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

N. Chakradhar1, P. Sampath Kumar2, K. Santosh Kumar3

1 M.Tech, Malla Reddy Institute of Technology, Hyderabad, India,

2 Associate Professor & HOD, Malla Reddy Institute of Technology, Hyderabad, India.

3 Assistant Professor, Malla Reddy Institute of Technology, Hyderabad, India.

Abstract: In this Paper, 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. 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. 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. 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 biometric samples reveals highly valuable information that may be very efficiently used to discriminate them from fake traits.

Index Terms— Image quality assessment, biometrics, security, attacks, countermeasures.

I. INTRODUCTION

The main objective of the proposed desertion is to develop a system to enhance the security of biometric recognition framework, by providing a two stage security using finger print and face detection applications and adding liveness assessment in a fast, user-friendly, and non-intrusive manner, 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 no spoofing attacks (multi-attack). I. Chingovska et al.,
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.

II. LITERATURE SURVEY

Literature survey is the most important step in project development process. Before developing the tool it is necessary to determine the time factor and economy. Once these things are satisfied, the next steps are determining resources like which hardware, operating systems and languages that can be used for implementing this project. Once we start implementing we require lot of external support. Before building the system the below considerations are taken into account for developing the proposed system. With embedded systems fast expanding its reach, subject matter related to this field is available in abundance. While working on this project we have studied matter from various sources such as books, online articles and reference manuals. The knowledge gained from this activity has been of great help to us in understanding the basic concepts related to our project and has ignited further interest in this topic.

1. “Linux for Embedded and Real time Applications”, by Doug Abbott has been of great help in providing an introduction to the process of building embedded systems in Linux. It has helped us understand the process of configuring and building the Linux kernel and installing tool chains.

2. We understood the preponderance of the ARM processors in the field of embedded systems and the features of ARM processors from the document “The ARM Architecture” by Leonid Ryzhyk. The ARM architecture is a confluence of many useful features that makes it better than other peer processors. Being small in size and requiring less power, they prove useful in providing an efficient performance in embedded applications.

Block diagram:
III. METHODOLOGY

EXISTING SYSTEM

Fake biometrics means by using the real images like iris images captured from a printed paper or fingerprint captured from a dummy finger of human identification characteristics create the fake identities like fingerprint, iris on printed paper. Fake user first captures the original identities of the genuine user and then they make the fake sample for authentication. There is no such technology to provide security for fake users.

PROPOSED SYSTEM

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. Here we are interfacing camera to Raspberry pi. The camera will capture face image of a person and send to controller. The controller will recognize the face and iris of the particular person from the image. The fingerprint module will take the fingerprint from the person and send to controller. The controller will recognize the fingerprint of particular person from the data base. If they are matched then it will display the data on display unit.

IV. HARDWARE AND SOFTWARE

In this section, we give an overview on the proposed system architecture. The system makes use embedded board which makes use of less power consumptive and advanced micro controller like BCM2836. BCM2836 is a Broadcom company’s microcontroller which is designed based on the structure of ARM 11 family. This microcontroller works for a voltage of +3.3V DC and at an operating frequency of 900 MHz. Here we are using Raspberry Pi board as our platform. It has an ARM-11 SOC with integrated peripherals like USB, Ethernet and serial etc. On this board we are installing Linux operating system with necessary drivers for all peripheral devices and user level software stack which includes a light weight GUI based on XServer, V4L2 API for
interacting with video devices like cameras, TCP/IP stack to communicate with network devices and some standard system libraries for system level general IO operations. The Raspberry Pi board equipped with the above software stack is connected to the outside network and a camera is connected to the Raspberry Pi through USB bus. On the other side we have to host a web server with cloud facility.

The system uses webcam which is places at forehead of visually impaired person and is connected to Raspberry Pi board through USB device. Install CMOS camera device driver in Raspberry pi board. Now the camera will capture the images. The board will take the images from camera and display it on monitor. Also it saves the images in the form of frames in pen drive.

After connecting all the devices then power up the device. When the device starts booting from flash, it first load the Linux to the device and initialize all the drivers and the core kernel. After initialization of the kernel it first check whether all the devices are working properly or not. After that it loads the file system and start the startup scripts for running necessary processes and daemons. Finally it starts the main application. 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 GUI for the user has the following options.

An optional label is displayed with the help of GUI

After assembling the entire hardware as per our block diagram described in third chapter we need to power up the entire kit. After this we can access the designed user interface in two ways. With the help of console output screen on desktop.

CONSOLE OUTPUT SCREEN ON DESKTOP

Open the shell on linux operating system and type the following command.

1. Sudo bash (converting from normal user to super user).
2. Startx (starting session)

Now go to accessories( ctrl+esc) ,in that click on terminal and press enter.with this we will get a terminal opened.

Now type following commands on the terminal.

```
cd mo click tab and press enter
./mo click tab and press enter
```

With this we will get a screen on the desktop as shown below
Fig 4.1 Console Output Screen

Now by using this screen we can control the devices in that network.

A. Linux 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.

A Linux-based system is a modular Unix-like operating system. It derives much of its basic design from principles established in UNIX during the 1970s and 1980s. Such a system uses a monolithic kernel, the Linux kernel, which handles process control, networking, and peripheral and file system access. Device drivers are either integrated directly with the kernel or added as modules loaded while the system is running.

Fig. Architecture of Linux Operating System

B. Qt for Embedded Linux:

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 a widget toolkit), and also used for developing non-GUI programs such as command-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 features the mobile platforms Non-GUI 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. Open CV Library:

Computer vision is a rapidly growing field, partly as a result of both cheaper and more capable cameras partly because of affordable processing power, and partly because vision algorithms are starting to mature. Open CV itself has played a role in the growth of computer vision by enabling thousands of people to do more productive work in vision. With its focus on real-time vision, Open CV helps students and professionals efficiently implement projects and jump-start research by providing them with a computer vision and machine learning infrastructure that was previously available only in a few mature research labs.

V. 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


BIOGRAPHIES

N. Chakradhar Pursuing (M.Tech)Post graduation in Electronics and Communication Engineering i.e., (VLSI & Embedded Systems), Malla Reddy Institute of Technology, Hyderabad
P.Sampath Kumar Pursuing Ph.D. Having 15 Years of Teaching Experience. Presently Working As Associate Professor and HOD in Department of Electronics and Communication Engineering, Malla Reddy Institute of Technology, Hyderabad.

K.Santosh Kumar, M.Tech, Presently Working As Assistant Professor in Department of Electronics and Communication Engineering, Malla Reddy Institute of Technology, Hyderabad.