International Journal Of Advance Research, Ideas And Innovations In Technology

ISSN: 2454-132X
Impact factor: 4.295
(Volume 3, Issue 6)
Available online at www.ijariit.com

Bio Metrics in Secure E-transaction

Siddhi Raviraj Awadhut
Kolhapur Institute of Technology's College of Engineering, Kolhapur,
Maharashtra
siddhi.awadhut2596@gmail.com

***Abstract:* Information security is concerned with the assurance of confidentially, integrity and availability of information in all forms. This is the ancient Greek word: bios = "life" and metron = "measure." In the present day world, online shopping using WAP enabled mobile phone has widely come into use. Credit cards serve as the currency during e-business and e-Shopping. As the Hacking or Spoofing or the Misuse of the credit card is continuously increasing even you are using a secure network. Also, some Spam software is sent to your system or device through the internet that helps spammers to get the desires relevant information about your credit card and financial data. To solve these problems or get out of these insecurities the Bio-metric System that provides the secure E-transaction by improving the prevention of data spoofing. So in this paper, we have proposed a multi-biometric model (integrating voice, fingerprint and facial scanning) that can be embedded in a mobile phone, this making e-transactions more secure.**

***Keywords:* Multi-biometric, Identification, E-commerce, e-transaction.**

1. INTRODUCTION

This paper provides a broad overview of the subject of biometrics, their usage, how performance is measured, the typical construction of systems and practical implementation issues. A basic understanding of computer networks is requisite in order to understand the principles of network security. A network has been defined as any set of interlinking lines resembling a net, a network of roads an interconnected system, a network of alliances. This definition suits our purpose well. A computer network is simply a system of interconnected computers.

Moving on to the definition of biometrics, a biometric system is a recognition system, which makes a personal identification by determining the authenticity of a specific physiological or behavioral characteristic possessed by the user. This method of identification is preferred over traditional methods involving passwords and PIN numbers for various reasons. Bioinformatics is a new engineering field served by traditional engineering curricula. Bioinformatics can be defined in several ways, but the emphasis is always on the use of computer and statistical methods to understand biological data, such as the voluminous data produced by high-throughput biological experimentation including gene sequencing and gene chips. Bioinformatics, the application of computational techniques to analyze the information associated with bimolecular on a large-scale, has now firmly established itself as a discipline in molecular biology and encompasses a wide range of subject areas from structural biology, genomics to gene expression studies. Bioinformatics is an integration of mathematical, statistical and computer methods to analyze biological, biochemical and biophysical data.

Biometric is a physical or biological attribute that can be measured. Biometric identification accepts or rejects the person's identity, based on his/her physiological or behavior characteristics. A biometric identification system is essentially a pattern –recognition system that recognized a person based on a feature derived from specific physiological or behavior characteristics the person possessed for authentication or identification purposes.

Characteristics of biometric:
1. UNIVERSALITY
2. UNIQUENESS
3. PERMANENCE
4. COLLECTABILITY
5. ACCEPTABILITY
6. PERFORMANCE

Fingerprint scanners can be integrated here.
Video camera assits in acquiring face images.
Built-in microphone helps in acquiring voice samples

2. MULTIBIOMETRICS

A multi-biometrics system is obtained by the integration of multiple individual biometrics models. Numbers of models integrating hand geometry, keystroke dynamics, face and iris recognition system have flooded the markets in recent years. Here we present a multimodal system that can be embedded in a mobile phone, which integrates fingerprint, voice and facial scanning. It shuts down the problem of high false rejection Rate of facial scanners, eliminates the fooling of fingerprint scanners and overshadows the disadvantage of voice recognition models.

3. LITERATURE REVIEW

- European Explorer Joao de Barros recorded the first known example of fingerprinting in China during the 14th century.
- 1980:- Alphonse Bertillon studied body mechanics and measurements to help in identifying criminals.
- Karl Pearson, an applied mathematician studied biometric research early in the 20th century at University college of London.
- In the 1960 and 1970, signature biometric, authentication procedures were developed.

Today, biometric lows and regulations are in process and biometric industry standard is being tested.
It divided into two parts,

1) Fingerprint
   Palmprint
   Hand veins
   Face
   Iris
   Retina
   DNA
2) Gait
   Voice
   Signature
   Keystrokes

TWO USAGE MODES FOR BIOMETRICS

Mode 1: Access Control:
- Only this exact person is allowed in
- Primary identifier uniquely identifies someone
  – Personal ID (public value)
  – PIN/password (private value)
- Biometric backs up the primary ID
  – 1:1-match biometric check weeds out the majority of impersonators
  – Match only this one identified person and no-one else

Mode 2: Identification
- Inexact match used to find things – Find one of 3 million people (DHS terrorist list) from a population of 6 billion
- Real-life analogy: “Was this the person who robbed you” vs. “Find the person who robbed you in these 25 shelves of books of mug shots”
- The answer to all your terrorism problems.

4. NEED FOR BIOMETRICS INMOBILE PHONES

Mobile phones have ceased to be the exclusive status of the high class and, today has become an indispensable electronic gadget in the life of many. The main reason for their higher market penetrations in recent days is their incredible array of functions at an affordable cost. Apart from setting remainders and sending e-mails, they are also used in

•e-business
•SMS messaging
•Chatting
•Telemedicine and teleconferencing

Thus, these phones with wide roaming facility prove to be a really versatile device

Nowadays, shopping through the internet has become very popular and surely, a WAP enabled mobile phone provides the facilities to consumers to shop online. Credit cards continue to be an efficient tool for online money transactions. But, on the other hand, credit card’s number can be stolen on its way to its destination and can be misused by hackers. Thus, e-Business through a mobile phone becomes insecure.

Also, a report in www.download.com stated that much anti-fraud Software, like those provided by Artic Soft and ISC, created a back door entry and were largely involved in data spoofing. In addition to this, many user and companies were prone to the attack of many viruses and Trojan horses.

With so much of problems faced, the service provides turned their attention towards biometrics to prevent data spoofing and to provide secure e-Transactions. Though security applications that verify a person's identity based on their physical attributes, such as fingerprint readers or iris scanners, have been in use for some time, biometric security has only recently started to appear in mobile phones, PDAs and notebook computers where the need for miniaturization represents a technological challenge. So far biometric data has been used to tie the device to a person to prevent it from being used illegitimately if lost or stolen. But the IST project Secure Phone is taking a new approach, employing physical attributes to enable the user to digitally sign audio, text or image files, providing proof of their origin and authenticity.

Although existing communications infrastructure based on the GSM, GPRS and UMTS mobile systems provide a secure means of communication, it lacks any robust method of user identification. Text, audio and image file scan be sent by anyone to anyone with no authentication and there are no guarantees the person you are talking to in a phone conversation, if you've never met them before, is really who they claim to be.

The upshot is that data exchanged over mobile devices are of limited use for legally binding transactions even though mobile devices, given their ubiquity, would be a prime candidate for carrying out e-commerce (or m-commerce), managing business processes such as signing contracts or even in securing the exchange of data in e-healthcare and e-government systems. A digitally signed and authenticated voice recording during a telephone conversation would, for example, give the speaker's words legal value."

The aim is to enable users to exchange information that can't be disputed afterward. That could be a voice recording that is authenticated to eliminate any doubt about who the speaker is, what they actually said and prove that it has not been manipulated," Ricci explains."To achieve that it is necessary to digitally sign the data and to ensure that only the legitimate user can perform the signing."

The system developed by the Secure Phone project partners consists of two main elements. The first, an authentication module, uses biometric security applications to verify the user's identity. That, in turn, gives them access to the second module which digitally signs the data using a Public Key Infrastructure (PKI).

The system, which is designed primarily for PDA-phones but could also be used in new generation smart phones and Wi-Fi-enabled PDAs, offers three methods of biometric identification. One employs the digital cameras that have become commonplace in mobile devices along with a face recognition application to identify the user based on their facial features. Another uses voice recognition software – also detecting any asynchrony between speech and lip movements - and the third verify the handwritten signature of the user on the device's touch screen. The three methods are used in combination to enhance the overall levels of security and reliability, and most importantly they require no hardware additions to mobile devices.

FACE RECOGNITION

Facial recognition is considered to be one of the most tedious among all scans. Further, difficulty in acquisition of face and cost of equipment make it more complex. However, some WAP enabled phones like CX 400K and LG-SD1000manufactured by LG electronics, have built in camera that can acquire images and can be transmitted over the internet. This it is sent to the credit card company to verify the face received matches with the face in their database. If it matches, the goods are sent, else the order is rejected. Face recognition uses mainly the following techniques:

•Facial geometry uses geometrical characteristics of the face. May use several cameras to get better accuracy (2D, 3D...)

•Skin pattern recognition: (Visual SkinPrint)
•Facial thermo gram: uses an infrared camera to map the face temperatures
•Smile: recognition of the wrinkle changes when smiling

Facial Geometry: Many different methods based on geometrical characteristics of the face have been developed such as "local feature analysis", "Eigen face or Principal Component Analysis",

Skin Pattern Recognition: Visual Skin Print relies on standard hardware -most web-cams and higher resolution mass-market video cameras, connected to a PC, will work. Visual Skin Print™ is based on a simple yet powerful idea: using the details of the skin for authentication

Facial Thermo Gram: Facial thermo gram requires an (expensive) infrared camera to detect the facial heat patterns that are unique to every human being. Technology Recognition Systems worked on that subject in 1996-1999. Now disappeared. Face Recognition in Hyper spectral Images" is an article describing a variant using several wavelengths.

Smile Recognition: The Stony Brook university system relies on probing the characteristic pattern of muscles beneath the skin of the face.

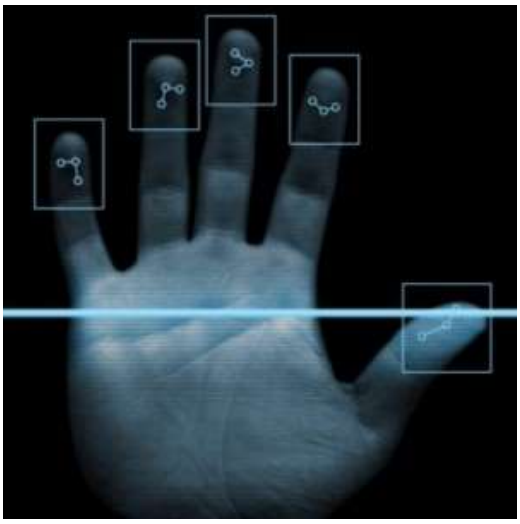
Guan takes two snaps of a person in quick succession, asking subjects to smile for the camera. He then uses a computer to analyze how the skin around the subject's mouth moves between the two images. The software does this by tracking changes in the position of tiny wrinkles in the skin, each just a fraction of a millimeter wide.

The data is used to produce an image of the face overlaid with tiny arrows that indicate how different areas of skin move during a smile. This movement is controlled by the pattern of muscles under the skin and is not affected by the presence of make-up or the size of the subject's smile. The system is sensitive enough to produce such a map from muscle twitches even when people are trying to keep their expression unchanged

Dynamic Facial Features: In A Dynamic Approach to Face Recognition paper, a new method for face recognition is proposed, which is based on dynamic instead of classification accuracy of 90% is achieved. For the four-class problem (arch and tented arch combined into one class), we are able to achieve classification accuracy of 94.8%. By incorporating a reject option, the classification accuracy can be increased to 96% for the five-class classification and to 97.8% for the four-class classification when 30.8% of the images are rejected.

Fingerprint Image Enhancement

A critical step in automatic fingerprint matching is to automatically and reliably extract minutiae from the input fingerprint images. However, the performance of a minutiae extraction algorithm relies heavily on the quality of the input fingerprint images. In order to ensure that the performance of an automatic fingerprint identification/verification system will be robust with respect to the quality of the fingerprint images, it is essential to incorporate a fingerprint enhancement algorithm in the minutiae extraction module.



We have developed a fast fingerprint enhancement algorithm, which can adaptively improve the clarity of ridge and furrow structures of input fingerprint images based on the estimated local ridge orientation and frequency. We have evaluated the performance of the image enhancement algorithm using the goodness index of the extracted minutiae and the accuracy of an online fingerprint verification system. Experimental results show that incorporating the enhancement algorithms improves both the goodness Index and the verification accuracy.

PRACTICAL PROBLEMS WITH BIOMETRICS

Biometric systems have never had to withstand serious attack:

• Smart cards took 15 years of criminals walking all over them before vendors started taking security seriously.

Fingerprint scanners work poorly with the elderly, manual workers, children:

• Children haven't developed strong fingerprints yet.

• Manual workers and the elderly don't have strong fingerprints left.

• German passport enrolment system ran into problems with people as "old" as 40 or 50.– 10% of senior citizens can't be reliably enrolled.

Established wisdom: 3-4% of the population (goats) have unstable biometric traits that can't be identified by sensors

• In practice, it's often much, much higher• Up to 50% reject rate, see later slides

Fingerprint readers have problems with outdoor use

Example: in winter cold

5. ATTACK

Train the system to accept less and less reliable images

• Has happened (inadvertently) in real-world deployments as sensors were subject to wear and tear.

• System would accept anything (elbow, nose) as a valid print

People forget which finger they enrolled with and try each one in turn

• Alternatively, a failure to verify the chosen print would lead to them trying all other fingers just in case

• (Happens to a lesser extent with passwords as well)

FARs for mass-market fingerprint readers are already wound sky-high to avoid consumer acceptance problems:

• Need to wind the FAR up to the point where FRR = 0.The readers will have a fairly broad tolerance on the basis that products that stop people using their own cars, computers or whatever because their fingers are a bit sweaty won't turn out to be very popular.

UK passport service required a biometric-compatible photo instead of the standard one:

• 80,000 of the first set of photos (600K) were rejected for not meeting the requirements

• Computer-based systems are vastly easier to confuse than humans.

UK Passport Service Enrolment Trial:

•Enrolled 9,000 travelers to evaluate the enrolment experience.

•10% of users couldn't enroll using the iris-recognition system

•30% of able bodied users couldn't have their facial biometrics verified

50% of disabled users couldn't have their facial biometrics verified (!!)

• Particularly problematic due to laws like ADA that forbid discrimination against the disabled.

"Fix" was probably to wind the sensitivity down so that almost anything would pass

• This is the universal solution for any failures in systems that employ approximate matching

German passport enrolment requirements stipulate the use of the least unreliable trait sample if no reliable one can be obtained

There doesn't seem to be any minimum acceptable quality measure for trait sampling• If all else fails, click the "No Hand" button another fingerprint software If the fingerprint isn't readable, which isn't uncommon, the passport records "No Hand"["Keine Hand"]. There is no provision for "Fingerprint not readable" This is an unfortunate 'solution'

Verification time was a full minute across a variety of systems:

• Current verification time for intra-EU travel is < 5s• Order-of-magnitude slowdown for traveler verification

Enrolment has similar problems:

• German biometric enrolment system was advertised as taking 2½ minutes, in practice takes > 10 minutes

One of the reasons why pre-biometric passports had a10-year life was that that was about the maximum throughput of the processing system

• Now, vastly more complex passports have to be rolled over in half the time

Failure rates were significantly higher for people with darker skin and/or eyes:

• Dark skin/dark eyes absorb more light

• Features don't stand out as much

These are all features of the ethnic group that these systems are targeting:

• The targets are the ones least likely to be correctly processed!

6. CONCLUSION

Thus, this mobile multi-biometrics can be embedded in the mobile phone. The phone is cost effective since no special hardware in required and is highly secured. Thus, this mobile phone becomes a reality will provide more e-Business and e-Transactions.

REFERENCES

1) http://ijettcs.org/Volume2Issue2/IJETTCS-2013-04-25-181.pdf
2) http://www.techrepublic.com/resource-library/whitepapers/biometrics-in-secure-e-transaction/
3) https://www.scribd.com/doc/21522715/Bio-Metrics-in-Secure-E-transaction
4) https://volumeoftech.wordpress.com/2013/06/07/secure-e-transaction-through-bio-metric-system/
5) http://1000projects.org/biometric-in-secure-e-transaction-computer-science-seminar-report.html
6) http://www.seminarsonly.com/computer%20science/BIOMETRICS-in-SECURE-E-transactions.php
7) http://www.slideshare.net/Pathik504/slideshow-on-biometrics
8) https://www.youtube.com/watch?v=cisw-g7A_Gk
9) http://www.ijarcsms.com/docs/paper/volume3/issue4/V3I4-0131.pdf