**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

Widespread use of fingerprint scanner can be seen in tablets and smartphones coupled with security and ease of use provided by the means of biometric authentication. It is difficult to obtain the performance metrics due to the form factor of the embedded sensors in these devices. The drawback of these sensors is that it captures pixelated biometric data due to the small size of the sensor. peepee!!

The data obtained from experiments suggests that each individual generates around 300 different biometric images.

Three cropped databases of 10x10mm2 ,12x12mm2 and 8x8mm2 are used. This data was processed using 2 different algorithms, namely NIST (National Institute of Standards and Technology) and the other is a commonly used commercial algorithm. Cropping of the input images results in degradation of the image quality.

The paper studies two different scenarios, first scenario includes capturing biometrics from the scanner embedded in the device and the second from an external scanner for enrolment. Full size images and the cropped images were compared to analyze the results.

The study shows that both have similar effects. The final results suggest that embedded sensors on devices reduce the quality of the scanned image than compared to the external biometric scanners which is greater in size.

Furthermore the results depend on the type of scanners and algorithms used for enrollment and authentication. The performance of the commercial algorithm shows a higher efficiency than the public algorithm.