TO PROVIDE AN ULTIMATE SECURITY TO BANK LOCKERS USING MULTI-MODEL BIOMETRIC SYSTEMS

Brij Pal Kamboj *

Arvind Singh **

ABSTRACT

This paper improves the safety & security of bank lockers using multi-model biometric technology. Biometrics can provide a high level of security while eliminating the need to remember multiple passwords, PINs and need not carry identity proof & keys etc. Biometric is most foolproof technology which recognizes the identity of a person on the behalf of their physical biological traits such as finger prints, Iris etc. This paper is based on the multi-spectrum imaging technology which improves the image quality many times captured from the biometrics sensors. Multi-spectrum imaging technology is most efficient technology for liveness detection because it uses different images, different polarization conditions, different wavelengths, and different optical geometry. It also scans surfaces as well as sub surface features.

This system will reduce the misuse and fraud by stealing Keys, Passwords, PIN and ID proofs. If the working hand of a person is injured, then he does not capable sign properly. In such case, the person can use another finger or hand or foot finger prints which will increase convenience. However, as privacy issues & challenges are addressed. The purpose of this paper is to get information from multiple biometric sources to overcome limitations such as non-universality, noisy sensor data, large intra-user variations and susceptibility to spoof attacks that are commonly encountered in mono modal biometric systems.

Keywords: *Biometrics, Fingerprint Scanner, Hand Geometry, Multi-spectrum Imaging, FAR, FRR, PINs.*

* Department of Computer Science & Engineering, Ambala College of Engineering and Applied Research Devasthali, Ambala Cantt, Haryana.

** Head, Department of Computer Science & Engineering, Ambala College of Engineering and Applied Research Devasthali, Ambala Cantt, Haryana.

INTRODUCTION TO BIOMETRICS

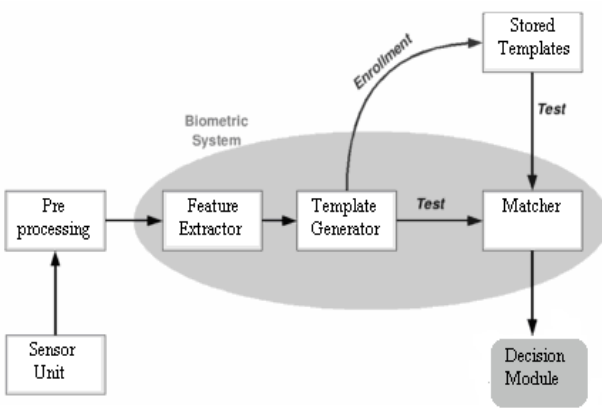
Biometrics is the science of using digital technology to identify an individual based on unique physical and biological qualities. Biometrics is also to verify a person's identity. It employs physical characteristics such as fingerprints, hand geometry, face geometry and iris patterns, and personal traits such as voice, handwriting and keystroke patterns. Biometrics can eliminate the need to remember multiple passwords and Personal Identification Numbers (PINs), or can be used to consolidate existing ones. It can be used to prevent unauthorized access in buildings, ATM machines, desktop PCs, laptop PCs, workstations, cellular telephones, wireless devices, computer files and databases, and both closed and open computer networks. Another advantage of biometrics is that you can use the same biometric everywhere, for everything. An individual's behavioral biometrics can legitimately change over time and therefore require frequent sampling. In contrast, physiological biometrics need far less sampling.

WORKING STEPS OF BIOMETRICS

- A user initially enrolls in biometric systems by providing biometric data, which is converted in to a templates.
- Templates are stored in biometric systems for the purpose of subsequent comparison.
- In order to be verified or identified after enrollment, the user provides biometric data, which is converted in to a template.
- The verification template is compared with one or more enrollment template.
- The result of a comparison between biometric templates is rendered as a score or confidence level which is compared to a threshold used for a specific technology, system, user or transaction.
- If the score exceeds the threshold, the comparison is a match otherwise comparison is not a match

FINGER PRINT SCANNER:

A generic biometric system has 4 important modules: (a) the sensor module which captures the trait in the form of raw biometric data; (b) the feature extraction module which processes the data to extract a feature set that is a compact representation of the trait; (c) the matching module which employs a classifier to compare the extracted feature set with the stored templates to generate matching scores; (d) the decision module which uses the matching scores.



(Figure 1)

HAND GEOMETRY

Hand geometry measures the physical characteristics of the hand and fingers of users. In addition to offering a good balance of performance characteristics, this biometric is one of the most established applications and is relatively easy to use. Hand geometry is ideal to use when users may access the system infrequently and may be less serious in their approach to the system. Moreover, obstructions such as dirt and cuts do not interfere with performance. Because of its ease of use and ease of integration with other systems and processes, hand geometry is an obvious first step for many biometric projects. Each person's hand is a distinct measurable characteristic. Hand geometry biometrics are comprised of a series of numeric measurements including finger length, hand thickness, palm shape, distance between the joints, skin translucency, and the shape of the knuckles. A digital map of the hand is stored, and the shape and features of the hand can be converted to an electronic security code that identifies each individual user. Hand scanning is commonly used for access control and to track time and attendance. Hand geometry systems are currently in use at various facilities including the San Francisco International Airport, the Columbian legislature, day care centers, a Los Angeles sperm bank, hospitals, and immigration facilities.

FACE RECOGNITION

The identification of a person by their facial image can be done in a number of different ways such as by capturing an image of the face in the visible spectrum using an inexpensive camera or by using the infrared patterns of facial heat emission. Facial recognition in visible light typically model key features from the central portion of a facial image. Using a wide assortment of cameras, the visible light systems extract features from the captured image(s) that do not change over time while avoiding superficial features such as facial expressions or hair. Several approaches to modeling facial images in the visible spectrum are Principal

Component Analysis, Local Feature Analysis, neural networks, elastic graph theory, and multi-resolution analysis.

Some of the challenges of facial recognition in the visual spectrum include reducing the impact of variable lighting and detecting a mask or photograph. Some facial recognition systems may require a stationary or posed user in order to capture the image, though many systems use a real-time process to detect a person's head and locate the face automatically. Major benefits of facial recognition are that it is non-intrusive, hands-free, and continuous and accepted by most users.

· No contact required.

· Commonly available sensors (cameras).

· Large amounts of existing data to allow background and/or watch list checks.

· Easy for humans to verify results.

PROBLEM FORMULATION

Bank Lockers play most important role in today life because it is considered the safest place. Storing too much jewellery and valuables in the house at this times becomes a security issue and an impediment in case of natural calamities. Bank lockers offers you, a safe, trustworthy space to store your valuables, jewellery, documents, deeds, Stock certificates and other things dear to you.

Problems in traditional bank lockers are :

1. Less security
2. Theft alarm does not exists
3. Loss of key
4. Duplicate key could be generated
5. Weapon & Arms will not be detected before placing in locker
6. if the key is stolen then impostor can access the locker.

BENEFITS OF BIOMETRIC SECURITY

Biometrics are one strong authentication technology, capable of providing higher degrees of certainty that a user is who claims to be, depending on the application. The benefit of using or deploying biometrics may be increased security, increased convenience, reduced fraud or delivery of enhanced services.

- Increased Security.
- Increased Convenience
- Increased Accountability

- Reduce Fraud & Risk
- Increase Privacy
- Increase Performance & accuracy
- Increase Reliability & robustness
- Non-repudiation & foolproof

MAJOR CHALLENGES

Major challenges that are still unresolved in terms of ensuring a secure biometric recognition system are:

(i) Noise in sensed data,

(ii) Intra class variations,

(iii) Inter class similarities,

(iv) non-universality,

(v) Interoperatability issues and spoof attack

LIVENESS DETECTION CHALLENGES:

To Check the body temperature, Blood Pressure, Heartbeat, Odor, Conductivity, Pulse Oximetry, Optical properties

- Fine movements of the fingertip surface
- Underlying texture and density of the fingerprint images
- Surface coarseness & Skin deformation
- Detection under epidermis

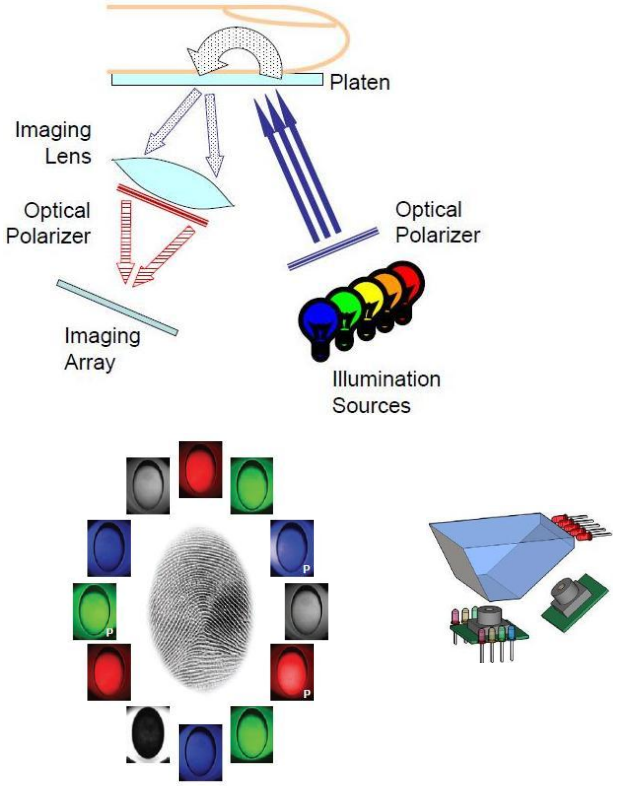
MULTISPECTRAL IMAGING TECHNOLOGY

Multispectral imaging is a sophisticated technology that was developed to overcome the fingerprint capture problems conventional imaging systems have in less-than-ideal conditions. The core problem was that conventional technologies rely on unobstructed and complete contact between the fingerprint and the sensor, a condition that is elusive in the real world.

The more effective solution was based on using multiple spectrums of light and advanced polarization techniques to extract unique fingerprint characteristics from both the surface and subsurface of the skin. The nature of human skin physiology is such that this subsurface information is both relevant to fingerprint capture and unaffected by surface wear and other environmental factors.

The basic operation of the multispectral sensor is straightforward. The sensor consists of two main components: a light source, which provides the light to illuminate the finger resting on a

platen; and an imaging system, which images this region of the platen onto a digital imaging array.

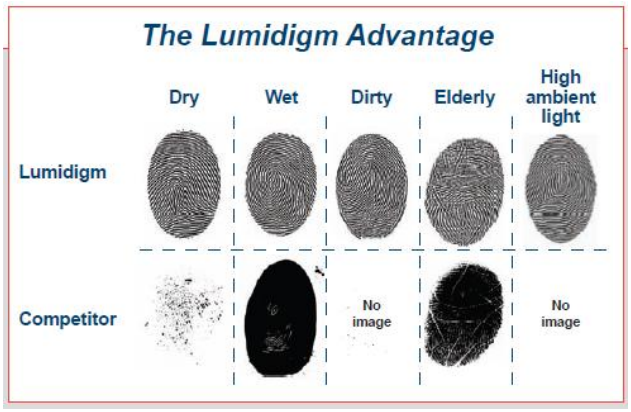


(Figure 2)

The multispectral illumination system consists of a source of multiple illumination wavelengths rather than the quasi-monochromatic illumination commonly used for TIR imaging. Linear polarizers are used in the illumination and detection portions of the sensor. The polarizers are arranged in an orthogonal configuration (a.k.a. polarizer-analyzer) to emphasize the light that penetrates the surface of the skin and undergoes multiple scattering events before emerging from the skin toward the image array.

- Different multiple images
- Different illumination wavelengths
- Different polarization conditions
- Different optical geometries
- Surface and subsurface features

Comparison between Lumidigm and Normal biometrics finger print scanner are shown in figure below.



(Figure 3)

False Acceptance Rates and False Rejection Rates

Errors will always take place, biometric devices are not perfect because they depend on human and environmental factors. Device performance can be affected by a multitude of factors including dust and dirt, background noise, temperature, lighting conditions, moisture, illness such as colds and hoarseness, cuts, and dry skin. Acceptance rates are an important factor in evaluating a biometric solution. A portion of the acceptance rate depends on the type of biometric device. The other part comes from the biometric being used. The power of a biometric system to correctly verify or identify individuals determined by the false rejection rate (FRR) and false acceptance rate (FAR).

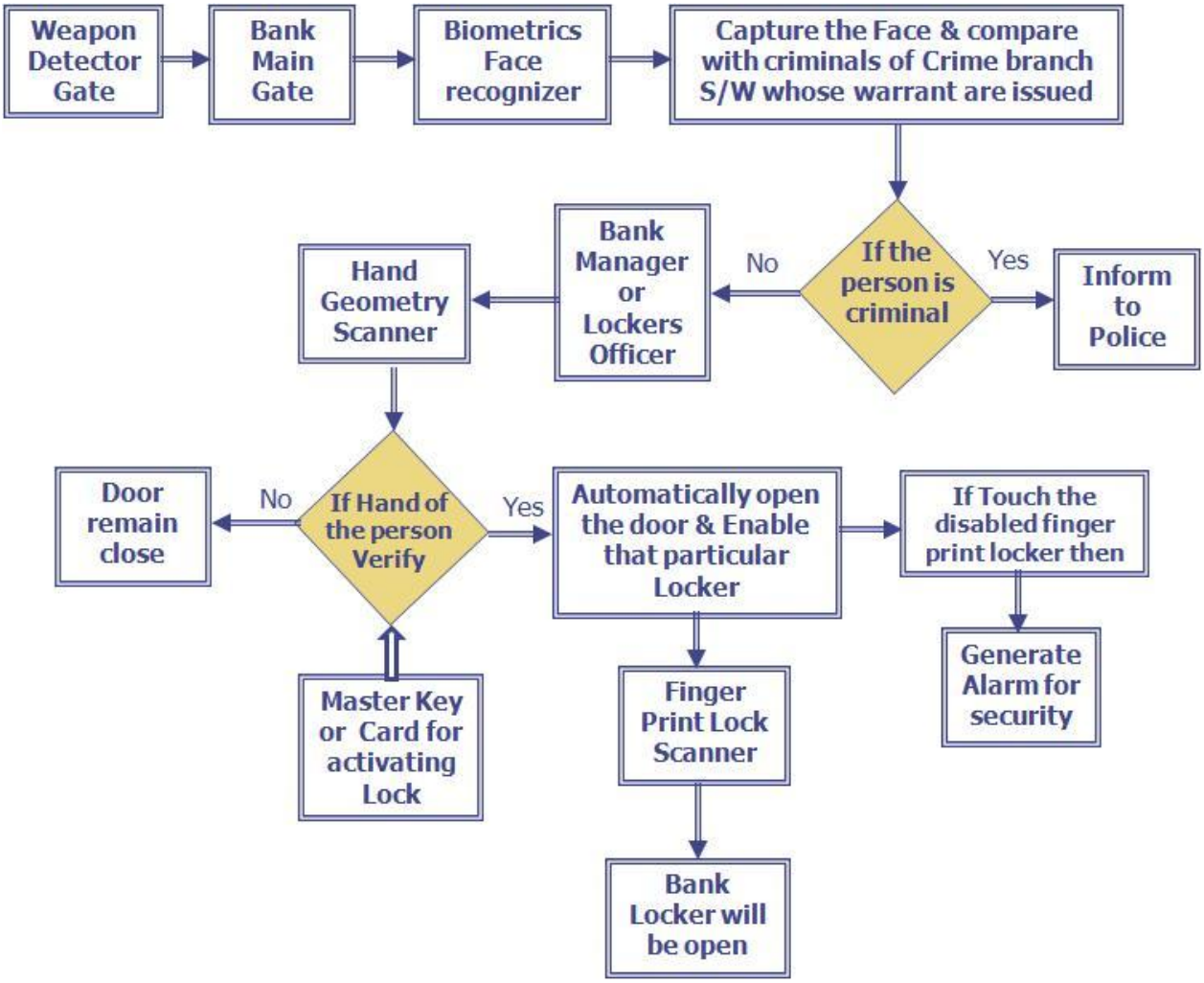
- Current biometric systems FARs ranging from 0.0001% to 0.2%, and as low as 1 in 1 billion. The industry average sits at about 1 in 10,000.
- Current biometric systems claim FRRs ranging from 0.00066% to 1.0%.
- Most biometric devices have the ability to adjust FAR and FRR thresholds to make access generally harder or easier.

PROPOSED SYSTEM :

Our Proposed system is to provide an ultimate security to banks & their lockers using multiple biometrics system. This system consists of high quality sensors & algorithms. A Weapon detector is used before the bank for checking the

weapons. If a person carrying a weapon will be not allowed in the bank otherwise he can enter in the bank. After then face is recognized at different angles by the face recognition biometrics and face is matched with the criminals of crime branch software. The Criminals whose arrest warrant are issued and face recognition biometric is directly connected to the police crime branch. The software matches his face with the criminals. If the face is matched, then send message to the police control room.

If the person is not a criminal then he can be able to access their bank locker. For that he should put his hand on hand geometry scanner which is based on multi-spectrum technology and is able to work in all conditions/environment like dry, wet, dirty, elderly, high ambient light etc. Lumidigm technology is the best technology in the world which capture very high quality & clear input image in all conditions. If the hand of the customer is matched with the template stored in the database then the door of the locker will be automatically open for a few second so that only one person will enter in the lockers area and also enable the finger print lock of that particular person.



The biometric finger print locker is based on verification technology, for that a mifare smart card is issued to the customer. The template & finger image of the customer is stored in the mifare card which provides ultimate against fake, spoof or Trojan hoarse attacks on template database. The finger print lock verifies the identity of the person & open the lockers. If a person open the another locker then alarm will generate.

The biometrics industry is introducing new and more secure ways of exchanging information, services, money, and goods through automated transactions. Many experts predict the science and technology of biometrics will continue to experience explosive growth. Biometrics could also be used to restrict access to dangerous items such as firearms and automobiles. There is the potential for identification and information assurance through smart cards that could accommodate a number of applications such as medical records, financial accounts.

APPLICATIONS

- Prevent unauthorized access to ATMs, Cellular phones, Smart cards, Desktop PCs, Workstations, Computer & network security.
- Criminal identification, prison security, Courts
- Electronic commerce, Electronic banking & Financial services
- In automobiles biometrics can replace keys with keyless entry devices.
- Airport security, voter cards, Healthcare, DNA Matching, Time and Attendance

CONCLUSION

Biometric is an emerging area with many opportunities for growth. Possibly in the near future, you need not to have remembered PINs and passwords and keys in your bags or pockets will be things of the past. There is no security system that is completely out of spoofing. Every system is subject to breakable. A single finger prints biometric can be easily forged and is not secured/reliable. So we proposed multiple biometrics & multi-spectrum technology to provide high performance, throughput, reliability, security and robustness. This system can be work in any environment condition (water proof, dry, wet, dirty, elderly, high ambient light, spray or cream on fingers etc.).

. Multiple biometric systems are those that utilize more than one physiological or behavioral characteristic for enrollment, verification, or identification. In applications such as border entry/exit, access control, civil identification, and network security, multiple biometric systems are looked to as a means of (a) reducing false acceptance and false rejection, (b) providing a secondary means of enrollment, verification, and identification if sufficient data cannot be acquired from a given biometric sample, and (c) combating attempts to spoof biometric systems through non-live data sources such as fake fingers.

FUTURE SCOPE

Multi-biometrics Model is more reliable than the mono-model or multi-model biometrics due to fusion of matching score and which gives more accurate result. If one of the trait does not sensed/match properly then multi-biometric scanner gives the result on the behalf of

combination of all biometrics sensors. Image sensing quality can be improved by using 3D image scanning & multi-spectrum technology. Proposed system performance can also be improved by using Hybrid biometric technology.

REFERENCES :

1. Yongchang Wang, Qi Hao, "Data Acquisition and Quality Analysis of 3-Dimensional Fingerprints" , Member, IEEE, Abhishika Fatehpuria, Jul. 2010
2. Robert K. Rowe, Ph.D. CTO & VP, "Comparative Image Quality of Multispectral Fingerprint Images", March 8, 2006
3. R. Cappelli, D. Maio, D. Maltoni, J. L. Wayman, and A. K. Jain, "Performance evaluation of fingerprint verification systems," IEEE Trans. Pattern Anal. Mach. Intell., vol. 28, no. 1, pp. 3–18, Jan. 2006.
4. R. Rowe, S. Corcoran, K. Nixon, and R. Ostrom, "Multi-spectral imaging for biometrics," Proc. SPIE Conf. Spectral Imaging: Instrumentation, Application, and Analysis, pp. 90–99, Mar 2005.
5. E. Tabassi, C. L. Wilson, and C. I. Watson, "Fingerprint image quality," NIST, Aug. 2004
6. Mojtaba Sepasian, Cristinel Mares, Wamadeva Balachandran, "Liveness and Spoofing in Fingerprint Identification: Issues and Challenges", School Of Engineering & Design Brunel University, Uxbridge, Moddlesex, Ub8 3 Ph, UK, 2002