International Journal of Engineering Research and General Science Volume 3, Issue 5, September-October, 2015
ISSN 2091-2730

IMAGE QUALITY ASSESSMENT FOR FAKE BIOMETRIC DETECTION: APPLICATION TO IRIS, FINGERPRINT, AND FACE RECOGNITION

Mohd Mujeed Uddin[1],S.V Altaf[2],Abdul Wasay Mudassir[3]

Mohd Mujeed Uddin[1],M.Tech student,ECE Department,Lords Institute of Engineering and Technology,Hyderabad,Telangana,India.mohdmujeebuddin2@gmail.com

S.V Altaf[2],Associate Professor,ECE Department,Lords Institute of Engineering and Technology,Hyderabad,Telangana,India.svaltaf@hotmail.com

Abdul Wasay Mudassir[3],Associate Professor,ECE Department,Lords Institute of Engineering and Technology,Hyderabad,Telangana,India.wasay403@gmail.com

Abstract— to ensure the actual presence of real legit i-mate in contrast to self manufactured or reconstructed sample is a significant problem in bio-metric 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 bio-metric systems to detect different types of fraudulent access attempts. The objective of the proposed system is to enhance the security of bio-metric recognition frameworks, by adding liveness assessment in a fast, user-friendly, and non-intrusive manner, through the use of image quality assessment. The proposed approach presents a very low degree of complexity, which makes it suitable for real-time applications, using 25 general image quality features extracted from one image (i.e., the same acquired for authentication purposes) to distinguish between legitimate and impostor samples.[3] The experimental results, obtained on publicly available data sets of fingerprint, iris, and 2D face, show that the proposed method is highly competitive compared with other state-of-the-art approaches and that the analysis of the general image quality of real bio metric samples reveals highly valuable information that may be very efficiently used to discriminate them from fake traits.[9]

Index Terms— Image quality assessment, bio-metrics, security, attacks, countermeasures.

I.INTRODUCTION

A novel software-based multi-biometric and multi-attack protection method which targets to overcome part of these limitations through the use of image quality assessment (IQA). It is not only capable of operating with a very good performance under different biometric systems (multi-biometric) and for diverse spoofing scenarios, but it also provides a very good level of protection against certain non-spoofing attacks (multi-attack).[15] Moreover, being software-based, it presents the usual advantages of this type of approaches: fast, as it only needs one image (i.e., the same sample acquired for bio-metric recognition) to detect whether it is real or fake; non-intrusive; user-friendly (transparent to the user); cheap and easy to embed in already functional systems (as no new piece of hardware is required).

An added advantage of the proposed technique is its speed and very low complexity, which makes it very well suited to operate on real scenarios (one of the desired characteristics of this type of methods). As it does not deploy any trait-specific property (e.g., minutiae points, iris position or face detection),the computation load needed for image processing purposes is very reduced, using only general image quality measures fast to compute, combined with very simple classifiers. It has been tested on publicly available attack databases of iris, fingerprint and 2D face, where it has reached results fully comparable to those obtained on the same databases and following the same experimental protocols by more complex trait-specific top-ranked approaches from the state-of-the-art.[14]

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.

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 start up 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 micro-controller 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 micro-controller.

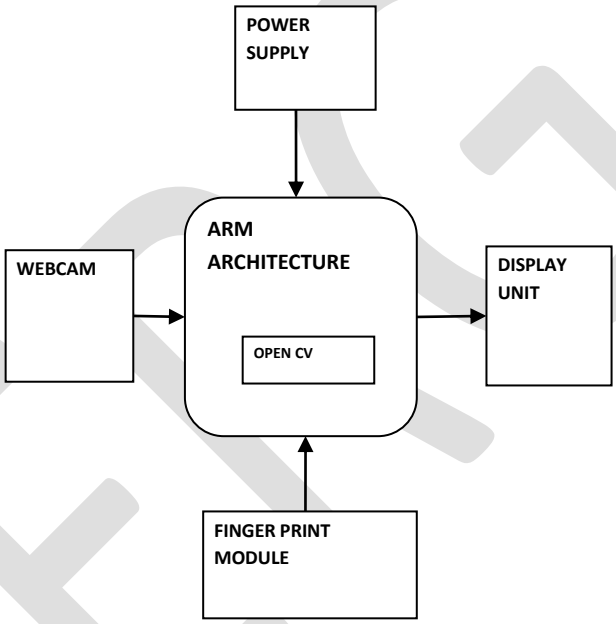


Fig.1: Block Diagram for Proposed System

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.

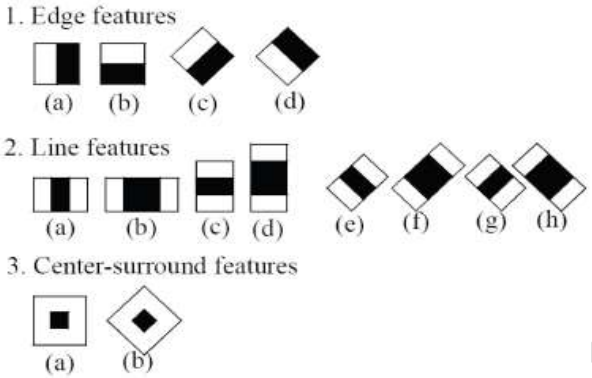


Fig.2: Haar Features

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.[1]

IV. PCA ALGORITHM:

PCA method (i.e., eigenface method) is M. Turk and A. Pent land proposed in the literature, the basic idea is: the image vector by KL transformation from high-dimensional vector is converted to low-dimensional vector, and the formation of low-dimensional linear vector space, that is, subspace, and then face the projector to the low dimensional space, with the resulting projection coefficients as the recognition feature vectors. Recognize faces, just the projection coefficient of samples to be identified in the target database sample set of projection coefficients were compared to determine what types of recently. PCA algorithm is divided into two steps: the core face database generation phase, the training phase and identification phase.

V.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. The Raspberry Pi is manufactured in two board configurations through licensed manufacturing deals with Newark element14 (Premier Farnell), RS Components and Ego-man. These companies sell the Raspberry Pi online. Ego-man produces a version for distribution solely in China and Taiwan, which can be distinguished from other Pi's by their red coloring and lack of FCC/CE marks.

Fig.3: Raspberry pi board

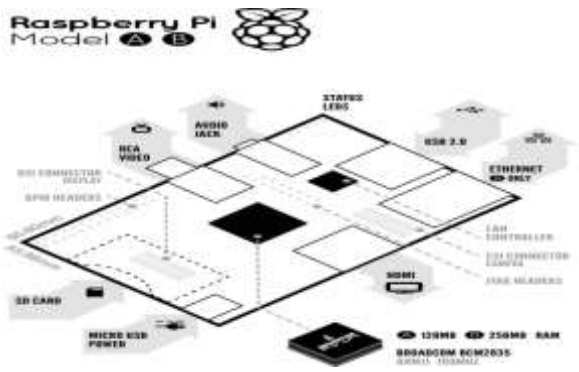


Fig.4: Board features

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.[7]

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 pal-mar (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 inter papillary (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).[11][13]

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.[10]

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:

- 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

VI. 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.[6]

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)

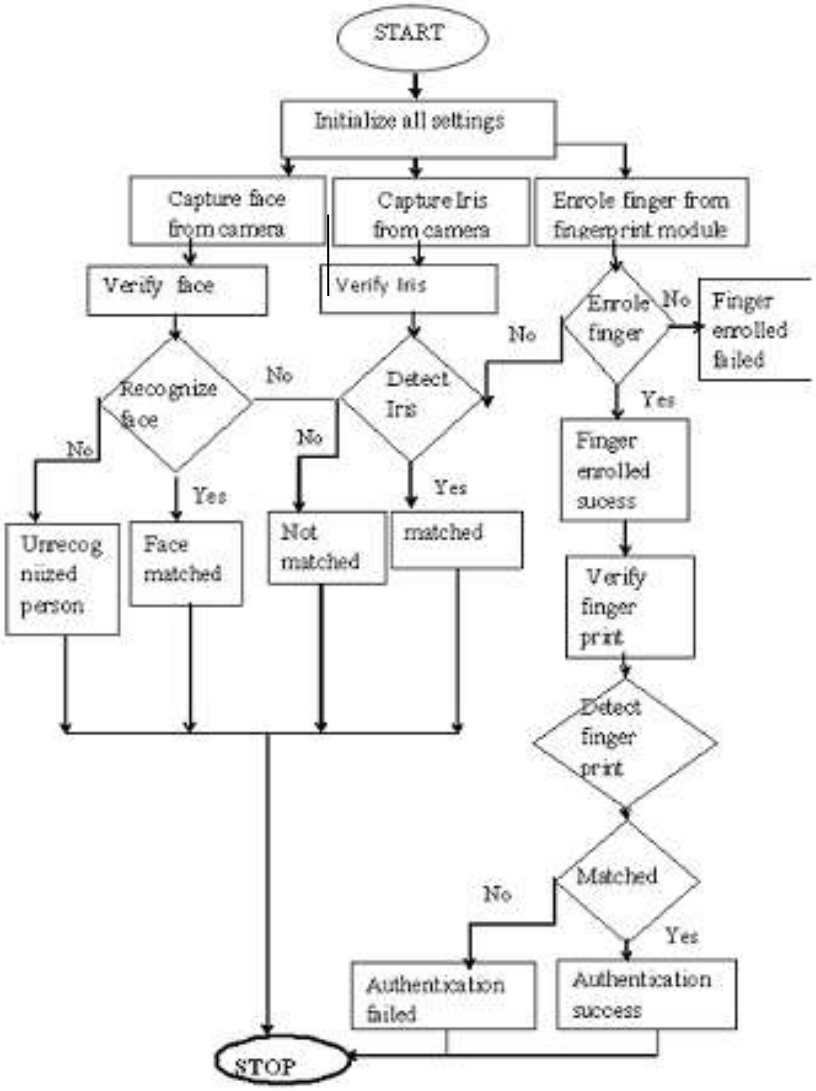
Qt is a cross-platform application framework that is widely used for developing application software with a graphical user interface (GUI) (in which cases Qt is classified as awidget toolkit), and also used for developing non-GUI programs such ascommand-line tools and consoles for servers.[8] Qt uses 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 programming 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).[2]

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.

Flow chart



VII. RESULT

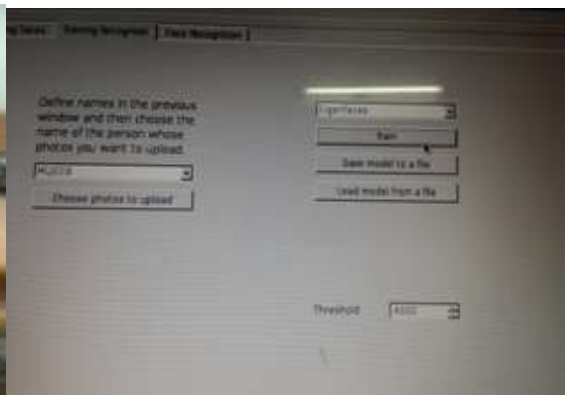


Fig.7:Overall view of the System Fig.8:View of the Software

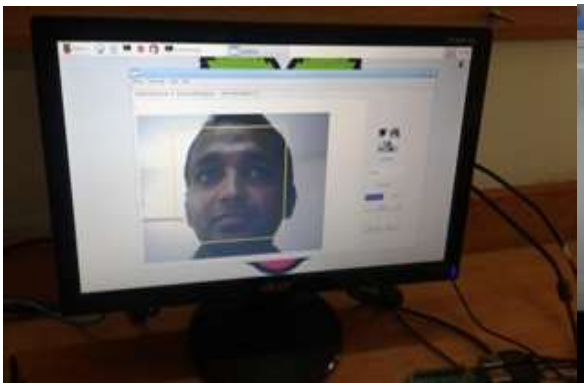


Fig.9:Identification of Person

Fig.10:Samples collection

After designing the system using Advance Raspberry Pi Board(BCM2835),Finger Print Module(R305),Web Camera etc as a Hardware Module and Qt Creator,Open CV library,Haar-cascade algorithm and Linux OS as Software Module the whole system is successfully designed and got the above results.

VIII. CONCLUSION

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

REFERENCES:

[1] Dmitry Pertsau,AndreyUvarov " Face Detection Algorithm Using Haar-Like Feature for GPU Architecture" The 7th IEEE International conference on Intelligent Data Aquisation and Advanced Computing Systems: Technology and Applications 12-14 september 2013

[2].Paul Viola and Michael Jones in their paper "Rapid Object Detection using aBoosted Cascade of simple Features" The IEEE International conference on computer vision and pattern recognition.

[3]Dr. Sunil Kumar Singlain his paper " A Review of Image Based Fingerprint Authentication Algorithms". The International Journal of Advanced Research in Computer science and Software Engineering: Volume 3, issue 6, june 2013

[4]J. Galbally, J. Ortiz-Lopez, J. Fierrez, and J. Ortega-Garcia, "Iris liveness detection based on quality related features," in *Proc. 5th IAPR ICB*, Mar./Apr. 2012, pp. 271–276.

[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]"Linux for Embedded and Real time Applications", by Doug Abbott .

[7]. Steve Furber, ARM SYSTEM-ON-CHIP ARCHITECTURE, Second Edition Person Education Limited, 2000.

[8].http://download.qt.io./learning/developerguides/qtquickappdevintro/QtQuickApp

[9]R. Cappelli, D. Maio, A. Lumini, and D. Maltoni, "Fingerprint imagereconstruction from standard templates," *IEEE Trans. Pattern Anal.Mach. Intell.*, vol. 29, no. 9, pp. 1489–1503, Sep. 2007.

[10]Liu Chun-cheng. USB Webcam Driver Development Based on Embedded Linux [J].Compter Engineering and Design, 2007, 28(8):1885-1888.

[11]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, ap.311–321, 2012.

[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]D. Maltoni, D. Maio, A. Jain, and S. Prabhakar, *Handbook of Fingerprint Recognition*. New York, NY, USA: Springer-Verlag, 2009.

[14]A. Liu, W. Lin, and M. Narwaria, "Image quality assessment based on gradient similarity," *IEEE Trans. Image Process.*, vol. 21, no. 4, ap.1500–1511, Apr. 2012.

[15]I. Chingovska, A. Anjos, and S. Marcel, "On the effectiveness of local binary patterns in face anti-spoofing," in *Proc. IEEE Int. Conf. Biometr. Special Interest Group*, Sep. 2012, pp. 1–7.

[16]H. R. Sheikh and A. C. Bovik, "Image information and visual quality," *IEEE Trans. Image Process.*, vol. 15, no. 2, pp. 430–444, Feb. 2006.

[17](2012). LIVE [Online]. Available: http://live.ece.utexas.edu/research/ Quality/index.htm

[18]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.

[19]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.

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