ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Image Quality Assessment for Fake Biometric Detection: Application to Iris, Fingerprint, and Face Recognition

V. Rakesh
M.Tech Student,
Department of ECE,
Aurora's Technological and Research Institute,
Uppal, Hyderabad, Telangana.

N. Nirmala Devi
Associate Professor,
Department of ECE,
Aurora's Technological and Research Institute,
Uppal, Hyderabad, Telangana.

Abstract:

To ensure the actual presence of a real legitimate trait in contrast to a fake self-manufactured synthetic or reconstructed sample is a significant problem in biometric authentication, which requires the development of new and efficient protection measures. In this paper, we present a novel software based fake detection method that can be used in multiple biometric systems to detect different types of fraudulent access attempts. In the proposed method, we present a novel software-based fake detection method that can be used in multiple biometric systems to detect different types of fraudulent access attempts. The objective of the proposed system is to enhance the security of biometric recognition frameworks, by adding liveness assessment in a fast, user-friendly, and non-intrusive manner, through the use of image quality assessment.

Index Terms:

Image quality assessment, biometrics, security, attacks, countermeasures.

I. INTRODUCTION:

Now a day's security plays a vital role in the daily lives of people starting from the common people to officials like VIPs, VVIPs. The existing security systems are having biometric systems as their core part. They are using biometric systems like FPRS (Finger Print Recognition System) and EIRS (Eye Iris Recognition System). There is a possibility to fraud these types of biometric based security systems. The traditional algorithms identify faces by extracting landmarks, or features from an image of the subject's face. For example the algorithm may analyze the relative position, size, and shape of the eyes, nose, cheekbones, and jaw. These features are then used to search for other images with matching features. Some algorithms normalize a gallery of face images and then compress the face data, only saving the data in the image that is useful for face detection. Recognition algorithms are divided into two types. First type is geometric which looks at distinguishing features and second type is photometric which distill an image into values and comparing the values with the templates to eliminate variances. Most popular recognition algorithms include PCA (Principal Component Analysis) using Eigen faces, LDA (Linear Discriminate Analysis), Elastic Bunch Graph Matching using the Fisher Face algorithm, the Hidden Markov Model, and neuronal motivated dynamic link matching. The latest technology that is emerged into facial recognition system is three- dimensional face recognition. This technique makes use of 3D sensors to capture information about the shape of a face. This information is later used to identify the distinctive features of the surface of a face such as contour of the eyes sockets, nose, and chin. One of the advantages of 3D face recognition is: this is not affected by changes in lighting like other techniques. It can also identify a face from a range of viewing angles, including a profile view. The FRS (Facial Recognition System) is having their major application as security systems. Other application is to prevent the voter fraud in elections. Some people will try to vote under several names in an attempt to place multiple votes. By comparing new facial image with those already there in the data base authorities can easily reduce the duplicate registrations. Similar techniques can be used to prevent the people from obtaining fake identification cards and driving licenses.

II.SYSTEM ARCHITECTURE:

The system makes use embedded board which makes use of less power consumptive and advanced micro controller like Raspberry Pi. Our ARM11 board comes with integrated peripherals like USB, ADC and Serial etc. On this board we are installing Linux operating system with necessary drivers for all peripheral devices .Mainly this system consists of peripherals like UVC driver camera and Fingerprint module.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

After connecting all the devices, power uPs the device. When the device starts booting from flash, it first loads the Linux to the device and initializes all the drivers and the core kernel. After initialization of the kernel it first checks weather all the devices are working properly or not. After that it loads the file system and starts the startup scripts for running necessary processes and daemons. Finally it starts the main application.This system captures image by means of web camera connected to ARM microcontroller through USB and the image is processed by using image processing technique. Image processing is any form of signal processing for which the input is an image, such as a photograph or video frame; the output of image processing may be either an image or a set of characteristics or parameters related to the image. Using algorithms child movement is monitored continuously like child position, child crying etc. And all these captured images are displayed on Display unit connected to ARM microcontroller.

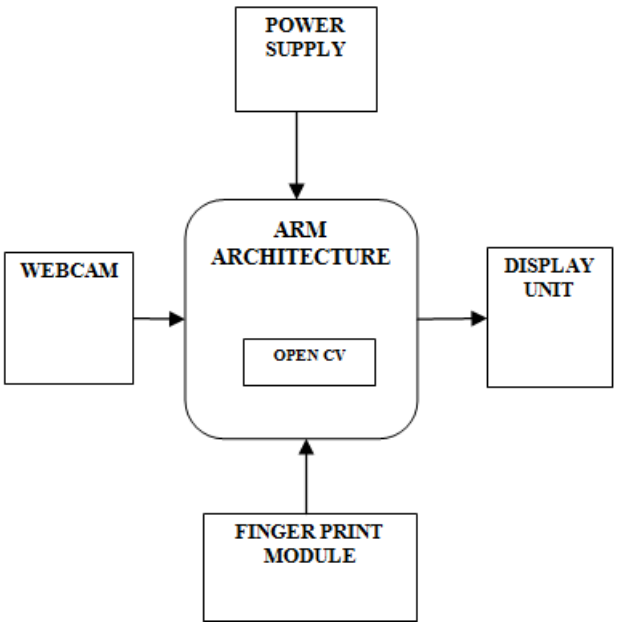


Fig.1: Block Diagram for Proposed System

When our application starts running it first check all the devices and resources which it needs are available or not. After that it checks the connection with the devices and gives control to the user. The controller will recognize the face and iris of the particular person from the image. The finger print module will take the finger print from the person and send to controller. The controller will recognize the finger print of particular person from the data base. If they are matched then it will display the data on display unit.

III.HAAR CASCADE:

Haar-like features are digital image features used in object recognition. They owe their name to their intuitive similarity with Haar wavelets and were used in the first real-time face detector. Here we will work with face detection. Initially, the algorithm needs a lot of positive images (images of faces) and negative images (images without faces) to train the classifier. Then we need to extract features from it. For this, haar features shown in below image are used. They are just like our convolutional kernel. Each feature is a single value obtained by subtracting sum of pixels under white rectangle from sum of pixels under black rectangle.

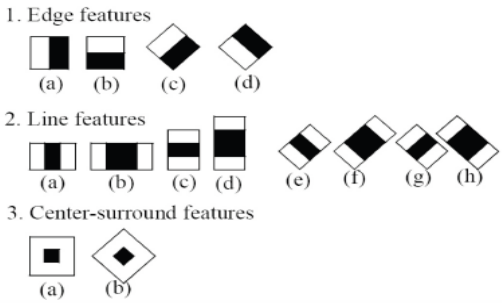


Fig.2: Haar Features

Now all possible sizes and locations of each kernel is used to calculate plenty of features. For each feature calculation, we need to find sum of pixels under white and black rectangles. To solve this, they introduced the integral images. It simplifies calculation of sum of pixels, how large may be the number of pixels, to an operation involving just four pixels.

IV.HARDWARE MODULES

A – ARM Architecture:

The Raspberry Pi is a credit-card-sized single-board computer developed in the UK by the Raspberry Pi Foundation with the intention of promoting the teaching of basic computer science in schools.

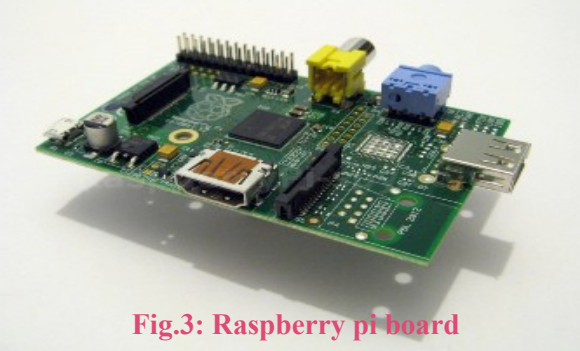


Fig.3: Raspberry pi board

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

The Raspberry Pi is manufactured in two board configurations through licensed manufacturing deals with Newark element14 (Premier Farnell), RS Components and Egoman. These companies sell the Raspberry Pi online. Egoman produces a version for distribution solely in China and Taiwan, which can be distinguished from other Pis by their red coloring and lack of FCC/CE marks. The hardware is the same across all manufacturers. The Raspberry Pi has a Broadcom BCM2835 system on a chip (SoC), which includes an ARM1176JZF-S 700 MHz processor, Video Core IV GPU, and was originally shipped with 256 megabytes of RAM, later upgraded to 512 MB. It does not include a built-in hard disk or solid-state drive, but uses an SD card for booting and persistent storage.

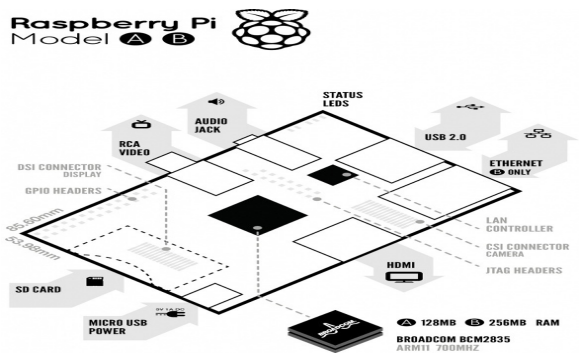


Fig.4: Board features

The Foundation provides Debian and Arch Linux ARM distributions for download. Tools are available for Python as the main programming language, with support for BBC BASIC (via the RISC OS image or the Brandy Basic clone for Linux), C, Java and Perl.

B – Fingerprint Module:

A fingerprint is an impression of the friction ridges on all parts of the finger. A friction ridge is a raised portion of the epidermis on the palmar (palm) or digits (fingers and toes) or plantar (sole) skin, consisting of one or more connected ridge units of friction ridge skin. These are sometimes known as “epidermal ridges” which are caused by the underlying interface between the dermal papillae of the dermis and the interpapillary (rete) pegs of the epidermis. These epidermal ridges serve to amplify vibrations triggered when fingertips brush across an uneven surface, better transmitting the signals to sensory nerves involved in fine texture perception. The ridges assist in gripping rough surfaces, as well as smooth wet surfaces.

Fig.5: Fingerprint Module

Fingerprints may be deposited in natural secretions from the eccrine glands present in friction ridge skin (secretions consisting primarily of water) or they may be made by ink or other contaminants transferred from the peaks of friction skin ridges to a relatively smooth surface such as a fingerprint card. The term fingerprint normally refers to impressions transferred from the pad on the last joint of fingers and thumbs, though fingerprint cards also typically record portions of lower joint areas of the fingers (which are also used to make identifications).

C – Universal Video Camera:

A UVC (or Universal Video Class) driver is a USB-category driver. A driver enables a device, such as your webcam, to communicate with your computer’s operating system. And USB (or Universal Serial Bus) is a common type of connection that allows for high-speed data transfer. Most current operating systems support UVC. Although UVC is a relatively new format, it is quickly becoming common.

There are two kinds of webcam drivers:

1.The one included with the installation disc that came with your product. For your webcam to work properly, this driver requires some time to install. It is specifically tuned for your webcam, designed by your webcam manufacturer and optimized for webcam performance.

2.A UVC driver:-You can only use one driver at a time, but either one will allow you to use your webcam with various applications.

It is a USB video camera using with laptop and Desktop computers.

The following Logitech webcams support UVC:

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

•Logitech® QuickCam® Pro 9000 for Business
•Logitech® QuickCam® Pro for Notebooks Business
•Logitech® QuickCam® Communicate MP for Business
•Logitech® QuickCam® Deluxe for Notebooks Business

Fig.6: UVC Driver Camera

V.SOFTWARE REQUIREMENTS:

A – Operating System:

Linux or GNU/Linux is a free and open source software operating system for computers. The operating system is a collection of the basic instructions that tell the electronic parts of the computer what to do and how to work. Free and open source software (FOSS) means that everyone has the freedom to use it, see how it works, and changes it.There is a lot of software for Linux, and since Linux is free software it means that none of the software will put any license restrictions on users. This is one of the reasons why many people like to use Linux.Projects that interface with the kernel provide much of the system's higher-level functionality. The GNU userland is an important part of most Linux-based systems, providing the most common implementation of the C library, a popular shell, and many of the common UNIX tools which carry out many basic operating system tasks. The graphical user interface (or GUI) used by most Linux systems is built on top of an implementation of the X Window System.

B – Integrated Development Environment (QT):

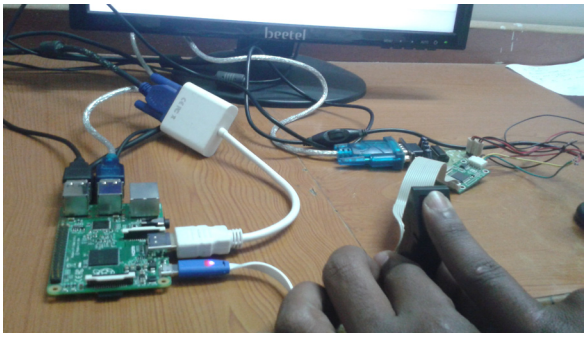
Qt is a cross-platform application framework that is widely used for developing application software with a graphical user interface (GUI) (in which cases Qt is classified as awidget toolkit), and also used for developing non-GUI programs such ascommand-line tools and consoles for servers. Qt uses standard C++ but makes extensive use of a special code generator (called the Meta Object Compiler, or moc) together with several macros to enrich the language. Qt can also be used in several other programming languages via language bindings.

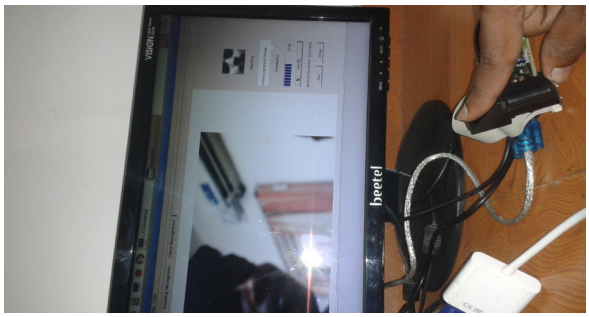
It runs on the major desktop platforms and some of the mobile platforms. Non-GUI features include SQL database access, XML parsing, thread management, network support, and a unified cross-platform application programing interface for file handling.It has extensive internationalization support.

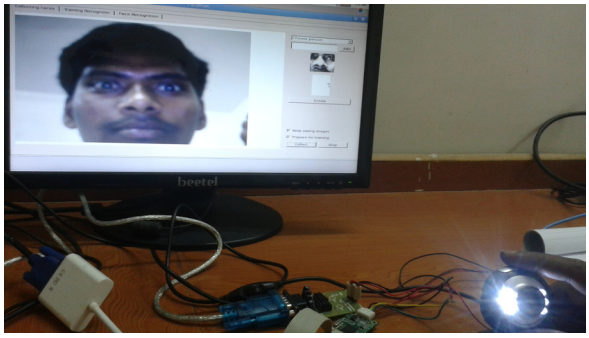
C – Opencv (image Processing library):

Open CV (Open Source Computer Vision) is a library of programming functions for real time computer vision. It is developed by Willow Garage, which is also the organization behind the famous Robot Operating System (ROS). Define abbreviations and acronyms the first time they are used in the text, even after they have been defined in the abstract. Abbreviations such as IEEE, SI, MKS, CGS, sc, dc, and rms do not have to be defined. Do not use abbreviations in the title or heads unless they are unavoidable.

VI.RESULTS:







ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

VII.CONCLUSION:

The project "DEVELOPMENT OF DIGITAL SECURITY SYSTEM FOR FAKE BIOMETRIC DETECTION" has been successfully designed and tested. It has been developed by integrating features of all the hardware components and software used. Presence of every module has been reasoned out and placed carefully thus contributing to the best working of the unit. Secondly, using highly advanced ARM9 board and with the help of growing technology the project has been successfully implemented.

VIII.REFERENCES:

[1] S. Prabhakar, S. Pankanti, and A. K. Jain, "Biometric recognition: Security and privacy concerns," IEEE Security Privacy, vol. 1, no. 2, pp. 33–42, Mar./Apr. 2003.

[2] T. Matsumoto, "Artificial irises: Importance of vulnerability analysis," in Proc. AWB, 2004.

[3] J. Galbally, C. McCool, J. Fierrez, S. Marcel, and J. Ortega-Garcia, "On the vulnerability of face verification systems to hill-climbing attacks," Pattern Recognit., vol. 43, no. 3, pp. 1027–1038, 2010.

[4] A. K. Jain, K. Nandakumar, and A. Nagar, "Biometric template security," EURASIP J. Adv. Signal Process., vol. 2008, pp. 113–129, Jan. 2008.

[5] J. Galbally, F. Alonso-Fernandez, J. Fierrez, and J. Ortega-Garcia, "A high performance fingerprint liveness detection method based on quality related features," Future Generat. Comput. Syst., vol. 28, no. 1, pp. 311–321, 2012.

[6] K. A. Nixon, V. Aimale, and R. K. Rowe, "Spoof detection schemes," Handbook of Biometrics. New York, NY, USA: Springer-Verlag, 2008, pp. 403–423.

[7] ISO/IEC 19792:2009, Information Technology—Security Techniques— Security Evaluation of Biometrics, ISO/IEC Standard 19792, 2009.

[8] Biometric Evaluation Methodology. v1.0, Common Criteria, 2002. [9] K. Bowyer, T. Boult, A. Kumar, and P. Flynn, Proceedings of the IEEE Int. Joint Conf. on Biometrics. Piscataway, NJ, USA: IEEE Press, 2011.

[10] G. L. Marcialis, A. Lewicke, B. Tan, P. Coli, D. Grimberg, A. Congiu, et al., "First international fingerprint liveness detection competition— LivDet 2009," in Proc. IAPR ICIAP, Springer LNCS-5716. 2009, pp. 12–23.

[11] M. M. Chakka, A. Anjos, S. Marcel, R. Tronci, B. Muntoni, G. Fadda, et al., "Competition on countermeasures to 2D facial spoofing attacks," in Proc. IEEE IJCB, Oct. 2011, pp. 1–6.

[12] J. Galbally, J. Fierrez, F. Alonso-Fernandez, and M. Martinez-Diaz, "Evaluation of direct attacks to fingerprint verification systems," J. Telecommun. Syst., vol. 47, nos. 3–4, pp. 243–254, 2011.

[13] A. Anjos and S. Marcel, "Counter-measures to photo attacks in face recognition: A public database and a baseline," in Proc. IEEE IJCB, Oct. 2011, pp. 1–7.

[14] Biometrics Institute, London, U.K. (2011). Biometric Vulnerability Assessment Expert Group [Online]. Available: http://www. biometricsinstitute.org/pages/biometric-vulnerability-assessment-expertgroup- bvaeg.html

[15] (2012). BEAT: Biometrices Evaluation and Testing [Online]. Available: http://www.beat-eu.org/

[16] (2010). Trusted Biometrics Under Spoofing Attacks (TABULA RASA) [Online]. Available: http://www.tabularasa-euproject.org/

[17] J. Galbally, R. Cappelli, A. Lumini, G. G. de Rivera, D. Maltoni, J. Fierrez, et al., "An evaluation of direct and indirect attacks using fake fingers generated from ISO templates," Pattern Recognit. Lett. vol. 31, no. 8, pp. 725–732, 2010.

[18] J. Hennebert, R. Loeffel, A. Humm, and R. Ingold, "A new forgery scenario based on regaining dynamics of signature," in Proc. IAPR ICB, vol. Springer LNCS-4642. 2007, pp. 366–375.

[19] A. Hadid, M. Ghahramani, V. Kellokumpu, M. Pietikainen, J. Bustard, and M. Nixon, "Can gait biometrics be spoofed?" in Proc. IAPR ICPR, 2012, pp. 3280–3283.

[20] Z. Akhtar, G. Fumera, G. L. Marcialis, and F. Roli, "Evaluation of serial and parallel multibiometric systems under spoofing attacks," in Proc.IEEE 5th Int. Conf. BTAS, Sep. 2012, pp. 283–288.