A review on
Biometrics in the Past, Present and Future

Hossein Jahankhani
University of East London, UK
Presented at 3rd International Conference on
Global E-Security, 2007
Email : h.jahankhani@uel.ac.uk

In spite of numerous technological advancements in the 21st century, there remain many cases of personal identification theft; this had directed thought towards Biometric technology. Since the September 11 attacks public and governments leaders have sought to increase their security and as well as law enforcement. There is public interest in better and more widely available identification technology, enforced by governments. While the risk of privacy infringement is still a matter of discussion, and there are arguments against the use of biometric technology in law enforcement. This paper will review and looking at some of the statistics and advancement in the use of Biometric technology today and future. It also considers advantages and disadvantages of use of biometrics in law enforcement on the public and in public places.

INTRODUCTION

In past most identity verification systems available were based on techniques such as passwords, personal identification numbers (PIN) and in the last two decades, smartcards. However these methods have their limits as it is often easy to steal this information and abuse the verification system. Biometric technology in its basic form has been around for long time. Since 14th century Chinese merchants stamped children's palm and footprints on paper with ink to differentiate the young children from one another. It is only in the last two decades that it has been considered important in the security area. Particularly since 9/11, biometrics has regularly hit the headlines, (Tom de Jongh, 2007). It is a very demanding task when identification verification and authorisation has to be automated with high accuracy. In the identification process there are two systems (Chilrillo 2003),

i) Traditional knowledge-based or token-based personal identification or verification systems which are very tedious, inefficient, time-consuming and costly. Normally, Token-based approaches use "something that you have" such as; passport, credit cards etc...., (Chilrillo 2003), (Zhang 2006).

ii) Knowledge-based approach, which uses "something that we know or remember" eg., passwords, and personal identification numbers, which are used for personal identification (Ratha et- al 1999).

Biometric technology applies automated screening methods to evaluate the physiological or behavioural characteristics of an individual for the purpose of determining or verifying identity.

Biometrics is a powerful combination of science and technology that can be used to protect and secure our most valuable information and property. Biometrics is one of the most critical emerging technologies of the 21st century. As the world becomes more volatile and potentially more vulnerable to fraudulent forces, our fate lies within our ability to secure and protect critical data and facilities. With heightened awareness and concern for personal, corporate, and national security, the importance of controlled access has become a necessity for the future, (Thian et al, 2002) and

(Rosenzweig P, 2004).

The term "Biometrics" and "Biometry" is derived from the words bio (meaning life) and metric to (measure) that have been in use since the early 20th century. In

information technology, biometric authentication refers to technologies that measure and analyse human physical and behavioural characteristics for authentication purposes. Biometrics is divided into two types: behavioural (the traditional signature and voice) and physiological (face, fingerprint, hand, and iris recognition).
All behavioural biometric characteristics have a physiological component, and, to a lesser degree, physical biometric characteristics have a behavioural element.
Biometrics has been around for quite some time. In fact, many people would be surprised to learn that biometrics emerged long before the Internet, Neil Armstrong's moon walk, television, the automobile, and the phonograph. Biometrics arguably precedes the births of Thomas Edison and Benjamin Franklin. The use of fingerprints as a means of identification was the first example of biometrics to emerge, and they continue to be used today. Of course, the technology used for scanning, reading, analysing, and recognising biometrics emerged well after the initial study of fingerprints, (Celent, LLC, 2006).

Due to rapid development of electronics and software-engineering Biometric technologies have developed enormously in recent years. The recent expanded use of biometrics brings this issue to light like never before. Biometrics is the automated capture of a person's unique biological data that distinguishes him or her from another individual. Biometrics can be measured in many forms, including fingerprints, voice patterns, head geometry, iris patterns, DNA, retina recognition, speaker recognition, mapping vein patterns, keystroke, hand geometry and face recognition. The main reason biometrics work for identification is that an individual can not control these unique aspects of their biology; for example, a person can not change their fingerprint or the identifying features of their iris, (McKenzie et al 2004).

Concept of Biometric

Biometric technology refers to the automatic recognition of individuals based on their physiological and/or behavioural characteristics. Biometric systems are rapidly being designed and applied to many aspects of our everyday lives. At end of 2006 the United Kingdom was one of the 27 countries signed up to the US Visa Waiver Program, which demands that all passports issued after October 2006 must contain a machine readable chip which holds the passport holder's details and a biometric identifier, (BBC News,26 October 2006).
Regardless of the type of biometric technology that is used, the basic concept of verification/authentication remains the same. The characteristic is evaluated and compared with a copy stored in a database or on a smart card. Comparison against card-stored or centrally recorded reference patterns can be carried out automatically using various software analyses methods. Biometric technologies are used almost exclusively for purposes of identification or authentication/verification. Identification is also often described as one-to-many matching.

Identification: this biometric process is represented by the question "*Who is this person?*" This may be answered by searching a central database of biometric template information to establish the identity of an individual unknown at the time of matching. This is known as a "one-to-many" or "1-n" search.

Verification/Authentication: this refers to the process attempting to verify the identity of a known individual. It is represented by the question "*Is this person who they claim to be?*" and will be answered by biometric comparison between a previously stored template and one provided by the authorised user at the time of transaction. This is termed a "one-to-one" or "1:1" search. Verification has the benefit of minimising transaction processing time to significantly speed the matching process.
A wide variety of systems require reliable personal recognition schemes to either confirm or determine the identity of an individual requesting their services. The purpose of such schemes is to ensure that the rendered services are accessed only by a legitimate user and no one else. Examples of such applications include secure access to buildings, computer systems, laptops,

mobile phones, and ATMs. In the absence of robust personal recognition schemes, these systems are vulnerable to the wiles of an impostor.

By using biometrics, it is possible to confirm or establish an individual's identity based on "who he/she is", (e.g., eye scan) rather than by "what he/she possesses" (e.g., an ID card) or "what she remembers" (e.g., a password), (Grillo 2007). In the past, biometrics were used primarily in conjunction with crime issues, with the most familiar being the fingerprint. Most citizens did not feel their privacy was violated because fingerprints were only required of criminals.

Biometrics Law and Privacy

Today's "new technological realities" force us to examine, from the law and policy perspectives, what is required to safeguard the public interest and to ensure accurate results for society. Biometrics is one such new technological reality. While not enjoying the media stature and public controversy associated with high tech issues like genetic cloning and cyberspace, biometrics – which seeks a fast, foolproof answer to the questions, "Who are you?" or "Are you the person whom you claim to be?" – will cause the law to take notice as it becomes more extensively used in the public and private sectors. Businesses, numerous government agencies, law enforcement and other private and public concerns are making increasing use of biometric scanning systems, (Woodward, John D, 2004)

Privacy must be balanced with many competing interests, including those of other individuals and society as a whole. With the rapid development of technology, it is more and more difficult to maintain the levels of privacy citizens knew in the past. Everywhere we turn, data is being collected, and with advances in databases, data mining, and telecommunications, it is almost effortless to circulate personal information to any interested party (Clarke, 1999).

After the events of September 11th, Governments paid a great deal of attention to the use of different types of Biometrics, automated human identification techniques, in most public situations.

Types of Biometric Technology

There are many types of biometric technology in use today; I will be focusing mainly on the most commonly used ones. I will, however, briefly mention some of the emerging technologies.

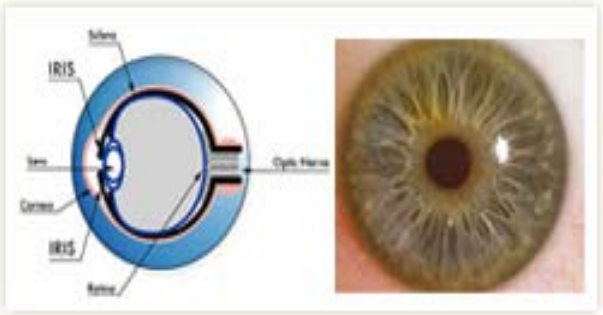
Iris Recognition :

Iris scanning uses the unique characteristics of the iris in the human eye to effectively verify the identity of an individual. The iris of the eye is extremely complex and has a wide variety of characteristics the imager can use to verify the individual. The differences in the human eye are so extreme that error is unlikely to occur. It is almost impossible to falsify a person's identity with the use of an iris scan. Each person's iris has a unique and complexly patterned structure. The structure is a combination of specific characteristics called corona, crypts, filaments, freckles, pits, radial furrows and striations. Glasses affect the quality of the image obtained, but contact lenses do not. Another reported advantage of iris recognition is that it is very unlikely that an artificial or dead iris could be used to fraudulently bypass the system.

The reasons why iris is used as a biometric technology are;

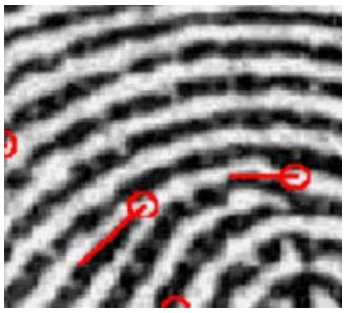
- It is an organ which can be measured and visible with the eye.
- The only organ which never changes
- It does not change since the 16th month of a baby till the death
- The rate of finding two similar iris is $1/10^{78}$
- Every eye on the earth is unique
- Twins has the same DNAs but different iris.
- Eye iris is the less effected part from the genetic formations
- Eye iris is not affected by constant diseases.
- Iris is nor effected by the race, sex and skin colour

- Eyelid is the protective cover of the eye.
- It is placed on our head where our reflexes and our senses are.
- Eye is the first organ to lose after death (3 sec). http://www.ergosis.com.tr/eng.

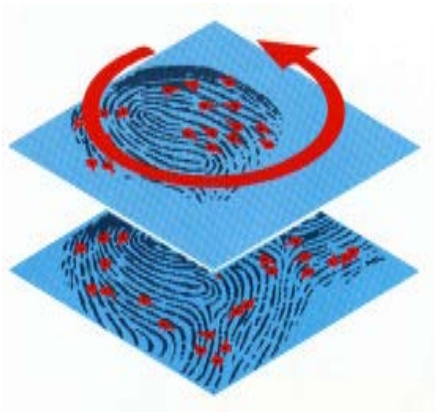


Picture from; Ergosis R&D engineers, http://www.ergosis.com.tr.

Fingerprint Scanning:
Fingerprints are the oldest and most commonly used biometric known. Fingerprints form in the womb and, barring injury, remain unique and consistent throughout life. Fingerprints analyses are an important technique in criminal investigations and the identification of individuals; (Prabhakar et al 2003) state that there are seven differences that should be looked at when deciding biometric limits. These seven limits are barriers to universality, distinctiveness, permanence, collectability, performance, acceptability, and potential for circumvention. "Fingerprints are used to identify an unknown victim, witness, or suspect, to verify records, and most importantly, as links and matches between a suspect and a crime" (O'Connor, 2004). O'Connor states that when looking at fingerprints, they are divided into three major categories. These are arches, loops, and whorls. These groups can, in turn, be sub-divided. When looking at fingerprints race becomes a factor, because different ethnic groups have different traits that stand out. Prints are read are by the measurement between the different arches, loops, and whorls.



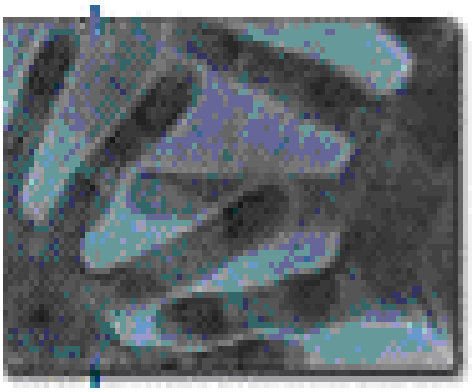
(a)



(b)

Pictures (a) and (b) from www.unilink.com, visited 2 March 2007.

Hand Shape:
In the hand shape method, a three-dimensional image of the hand is taken and measurements of the shape and length of fingers and knuckles are made. This was one of the first biometric technologies developed. Both hand and finger geometry do not achieve the highest levels of accuracy but they are convenient and it is possible to process large volumes of identification data quickly. Their predominant use is for access control. The size and shape of hands are unique to individuals. To identify or verify individuals, an imaging device scans the three-dimensional geometry of the hand and fingers, and creates a mathematical picture, which can then be compared against an image stored in a database.



Pictures from;
http://et.wcu.edu/aidc/biowebpages,
visited 15 March 2007.

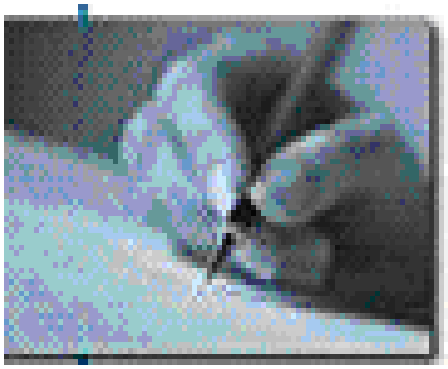
Face Recognition :

The relationships between the parts of the face remain relatively stable from childhood onward. Facial recognition techniques use this stability as their point of departure. Facial recognition technologies utilise digital photographs to create mathematical descriptions of individual faces and then compare them against those stored in a database. Facial recognition requires a large image capture device and clear lighting conditions, and is therefore most suitable to authenticate identity at fixed locations, such as airports facilities. Facial recognition data is also being encoded via mobile technologies, such as the new generation of biometric passports.

Our faces make lasting impressions. Despite the growing popularity of cosmetic surgery, research has shown that the face we are born with remains identifiable throughout our lives. Facial scanning applications are most often used in conjunction with other verification methods such as identification cards systems or with existing security cameras and monitors. This method utilises high resolution images of distinct facial features such as eye sockets, shape of the nose, or the position of certain features relative to each other. Problems arise with this application if the subject is not properly positioned for the camera or if environmental changes such as lighting prevent an accurate read.

Signature :

Signature scanning technology involves the evaluation of both the resulting signature and the behavioural characteristics , pressure, speed, and type of stroke - used to create the signature. The use of behavioural characteristics prevents counterfeit signatures and makes this biometric method highly accurate. This biometric technology is referred to as dynamic signature verification (DSV). It is the method of signing rather than the finished signature which is important and is not the same as the study of static signatures on paper (handwriting analysis.) A number of characteristics are examined by DSV including the angle, at which the pen is held, the time taken to sign, the speed and acceleration of the signature, the pressure exerted when holding the pen and the number of times the pen is lifted from the paper. An advantage of signature biometrics is the acceptance of a signature as a means of asserting identity, and in a number of situations to legally bind an individual. This form of biometric is commonly used.



Pictures from;
http://et.wcu.edu/aidc/biowebpages,
visited 15 March 2007.

Voice Recognition :

This type of biometric focuses on the sound of the voice rather than trying to recognise words. This is quite distinct from the technology that recognises words and acts on commands. To avoid confusion, the terms "speaker recognition," "speaker verification" and "speaker identification" are used. The sound of a human voice is created by resonance in the vocal tract. The

length of the vocal tract and the shape of the mouth and nasal cavities affect the sound measured by this technology.

The techniques for analysing the voice may involve the user uttering a specifically designated password combining phrases, words or numbers, or with the user saying any form of phrase, words or numbers. Currently the former technique is most often used. This technology also has the advantage of being useful for telephone-based applications. However, environmental background noise and interference over telephone networks can affect the performance of these systems. Also, if the user has a cold or some other infection that may affect the sound of the voice, it may not properly identify the user.

Picture from;
http://et.wcu.edu/aidc/biowebpages,
visited 15 March 2007.

Keystroke Recognition:
Keystroke Recognition works in different way in comparison to the other biometric technologies examined. Keystroke Recognition is probably one of the easiest to implement and administer. This is so because at the present time, Keystroke Recognition is completely a software based solution. There is no need to install any new hardware. All that is needed is the existing computer and keyboard that the individual is currently using.

To start the enrolment process, the individual must type a specific word or group of words. In most cases, the username and password of the individual is used. It is very important that this same word or phrasing is used in both the enrolment and verification processes. Otherwise, the behavioural characteristics of typing will be significantly different, and as a result, there will be a mismatch between the enrolment and verification templates. To create the enrolment template, the individual must type their user name and password about fifteen times. It is highly recommended that the enrolment process occur over a period of time, rather than at a single point in time. This is so because the behavioural characteristics will be much more consistent.

The distinctive, behavioural characteristics measured by Keystroke Recognition include:

1. The cumulative typing speed;
2. The time that elapses between consecutive keystrokes;
3. The time that each key is held down;
4. The frequency of the individual in using other keys on the keyboard, such as the number pad or function keys;
5. The sequence utilised by the individual when attempting to type a capital letter - for example, does the individual release the shift key or the letter key first?

These behavioural characteristics are then turned into statistical profiles, which then essentially become the enrolment and verification templates. These templates also store the actual username and password. The statistical profiles can either be "global" or "local". With a "global" profile, all behavioural characteristics of the typing can be combined, or with a "local" profile, the behavioural characteristics are measured for each keystroke.

It is important at this point to make a distinction between static and dynamic keystroke verification. With the former, verification is established only at certain times, for example, when the individual logins into their computer. However, with the latter, the individual's keystroke and typing patterns are recorded during the entire session.

The Strengths and Weaknesses of Keystroke Recognition :

Keystroke Recognition possesses a number of strengths and weaknesses. In terms of strengths, probably the biggest one is that it does not require any additional, specialised hardware to implement. As stated before, Keystroke Recognition is purely a software based solution. Secondly, Keystroke Recognition can be easily integrated with other, existing authentication processes. Thirdly, everybody is familiar with typing their username and password. As a result, there is very minimal training required in order for an individual to use a Keystroke Recognition system properly.

In terms of weaknesses, Keystroke Recognition possesses the same flaws a username/password system has. For example, passwords can be forgotten or compromised, and individuals will have to continue to remember multiple passwords in order to gain access to the network system. It should be noted that Keystroke Recognition does not ease the burden of having to remember multiple passwords, or decrease the administrative costs of having to reset passwords. It only enhances the security to an existing username/password based system. Secondly, Keystroke Recognition is still not a proven technology, like other biometric systems, and as a result, has not been tested in wide scale deployments. Finally, Keystroke Recognition does not enhance convenience to the individual using the system, (Ravi Das, 2004).

Picture from ;
http://et.wcu.edu/aidc/biowebpages,
visited 15 March 2007.

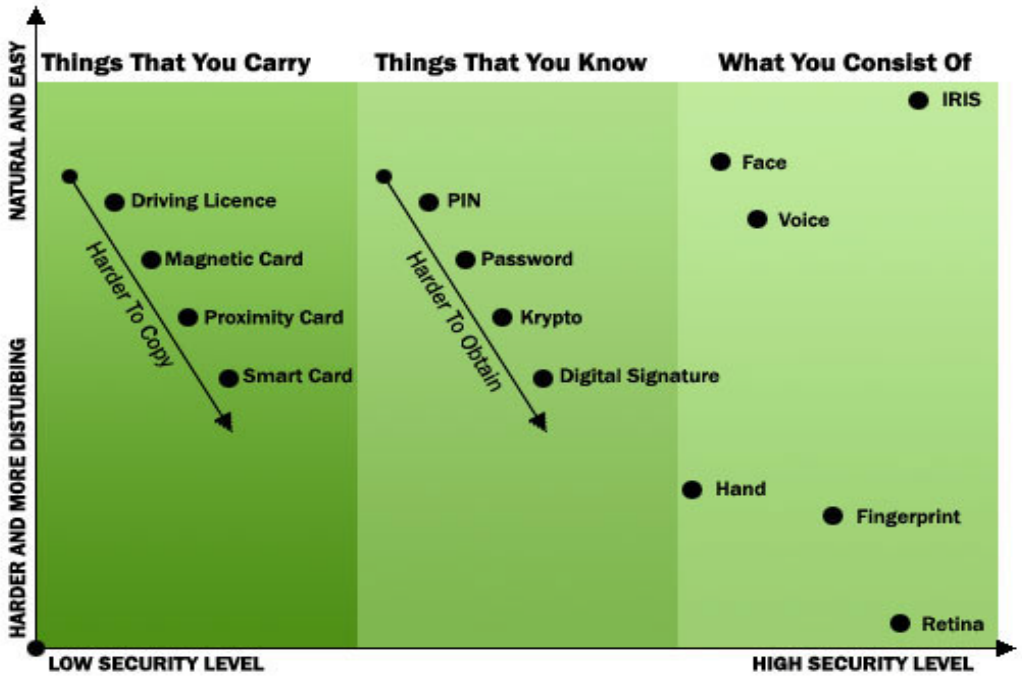
Comparison between different Types of Biometric Technology

All biometric types have their specific uses, and can either be combined or used on their own to identify/authenticate a user. The table below shows the misidentification rate of some of the method (types) explained above. This figure was obtained from a study that was done by AIM Japan (2004), where each method was tested.

Type of Biometric	Biometric authentication Method	Mis-identification rate	Security level	Applications
Iris Recognition	Iris pattern	1/1,200,000	High	High-security facilities
Fingerprinting	Fingerprints	1/1,000	Medium	Universal
Hand Shape	Size, length and thickness of hands	1/700	Low	Low-security facilities
Facial Recognition	Outline, shape and distribution of eyes and nose	1/100	Low	Low-security facilities
Signature	Shape of letters, writing order, pen pressure	1/100	Low	Low-security facilities
Voice Recognition	Voice characteristics	1/30	Low	Telephone service

Table above shows the comparison of the different types of biometric technology.

(Statistic obtained from AIM Japan 2004)



Data from Ergosis R&D engineers, http://www.ergosis.com.tr.

Biometrics in future

One option for future use of biometrics is in finger-scanning in ATM payment machines. This would help pensioners to get their money from any ATM machines instead queuing up in line for hours on specific dates. In last few years a Colombian Bank implemented Biometric verification at their ATM machines, in order to help the coffee growers in urban areas access to their money easily and much more safely.

From 2007/2008 will be mandatory for every passport renewed in the United Kingdom will carry a have a micro chip in it. The chip will hold biometric data-unique physiological or behavioural characteristic. Growing public concerns about home and global security, asylum and immigration as well as identity theft the official United Kingdom travel document will not just carry a photograph, BBC news, 2004. Most governments departments are creating more data bases and biometrics reader in their departments. Gradually, more publics and privates businesses are using biometrics in their premises. Here some of the example of recent developments in biometrics security equipments.

Picture from;
http://www.buyasafe.com/Fingerprint visited 15 Feb 2007.

Picture from, http://news.bbc.co.uk

Conclusion

Review showed that there is a strong need to use and involvements Biometrics in future. Need to use different types of Biometrics for different purpose of identification. A single Biometrics system alone likely is not an ideal form of security. Biometrics can be implemented in connection with username - password pair. Username-password pair alone is rarely described for secure installations. This paper review showed that importance of the biometrics. There are two important key drivers of support for biometrics; i) fighting terrorism and concerns about identity Fraud. ii) Future levels of support will depend upon : levels of accuracy and error in specific applications, future terrorist attacks, whether

government uses are proper and whether safeguards operate effectively. The possible negative point about use of biometrics technologies is some about 40-50% of public are concerning about identity theft.

References :

1. Tom de Jongh, (2007) article on Biometrics, European Reseller magazine.

2. Chilrillo J, et al (2003), Implementing Biometric Security, Indianapolis, Indiana, Canada, Wiley Publishing, Inc.

3. Zhang D., et al , (2006), Biometric image discrimination technologies, Hershey, USA, Idea group Inc publications.

4. Ratha et al (1999), Automated Biometrics, Yorktown Heights, IBM Thomas Research Centre, NY 10598.

5. Wildes, R.P. (2005) Iris recognition: an emerging biometric technology.

6. Anil K. Jain, (2004) Biometrics: A Grand Challenge, 17th International Conference on Pattern Recognition, Vol 2, p35-42.

7. Thian, Bengio, Korczak (2002) A Multi-sample Multi-source Model for Biometric Authentication.

8. Grillo A, (2007), MSc dissertation, in progress.

9. Rosenzweig, P,(2004) Biometric Technologies: Security, Legal, and Policy Implications,http://www.heritage.org/ Research/ HomelandDefense/lm12.cfm

10. Clarke, R. 1999, Internet Privacy ConcernsConfirm the Case for Intervention; Industry Trend or Event.

11. BBC News in 2 minutes, 26 October 2006, www.bbc.co.uk.

12. McKenzie, M. Jahankhani Hossein, (2004), Biometrics'Big Brother Exposed', Global e-Security, Proceedings of the 1st International Conference.

13. Celent, LLC., (2005), Reproduction prohibited at www.celent.com.

14. Woodward John D., (2004), Identifying Law and Policy Concern.

15. Biometric Technologies: Are We There Yet? January 2006.
16. Prabhakar, Pankanti, and Jain (2003), Security &Privacy Magazine, IEEE, Vol 1, Issue 2.
17. Ravi Das, 2004, www.htgsolutions.com.
18. O'Connor, S.M, (2004), Biometrics and Identification After 9/11. Bender's Immigration Bulletin, Vol 7, p150.