**Multi-level Security embedded with Surveillance system** by Sanket Goyal,SRM University,Pranali Desai,Student,SRM University

The paper presents a model to develop a multilevel security system. The primary levels include Hex keypad, RFID & Bluetooth. To get to the secondary level which consists of the final authentication i.e. Fingerprint scanner we need to clear the priori.

The primary level security measures are connected to a controller while the fingerprint system is connected to a microprocessor with a seperate power supply.

It consists of a R305 finger print module. To access the valuable item only top officials with fingerprint access has to be scanned.

Supply voltage of3.6-6.0 VDC with 120mA max current. Use secure TTL to interface with the web.

**Steps to solving the infant biometric problem with ridge-based biometrics** by Johannes Kotzerke,Stephen Davis,Jodie McVernon,Kathy J.Horadam

The pressing biometric problem here is to find a biometric mean to identify infants cheaply, reliably and automatically.

Physical traits of infants are tiny, delicate and grow rapidly. The author focuses on novel area of friction ridge skin as the potential answer.

IRS algorithm is a global level characteristic of a ridge skin that varies across any area of ridge skin and across the body. It depends on gender ethnicity and age but distinctive enough to broadly classify individuals from a wide variety of the same population.

The Image Quality Algorithm EVA EV algorithm is based on image features extracted from captures of adult fingermarks and a ground truth.

For best results a classifier is trained on the scanner images and its parameters are chosen via the lowest error at a fixed rate for the camera and phone images.

This classifier employs various support vector machines and k-nearest neighbor algorithms.

**Small fingerprint scanners used in mobiles devices: the impact on biometric performance** by Belen Fernandez-Saavedra,Raul Sanchez-Reillo,Rodrigo Ros-Gomez,Judith Liu-Jimenez

Fingerprint scanners are being embedded in smartphones and tablets with security and usability provided by biometric authentication mechanisms. However, performance metrics cannot be extrapolated to mobile devices.

The conditions change especially at capture process due to reduced sensing areas of the scanners used. The impact of small biometric scanners in devices is studied in this paper.

The authors have examined user's interaction process for a set of 589 subjects collecting more than 180000 fingerprint images.

Three cropped databases of 10x10mm2 ,12x12mm2 and 8x8mm2 are used.

The processing algorithms used are: one is public distribution of National Institute of Standards and technology (NIST) fingerprint algorithm and the other is a commercial algorithm.

The results clearly indicate that the quality of the images get worse as the image is cropped.

The paper studies two different scenarios. First when the same scanner (included in the mobile devices) is used for enrolment and authentication.

Second one models the case of a different scanner being used for enrolment than for authentication. In this case the original full size enrolment were compared with the cropped images obtained during acquisition.

Considering the experiments, the error rates during enrolment and acquisition suffer similar effects. The results means that the impact of small sensors embedded on the mobile devices can be reduced if the enrolment is carried out externally to the mobile device, using a larger scanner.

Further it is important to note that the type of scanners and algorithms used for authentication process may also impact the performance results obtained. The commercial algorithm has better performance rates than the public algorithm.