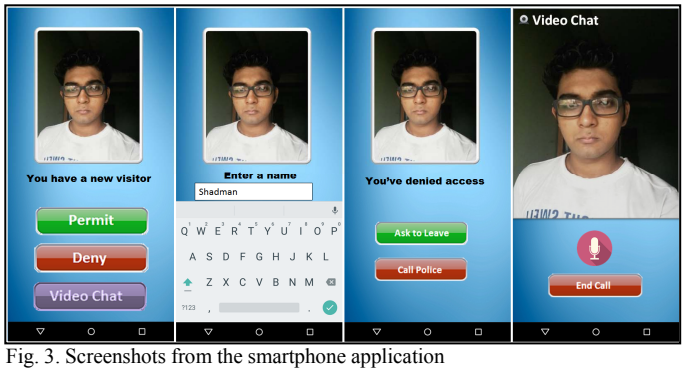

Fig. 3. Screenshots from the smartphone application

A 7" touchscreen panel placed on a wall inside of the home, connected to the Raspberry Pi's Display Serial Interface (DSI) port would display a detailed version of the smartphone application's interface, providing the live video feed from the camera on the left. On the center, the buttons reside which allow the user to permit or deny access to a visitor, add a new person to the database, initiate a video chat or take assistance from the police. In addition to these, there will be history log displayed on the right that would show the record of people processed through the system, regardless of authorized or unauthorized as can be seen from the screenshot in Fig. 4. The logical control flow process of the entire system is illustrated in the flowchart in Fig. 5.

IV. Facial Recognition and Voice Detection

The Raspberry Pi 2 runs on Raspbian OS, a variant of Debian operating system and uses the OpenCV library to detect and recognize faces. The underlying algorithm responsible for identifying faces is known as Eigenfaces. The face is detected by using the Viola-Jones method and the subsequent face recognition is implemented by using the Principal Component Analysis (PCA) [12-13]. Facial recognition conducted by PCA is generally referred to as the use of Eigenfaces and that is where the algorithm inherits its name from. For reaching a certain threshold of confidence level, a match is marked as positive, else it is marked negative. Since PCA decreases the dimensions of face images without losing important features, facial images of a lot of people can be stored in the database residing in the Raspberry Pi's limited mass storage. Although many training images are used, computational efficiency does not diminish by measurable levels. Consequently, face recognition using PCA proves to be more useful for door security system as compared to other available face recognition methods [12-15].

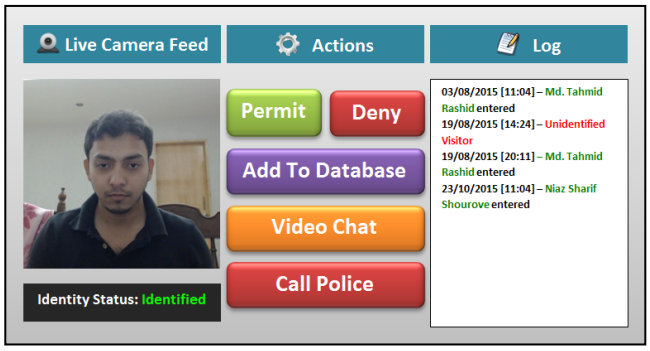

Fig. 4. Screenshot from the wall mounted 7" touchscreen panel

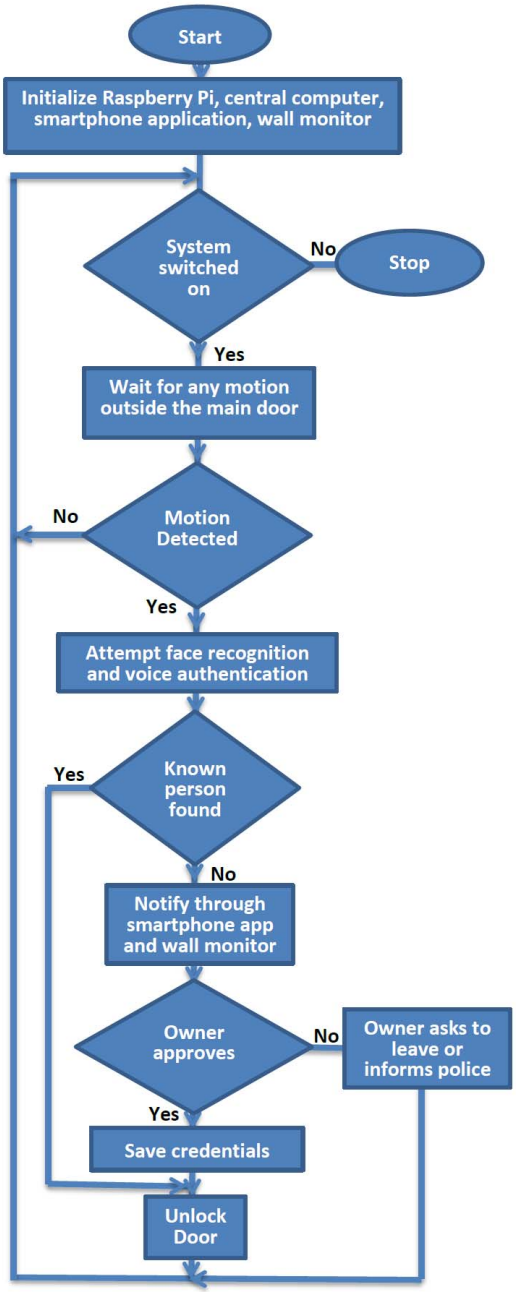

Fig. 5. Logical control flow process of the entire system

The matching database used in our system is nothing but a collection of positive and negative images linked to an xml file going by the name "Haar-Cascade". Face Recognition making use of Haar feature-based cascade classifiers is an effective object detection method proposed by Viola and Jones [13]. Basically, it is a machine learning based approach where a cascade function is trained from a lot of positive and negative images. Afterwards, the feature is used to detect specific objects in other images. Primarily, the algorithm requires quite a good number of positive images i.e. images of acceptable faces and negative images, which are unacceptable faces to train the classifier. Subsequently, the features need to be extracted from it bearing a close resemblance to convolutional kernel [13-14]. It is needless to mention that the Viola-Jones

method spontaneously adapts to incremental updates to the database and has a negligible tendency to render false positives or negatives [16-17]. To add confidence to our choice of detection method, we consulted a recent research that provided a detailed scrutiny of Haar-Cascade classifiers using two different face databases- the Yale face database and the FEI face database [18]. The results indicate that a person's face is best detected and recognized from the fontal position rather than faces turned sideways. Consequently, we made modifications to our system and placed the camera module on the front surface of the door facing towards the visitor. In the audible greeting, the visitor is asked to look towards the camera if a match is not found immediately.

From similar implementation of other security systems, we learned about a key technique behind successful facial recognition and that is background subtraction or isolation [19-20]. For our application, background subtraction was an easy task as the camera always pointed at the background. Any change in the background would be readily secluded as a foreground mask over which the image processing would be carried out. Thus, the time to process an image and recognize a face from it was relatively fast.

Upon verifying the face of the visitor, the next step is recognizing the voice. The person is asked by the system to read aloud his or her name. This process is carried out using a USB webcam's built-in microphone connected to the Raspberry Pi and Pocketsphinx, a speech recognition software running on the Raspbian operating system of the Raspberry Pi. Until now, there is no proper method for voice identification on the Raspberry Pi platform, although there are quite a handful of programs that can identify voice commands from any voice. Though Pocketsphinx is not well known for working with voice commands, it has an excellent feature that gives it near enough capability to differentiate between two persons' voices. The audio processing conducted by Pocketsphinx involves bit by bit comparison of sampled audio clippings [21]. Every person's voice signature differs in tone, pitch, intonations and delivery, giving rise to very noticeable variations in their captured audio samples. We have put this theory to test and have found that Pocketsphinx could differentiate between multiple people's voices with acceptable level of success.

Both the face recognition and voice identification applications are configured to run simultaneously on the Raspbian OS. A frontend graphical user interface (GUI) has been designed using C++ programming language under Qt Creator IDE. The GUI is displayed on the 7" LCD touchscreen panel connected to the HDMI output of the Raspberry Pi. A python script running on the background serves as an intermediate layer between the frontend and the core hardware.

The smartphone application has been developed using Android Studio for Android platform that utilizes Java Programming Language. The communication between the app and the Raspberry Pi SoC is established by the means of Transmission Control Protocol (TCP) and Real-time Transport Protocol (RTP), both of which have been modified to meet a peer-to-peer (P2P) architecture for our case. The live video feed is transferred through RTP while the audio and commands is relayed with TCP. On the Raspberry Pi side, the Python script mentioned earlier also performs a similar task by linking the Raspberry Pi with the app. The smartphone application requires constant network connectivity through Wi-Fi or data connection to operate and alerts the user through push notifications.

The last part of the system is the magnetic door lock placed on the door and operated through the relay controlled by the Raspberry Pi. To turn on, the relay requires a switching circuit built using MOSFETS and diodes. When the Raspberry Pi sends signal to the switching circuit, the relay turns on, energizing the magnetic lock and locking the door. On another signal, the relay turns off, de-energizing the magnetic lock and opening the door.

IV. TESTING AND EVALUATION

The system was installed and put to test in a home that has frequent visitors. The camera was housed in an aluminum enclosure outside the front door and the touchscreen was mounted on the inner wall of the home close to the door. The credentials of 5 authorized people were entered into the database as ENT-01, ENT-02 and so on. Testing was performed over a course of 18 days. There were a total of 26 events of which 8 involved the known faces and 18 involved strangers. Known faces were correctly recognized in 6 out of 8 cases and for the rest 18 cases, all the visitors were marked as unauthorized. This insists that a more rigorous training process has to be carried out in order to ensure a 100% success, which, even if lengthy, is not impossible. Table I shows the results in details.

TABLE I. Test results of the visitor identification system

Timestamp	Actual Visitor	Displayed Visitor	Accurately identified?
2015-09-13	ENT-01	ENT-01	Yes
2015-09-13	Stranger	Stranger	Yes
2015-09-14	Stranger	Stranger	Yes
2015-09-15	Stranger	Stranger	Yes
2015-09-16	Stranger	Stranger	Yes
2015-09-17	Stranger	Stranger	Yes
2015-09-17	Stranger	Stranger	Yes
2015-09-17	**ENT-03**	**Stranger**	**No**
2015-09-18	Stranger	Stranger	Yes
2015-09-19	ENT-01	ENT-01	Yes
2015-09-20	Stranger	Stranger	Yes
2015-09-21	Stranger	Stranger	Yes
2015-09-22	Stranger	Stranger	Yes
2015-09-23	Stranger	Stranger	Yes
2015-09-24	ENT-05	ENT-05	Yes
2015-09-25	Stranger	Stranger	Yes
2015-09-26	Stranger	Stranger	Yes
2015-09-26	Stranger	Stranger	Yes
2015-09-26	Stranger	Stranger	Yes
2015-09-27	Stranger	Stranger	Yes
2015-09-27	ENT-02	ENT-02	Yes
2015-09-28	ENT-04	ENT-04	Yes
2015-09-29	**ENT-01**	**ENT-03**	**No**
2015-09-30	Stranger	Stranger	Yes
2015-09-30	Stranger	Stranger	Yes
2015-09-30	ENT-01	ENT-01	Yes

V. CONCLUSION

The recurring concern of sound household security cannot be resolved by a single package. Nevertheless, as opposed to commercially available systems, our solution provides a smarter, more user friendly approach which also comes at a lower price. The components used are readily available at electronics hobbyist shops and do not escalate the total system's cost from any aspect. Our designed system has shown satisfactory performance in real world test and as such it assets a practical implementation. In the near future, the system would be adapted to incorporate machine learning capability and would attempt to intelligently detect potential intruders by heuristically analyzing their behaviors.

REFERENCES

[1] RFC 4949, *Internet Security Glossary*, Version 2, August 2007.

[2] Y. Luo, S. Cheung and S. Ye, "Anonymous Biometric Access Control based on homomorphic encryption", *2009 IEEE International Conference on Multimedia and Expo*, 2009.

[3] S. Kundu, G. Deb, S. Sengupta and U. Saha, "Low EMI design of a microprocessor based password access control system-a case study", Proceedings of the International Conference on Electromagnetic Interference and Compatibility '99 (IEEE Cat. No. 99TH 8487), 1997.

[4] P. Teh, H. Ling and S. Cheong, "NFC smartphone based access control system using information hiding", *2013 IEEE Conference on Open Systems (ICOS)*, 2013.

[5] R. Newman, "Security and Access Control Using Biometric Technologies: Application, Technology, and Management" (1st ed.), Course Technology Press, Boston, MA, United States. 2009.

[6] Schneier.com, "The Failure of Two-Factor Authentication - Schneier on Security", 2015. [Online]. Available: https://www.schneier.com/blog/archives/2012/02/the_failure_of_2.html.

[7] K. Zetter, "Reverse-Engineered Irises Look So Real, They Fool Eye-Scanners", WIRED, 2015. [Online]. Available: http://www.wired.com/2012/07/reverse-engineering-iris-scans/.

[8] Huu-Quoc Nguyen, Ton Thi Kim Loan, Bui Dinh Mao and Eui-Nam Huh, "Low cost real-time system monitoring using Raspberry Pi", 2015 Seventh International Conference on Ubiquitous and Future Networks, 2015.

[9] K. Kumar, J. Thomas, J. Alex and R. Malhotra, "Surveillance System Based On Raspberry Pi for Monitoring a Location Through A Mobile Device", International Journal of Advanced Multidisciplinary Research (IJAMR), vol. 2, no. 3, pp. 103-108, 2015.

[10] S. Jogdand and M. Karanjkar, "Implementation of Automated Door Accessing System with Face Design and Recognition", International Journal of Science and Research (IJSR), vol. 4, no. 10, 2015.

[11] M. Doi, K. Sato and K. Chihara, "A robust face identification against lighting fluctuation for lock control", Proceedings Third IEEE International Conference on Automatic Face and Gesture Recognition, 1998.

[12] Zhujie and Y. Yu, "Face Eecognition with Eigenfaces", Proceedings of 1994 IEEE International Conference on Industrial Technology - ICIT '94, 1994.

[13] P. Viola and M. J. Jones "Rapid Object Detection using a Boosted Cascade of Simple Features", IEEE CVPR, 2001

[14] P. Viola, M. J. Jones, "Robust Real-Time Face Detection", International Journal of Computer Vision, 57(2), 2004.\

[15] A. Gupta, E. Sharma, N. Sachan and N. Tiwari, "Door Lock System through Face Recognition Using MATLAB", International Journal of Scientific Research in Computer Science and Engineering, Vol-1, Issue-3, 30 June 2013.

[16] A. Kasinski and A. Schmidt, "The architecture and performance of the face and eyes detection system based on the Haar cascade classifiers", *Pattern Anal Applic*, vol. 13, no. 2, pp. 197-211, 2009.

[17] S. Pandey and S. Sharma, "An Optimistic Approach for Implementing Viola Jones Face Detection Algorithm in Database System and in Real Time", *IJERT*, vol. 4, no. 07, 2015.

[18] R. Padilla, C. Filho and M. Costa, "Evaluation of Haar Cascade Classifiers Designed for Face Detection", *International Journal of Computer, Electrical, Automation, Control and Information Engineering*, vol. 6, no. 4, pp. 466-469, 2012.

[19] N. Gadhe, B. Lande and B. Meshram, "Intelligent System for detecting, Modeling, Classification of human behavior using image processing, machine vision and OpenCV", *IJARCET*, vol. 1, no. 4, pp. 590-599, 2012.

[20] P. Jodoin, "Comparative study of background subtraction algorithms", *J. Electron. Imaging*, vol. 19, no. 3, p. 033003, 2010.

[21] D. Huggins-Daines, M. Kumar, A. Chan, A. Black, M. Ravishankar and A. Rudnicky, "Pocketsphinx: A Free, Real-Time Continuous Speech Recognition System for Hand-Held Devices", 2006 IEEE International Conference on Acoustics Speed and Signal Processing Proceedings, 2006.