iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 3 **Issue:** VI **Month of publication:** June 2015

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Design of an Embedded System for Fake Biometric Detection Using Image Quality Assessment

M.Aswadhama, P.Sreenivasulu, M.Tech(ph.d)
Department of Electronics and communication Engineering
Audisankara College of Engineering & Technology, Gudur (Autonomous)

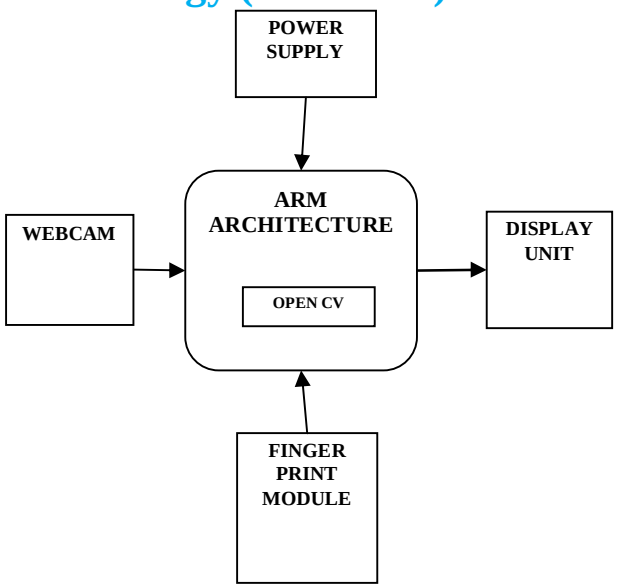
Abstract: ***To ensure the actual presence of a real legitimate trait in contrast to a fake self-manufactured synthetic or reconstructed sample is a significant problem in biometric authentication, which requires the development of new and efficient protection measures. In this paper, we present a novel 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

In recent years, the increasing interest in the evaluation of biometric systems security has led to the creation of numerous and very diverse initiatives focused on this major field of research: the publication of many research works disclosing and evaluating different biometric vulnerabilities, the proposal of new protection methods, related book chapters, the publication of several standards in the area, the dedication of specific tracks, sessions and workshops in biometric-specific and general signal processing conferences , the organization of competitions focused on vulnerability assessment the acquisition of specific datasets, the creation of groups and laboratories specialized in the evaluation of biometric security, or the existence of several European Projects with the biometric security topic as main research interest. All these initiatives clearly highlight the importance given by all parties involved in the development of biometrics (i.e., researchers, developers and industry) to the improvement of the systems security to bring this rapidly emerging technology into practical use. Among the different threats analyzed, the so-called *direct* or *spoofing* attacks have motivated the biometric community to study the vulnerabilities against this type of fraudulent actions in modalities such as the iris, the fingerprint, the face, the signature, or even the gait and multimodal approaches. In these attacks, the intruder uses some type of synthetically produced artifact (e.g., gummy finger, printed iris image or face mask), or tries to mimic the behaviour of the genuine user (e.g., gait, signature), to fraudulently access the biometric system. As this type of attacks is performed in the analog domain and the interaction with the device is done following the regular protocol, the usual digital protection mechanisms (e.g., encryption, digital signature or watermarking) are not effective. The aforementioned works and other analogue studies have clearly shown the necessity to propose and develop specific protection methods against this threat. This way, researchers have focused on the design of specific countermeasures that enable biometric systems to detect fake samples and reject them, improving this way the robustness and security level of the systems.

II.SYSTEM ARCHITECTURE

The system makes use embedded board which makes use of less power consumptive and advanced micro controller like S3C2440. S3C2440 is a Samsung company's microcontroller which is designed based on the structure of ARM 920T family. This microcontroller works for a voltage of +3.3V DC and at an operating frequency of 400 MHz, The maximum frequency up to which this micro controller can work is 533 MHz. We cannot get S3C2440 microcontroller individually. We will get it in the form of FRIENDLY ARM board otherwise we can call it as MINI 2440 board. Our ARM 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 startup scripts for running necessary processes and daemons. Finally it starts the main application.

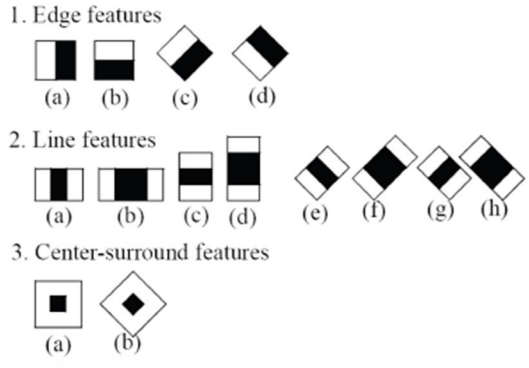


When our application starts running it first check all the devices and resources which it needs are available or not. After that it checks the connection with the devices and gives control to the user. This system captures image by means of web camera connected to ARM microcontroller through USB and 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.

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.

A. 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.



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.

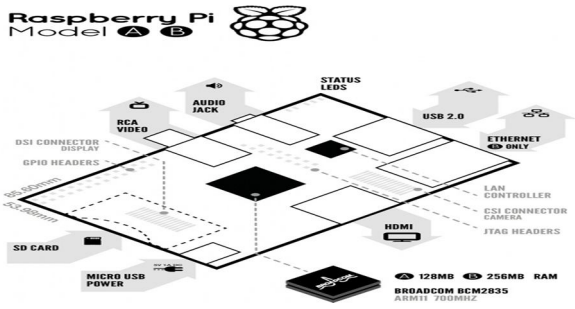
III. HARDWARE MODULES

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.

Raspberry pi board

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.



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. 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

It is a USB video camera using with laptop and Desktop computers.
The following Logitech webcams support UVC:

1) Logitech® QuickCam® Pro 9000 for Business
2) Logitech® QuickCam® Pro for Notebooks Business
3) Logitech® QuickCam® Communicate MP for Business
4) Logitech® QuickCam® Deluxe for Notebooks Business

IV. 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 user land 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.

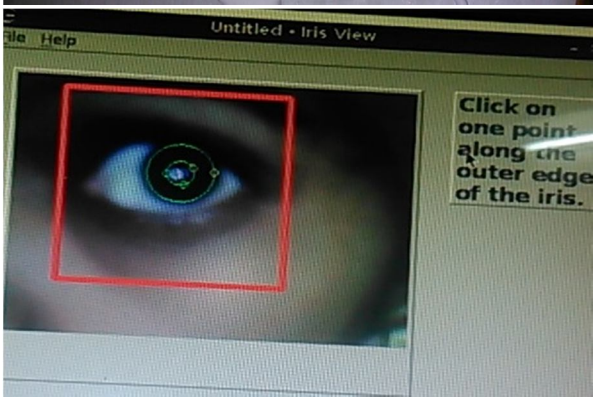
B. Integrated Development Environment (QT)

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 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 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). 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.

V. RESULTS



VI. CONCLUSION

The project "DESIGN OF AN EMBEDDED SYSTEM FOR FAKE BIOMETRIC DETECTION USING IMAGE QUALITY ASSESSMENT" 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

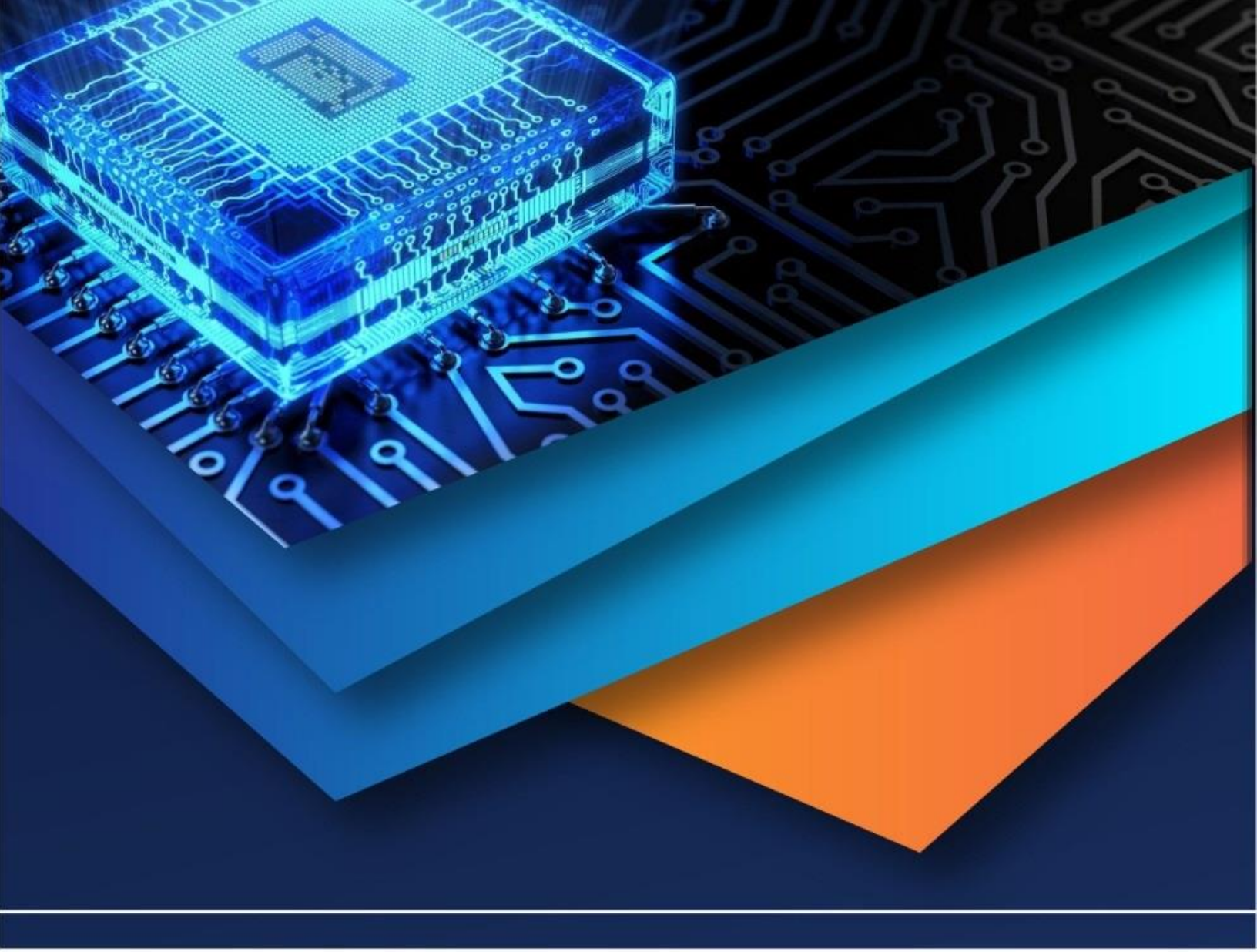
[1] S. Prabhakar, S. Pankanti, and A. K. Jain, "Biometric recognition: Security and privacy concerns," IEEE Security Privacy, vol. 1, no. 2, pp. 33–42, Mar./Apr. 2003.
[2] T. Matsumoto, "Artificial irises: Importance of vulnerability analysis," in Proc. AWB, 2004.
[3] J. Galbally, C. McCool, J. Fierrez, 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.

AUTHORS

[1]M.Aswadhama received his B.TECH degree in Electronics and Communication Engineering from A.V.S College Of Engg& Technology,Veeranna Kanupur,SPSR Nellore(Dist), affiliated to JNTU Anantpur. He is currently pursuing M.Tech Embedded systems in Audisankara college of Engineering and Technology, Gudur(Autonomous), Nellore (Dist), affiliated to JNTU Anantapur.

[2]P.Sreenivasulu He received his M.Tech in ECE from S.V UNIVERSITY,Tirupati. He has 11 years teaching experience. He Presented 4 International Conferences.Presently working as Assoc. Professor in the department of ECE, Audisankara College of Engineering and Technology,Gudur (Autonomous), Affiliated to JNTU, Anantapur.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY