International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)
Web Site: www.ijettcs.org Email: editor@ijettcs.org, editorijettcs@gmail.com
Volume 2, Issue 1, January – February 2013 ISSN 2278-6856

Recent Advances in Emerging Biometrics

C. Sesha Ratnam[1], C.Raja[2], G.Ramesh[3], N.V.Vinodkumar[4], N.Jyothsna[5]

[1, 2,3,4,5] SREE RAMA ENGINEERING COLLEGE, TIRUPATHI.

Abstract - ***Biometrics or (biometric authentication) refers to the identification of humans by their characteristics or traits. Biometrics is used in computer science as a form of identification and access control. It is also used to identify individuals in groups that are under surveillance Biometric identifiers are the distinctive, measurable characteristics used to label and describe individuals. Biometric identifiers are often categorized as physiological versus behavioral characteristics. A physiological biometric would identify by one's voice, DNA, hand print. Behavioral biometrics are related to the behavior of a person, typing rhythm, gait, and voice. Some researchers have coined the term behaviometrics to describe the latter class of biometrics.***

Keywords - Biometrics, Security, Protection, Development, Emerging Techniques

1. INTRODUCTION

History of Biometrics

Biometrics has been around since about 29,000 BC when cavemen would sign their drawings with handprints. In 500 BC, Babylonian business transactions were signed in clay tablets with fingerprints. The earliest cataloging of fingerprints dates back to 1891 when Juan Vucetich started a collection of fingerprints of criminals in Argentina.

How does Biometric Technology Works?

There are many different types of biometric systems, including facial recognition, hand geometry, iris recognition, retina recognition, and speaker recognition. Each of these systems involves similar processes such as Enrollment, Verification, Identification and Screening.

Enrollment

In the enrollment step the user needs to prove his or her identity, furnishes the identification document. The biometric characteristics of the concerned user are linked to the identity specified in the identification document. This ensures that the reference template is linked to the right identity. This is a key step which determines the integrity of the system.

After the enrollment process the user provides any or the required biometric samples (like Fingerprint, Iris Pattern or Hand Geometry) to an acquisition device, usually a biometric sensor. Here the system acts operates in the data acquisition mode, where the device or scanner is used to populate the database. The acquired data is encrypted using any secure algorithm and stored in the central/remote database. The storage can also be made in the memory chips or cards.

The user may need to enroll and present the samples multiple times as small changes in positioning, distance, pressure, environment, and other factors influence the generation of a template, and it is expected to be unique. Therefore, a person may need to present biometric data several times in order to enroll. The reference template may then represent an amalgam of the captured data, or several enrollment templates may be stored. In addition, because biometric features can change over time, people may have to reenroll to update their reference template.

Verification

The verification step objective is to confirm that a person is in fact who he or she claims to be. Here the real time input is compared with the stored template to determine whether or not there is a match. Verification is always considered to be "one-to-one" matching. Out of the millions of reference templates, only one needs to be compared to the sample template. The output of the verification systems is a match /no match decision in less than a second. In case of using multimodal or liveness detection priorities are set and also the system acts as a toll gate.

Identification

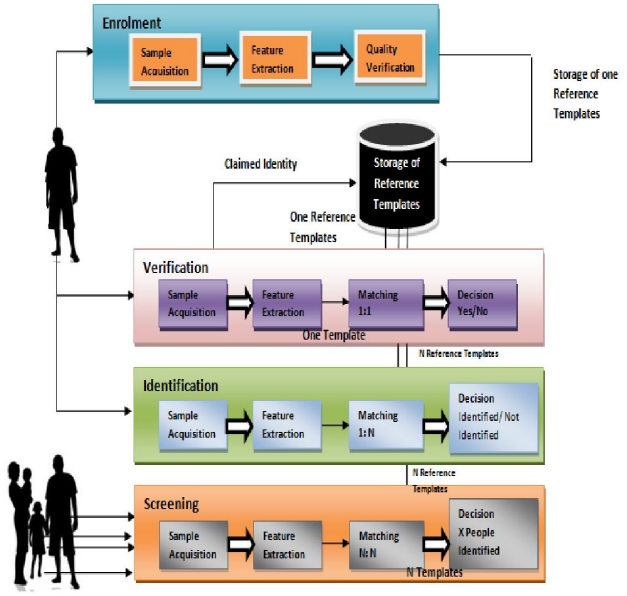
The identification systems are considered to perform "one-to-many" matching, where the sample template is compared against the stored reference templates of all individuals enrolled in the system. There are two types of identification systems – Positive and Negative.

Positive identification systems: Determine whether a user seeking access can be identified as having been enrolled in the system.

Negative identification systems: Ensures that a user's biometric information is not present in a database. For example, a negative identification system may be designed to identify people on a watch list.

Screening

It is a step where the input templates are collected from many users and the process of comparing is done with all the Enrolled reference templates. It is considered to be "many to many" matching. The outcome of this step is a decision where it notifies X people out of the N numbers are identifies.



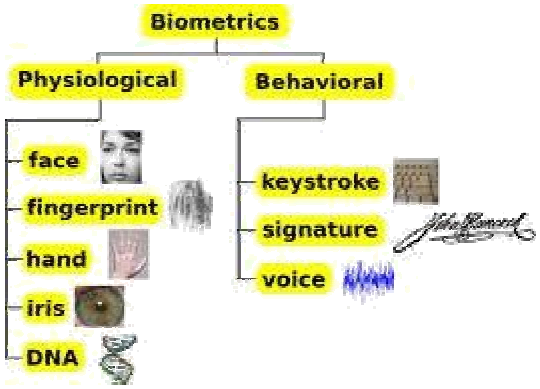
Countries applying biometrics

Countries using biometrics include: Australia, Brazil, Canada, Gambia, Germany, India, Iraq, Israel, Italy, Netherlands, New Zealand, Norway, United Kingdom, and United States.

Danger to owners of secured items

When thieves cannot get access to secure properties, there is a chance that the thieves will stalk and assault the property owner to gain access. If the item is secured with a biometric device, the damage to the owner could be irreversible, and potentially cost more than the secured property. For example, in 2005, Malaysian car thieves cut off the finger of a Mercedes-Benz S-Class owner when attempting to steal the car.

2. BIOMETRIC RECOGNITION ALREADY USED OR PROPOSED



For many years, biometric identifiers like fingerprints and DNA have been the most accurate. Unfortunately, fingerprints can be altered and DNA can be difficult to collect and slow to process. Even retina and iris scanners can be rendered inaccurate by medical changes like astigmatism. Is there anything else that works better? Scientists and researchers claim there are two possibilities – brain waves and heart rhythms.

Recognition by the way someone walk (their gait), the shape of their ears, the rhythm they make when they tap and the involuntary response of ears to sounds all have the potential to raise the stock of biometric techniques. According to Professor Mark Nixon, of the Image Speech and Recognition Research Group at the University of Southampton, each has unique advantages which make them worth exploring.

Recognition by ear has already been used in criminal cases and has the advantage that the ear does not change shape with age. Smiling doesn't confuse ear recognition but hair might. Newer techniques such as the otoaustic effect (the response of the ear to sound) has the advantage that it is non-invasive and yet voluntary. However practical implementation is still some way off.

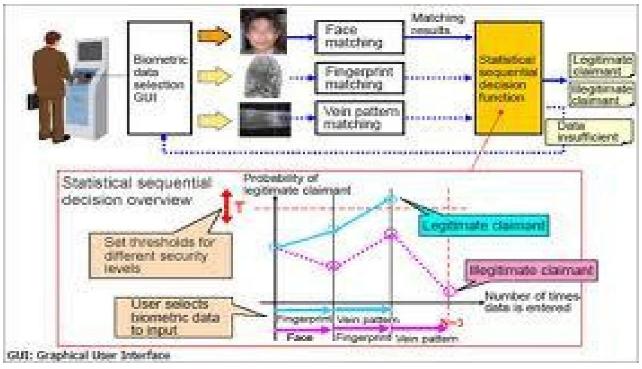
One of the technologies, palm vein verification, was implemented in the banking industry in Japan because users of traditional fingerprint scanners felt that these were unhygienic.

Facial recognition has also been taking off due to the unobtrusive nature of its process, which does not require contact with the user.

Advantage of finger vein recognition

The benefits of vein recognition in particular are significant - and the system is already proving highly effective in the banking sector in Japan. Palm vein technology was developed by Fujitsu and Finger Vein technology by Hitachi to help combat the increasing incidence of financial fraud and forgery, problems which have plagued many financial institutions in Japan for a number of years - at great cost to the country's economy.

One of the main benefits of vein readers is that, unlike fingerprints which change during childhood, the palm and finger vein pattern is established in the womb and is constant throughout a person's life. The scanners operate on near-infrared light to read the palm vein pattern, which lies underneath the epidermis and so can't be distorted by damage to the skin, age or the wearing of gloves. Vein readers also benefit from being non-contact - a particular advantage in environments such as health care, where hygiene may be an issue.



Several of Japan's major banks have been using palm and finger vein recognition at cash points, rather than PINs, for almost 3 years now and are confirming extraordinarily high standards of accuracy, with false rejection rates of 0.01% and false acceptance rates of less than 0.00008%. TDSi is working closely with both Fujitsu and Hitachi to incorporate this sensing technology into readers that can be deployed in physical access security applications. The first of these readers, PalmGarde (utilizing Fujitsu's Pam Secure sensor), was made available for sale in July 2007.

Vein readers offer a highly attractive combination of accuracy and reliable performance

Eye recognition development

In terms of eye recognition, developments are being seen in both iris and retina scanning. Iris recognition offers a highly effective and reliable security option; each individual iris has around 260 unique characteristics and individuals' irises tend not to experience great changes over time. Furthermore, recognition is only very marginally affected by the angle of image capture and ambient light conditions and the technology is equally effective through glasses, contact lenses and goggles.

Performance can be affected by certain eye problems, such as cataracts, and if the user is wearing colored contact lenses or sunglasses - but these potential drawbacks can all be overcome with a degree of cooperation from the user. TDSi has successfully integrated the Panasonic Iris reader system into our eXguard Pro software platform and have several installations ranging from banks, to pharmaceutical companies to construction sites deploying this solution to augment their physical access security regimes and processes.

Retinal scanning takes the technology a step further and examines the characteristics of patterns of blood vessels at the back of the eye. Although highly effective and incredibly accurate, this is a particularly time intensive process and is seen by users to be quite intrusive - each individual must look directly into a reader, where a low intensity light is directed through the pupil and performs a 360-degree retinal scan.

Currently, both iris and retina recognition equipment are rather cost-prohibitive, although strides are being made to bring down the unit cost. But, given the speed and user issues associated with retina scanning, it is likely that it will only be used in the most high-security situations in the short to medium term, with iris recognition being the more dominant technology - potentially being used in conjunction with facial recognition systems.

3. EXPANDING BIOMETRIC SYSTEM

Imaginable today:

1. Body shape recognition.

2. Investigation of internal structure of body parts and its living structures.

3. Analysis of other electrical and magnetic fields, created by man's body or of its reactions to such fields.

4. Analysis of face and head vibrations during speaking.

Recent advances in emerging biometrics

In recent times, biometrics based on brain (electroencephalogram) and heart (electrocardiogram) signals have emerged. The research group at University of Wolverhampton lead by Ramaswamy Palaniappan has shown that people have certain distinct brain and heart patterns that are specific for each individual. The advantage of such 'futuristic' technology is that it is more fraud resistant compared to conventional biometrics like fingerprints. However, such technology is generally more cumbersome and still has issues such as lower accuracy and poor reproducibility over time

Recent advances in sensor technology and wide spread use of various electronics (computers, PDA, mobile phones etc.) provide new opportunities for capturing and analyses of novel physiological and behavioral traits of human beings for biometric authentication. This paper presents an overview of several such types of human characteristics that have been proposed as alternatives to traditional types of biometrics. We refer to these characteristics as emerging biometrics. We survey various types of emerging modalities and techniques, and discuss their pros and cons. Emerging biometrics faces several limitations and challenges which include subject population coverage (focusing mostly on adults); unavailability of benchmark databases; little research with respect to vulnerability/robustness against attacks; and some privacy concerns they may arise. In addition, recognition performance of emerging modalities is generally less accurate compared to the traditional biometrics. Despite all of these emerging biometrics posses their own benefits and advantages compared to traditional biometrics which makes them still attractive

for research. First of all, emerging biometrics can always serve as a complementary source for identity information; they can be suitable in applications where traditional biometrics are difficult or impossible to adapt such as continuous or periodic re-verification of the user's identity etc.

Whenever security technology advances, criminals eventually adapt and improve their skills, too. Even when it seems there is a foolproof system in place, there is almost always someone who will figure out how to circumvent it, whether it's to steal something or to impersonate someone else. The government has always been a lead innovator in access security and biometrics, attempting to come up with ways of authenticating a person's identity with complete accuracy and little-to-no chance for error.

Unique Internal Identifiers

No two people have the same fingerprints or patterns on their irises and retinas. Identifiers like these, however, are external and can be manipulated, or there are some circumstances under which they can change. Because of this, they are not foolproof methods of identifying someone. Brain waves and heart rhythms are internal identifiers that are much more difficult or impossible to change. Heart rhythms are slightly more difficult because they can change with the onset of heart problems, and they may also change when a person is under stress. In general, however, your heart rhythm is unique to you. Your brain waves are essentially foolproof, because they simply cannot be changed.

4. ENHANCED SECURITY AND PROTECTION

Because brain waves and heart rhythms are basically unalterable, they are technically the most secure indicators for access control. In order to test someone's brain waves, some electrodes are simply hooked to their head and an EEG (electroencephalogram) is performed. For heart waves, electrodes are attached to the chest and an ECG (electrocardiogram) is performed. The results would need to be recorded one time, and afterward any time a person requested access, they would be hooked up to the electrodes again for a quick, painless evaluation to see if the results match. While it could be possible that an individual's waves or rhythms could change in very rare circumstances, it is, more importantly, simply impossible for someone to impersonate someone else using these identifiers.

5. THE FUTURE OF FOOLPROOF BIOMETRICS

As more research is being done on brain waves and heart rhythms as biometric data, what will it mean for the future of access control technology? The government and other agencies already use retina or iris scanners. Will they soon begin using EEGs and ECGs? It's possible. There has been lots of talk about retina or iris scanners on ATMs and other consumer devices or in other public places. While these may be the fastest and easiest methods, they are more expensive to test than brain waves and heart rhythms, and the results are not quite as guaranteed. As technology in general advances, don't be surprised if more advanced biometrics begins being used in a more widespread manner.

Brain of each human being is completely unique. Its structure is highly influenced not only by our DNA but also by everything we experience in our life. You can find people even with the same DNA – but life history is something that cannot be duplicated.

So brain activity is unique biometric every person has. And such biometrics are used in access control systems when security is needed. Simply, you can use your biometric as a password to gain access to resources protected from everyone except you. And brain activity has a lot of advantages over other biometrics traditionally used in access control systems (such as fingerprints). Here are the most important ones:

Brain activity is secure. In case of fingerprints, for example, we leave biometric in every place we touch with our hands, so everyone who needs to attack the system can collect & replicate it. Brain, in contrary, is safely hidden inside a skull.

Brain activity is changeable. You cannot influence other biometrics – your iris pattern, DNA, heart beats, fingerprints – are determined by nature and there is no easy way to modify them. If system based on these biometrics is compromised once, it is compromised forever. Brain activity, conversely, can be easily changed just by simple thought.

Brain activity can be captured by different methods. Most of them are quite expensive and require a lot of time and effort, and hence cannot be used in access control systems. EEG method is most extensively studied for person identification. Traditional devices for EEG recording are bulky & expensive too, but technology moves forward, and cheaper & more convenient devices are now developed.

EEG as potential biometric for person identification has been studied since 1998. First papers were published by Marios S. Poulos. References to these works can be found on Poulos' website. He recorded background EEG – i.e. EEG recorded while people were resting – and used it to identify these people.

6. MARKET FACTS AND TRENDS

1. Morgan Keegan Survey

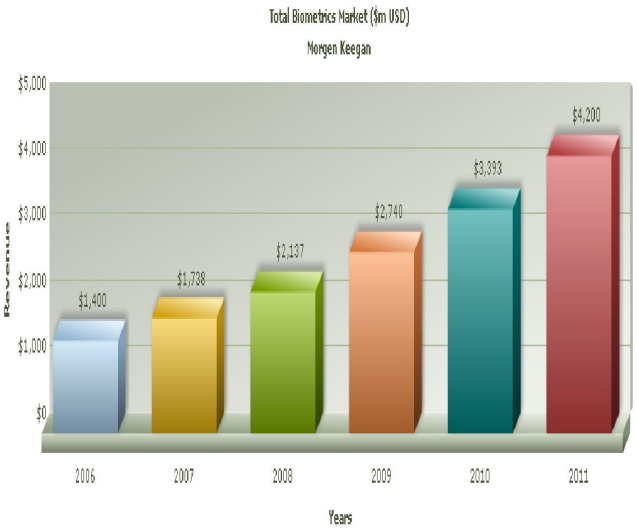
According to US based Morgan Keegan biometrics is being incorporated into numerous governmental programs and security systems. In parallel, Private sector organizations are rapidly ramping-up the use of biometric technology to increase security, productivity, and profitability.

Key Forecasts

The total biometrics market will grow at a 25% CAGR, reaching $4.2 billion in 2011 in industry revenue.

Fingerprint technology will remain the dominant biometric identifier across all applications (in terms of revenue) due to high familiarity, low overall cost factors, and the existence of large legacy fingerprint databases.

Private sector organizations are rapidly ramping-up the use of biometric technology to increase security, productivity, and profitability.



2. IBG Survey

According to International Biometrics Group (IBG) research report, the global market for Biometrics slated for high growth through 2014. In terms of technology, Automatic Finger Identification System (AFIS)/ Live Scan will be the main revenue contributor, which was worth $1.3 billion in 2009; this market is forecasted to grow to $2.9 billion by 2014.

Key Forecasts

The total biometrics market will grow at a 22.3% CAGR for the next five years, thus reaching $9.37 billion in 2014 in industry revenue.

International Biometric Group Expects Biometric Market to Nearly Triple by 2014.

Global biometric revenues are projected to grow from US$3.42billion in 2009 to $9.37 billion in 2014, driven in part by government identity management and border management programs.

Fingerprint recognition including AFIS is dominant: 2/3 of biometric market. Fingerprint is expected to gain 45.9% of the non-AFIS biometrics market in 2009, followed by face recognition at 18.5% and iris recognition at 8.3%.

Annual iris recognition revenues are projected to approach $700 million by 2014

Asia and North America are expected to be the largest global markets for biometric product and services

Vein recognition is expected to play a larger role in access control applications, eventually comprising more than 10%of this market

3. Acuity Market Intelligence Survey

A more recent long-term forecast from the US-based Acuity Market Intelligence indicates similar expected growth.

Key Forecasts

The total biometrics market will grow at a 19.69% CAGR for the next eight years, thus reaching $10.9 billion in 2017 in industry revenue.

The Central and South American region will experience the highest CAGR over the forecast period of 39.46%, the overall market dominance will shift from Europe (and the greater EMEA region) and the US (and the greater North America region) to Asia (and the greater Asia Pacific region). By 2017, the Asia Pacific Region will generate the greatest percent of revenues for the biometrics industry with more than 32% of global revenues.

The dominance of AFIS/Livescan and Fingerprint continues thorough 2009-14. However, by 2017 iris and face recognition begin to rival their dominance together accounting for more than 33% of global revenues.

Commercial deployment revenues match to Public Sector revenues in 2014 and then surpass Public Sector representing more than 55% of the total global market for biometrics core technology by 2017.

The percent of revenue from Identification Services declines over the period 2009-14 but only from 65% to 47%. Surveillance and Monitoring posts the strongest percentage gain growing from less than 1% to nearly 8% of total market revenue.

7. CONCLUSION

It is probably not only my opinion, that further development of biometric technologies will significantly change the world. This technologies can be surely not only used for making the life easier, but also for more perfect invigilation.This will be surely not hinder the development of this techniques. Almost every technology can be used for good and bad purposes – this depends only on people using it.

REFERENCES

[1] S. Prabhakar, S. Pankanti, A. K. Jain, "Biometric Recognition: Security and Privacy Concerns", *IEEE Security & Privacy*, March/April 2003, pp. 33-42

[2] A. K. Jain, A. Ross, S. Prabhakar, "An Introduction to Biometric Recognition", *IEEE Trans. on Circuits and Systems for Video Technology*, Vol. 14, No. 1, pp 4-19, January 2004

[3] D. Maio, D. Maltoni, R. Cappelli, J. L. Wayman, A. K. Jain, "FVC2002: Fingerprint verification competition" in *Proc. Int. Conf. Pattern Recognition (ICPR)*, Quebec City, QC, Canada, August 2002, pp. 744-7473.

[4] Morgan Keegan - Biometrics, Industry Overview for the Investment Community, October 2006

[5] IBG Survey - Biometrics Market and Industry Report 2009- 20146.

[6] Future of Biometrics- Published by Acuity Market Intelligence August 2009

AUTHOR

C. Sesha Ratnam received the MCA from Madras University in 2001 AND MTECH in computer science and engineering from Nagarjuna University in 2010.

C. Raja received the MCA from Madras University in 2006.

G.Ramesh received the MCA from Madras University in 2007 AND M.TECH in computer science and engineering from JNTU Anantapur in 2012.

N.Jyothsna received the B.Tech from JNTUA in 2009.

N.V.Vinod Kumar received the B.Tech from JNTUA in 2011.