"A Conceptual Study Of Biometric Security And Its Perception Towards Usability"

[1]Dr.A.Lakshmi and [2]G.Gokulkumari

[1]Director & Professor, MBA Department, KSR.College of Technology, Tiruchencode.
[2](Research Scholar) Asst. Professor, CSE Department, Shirdi Sai Engineering College,Bangalore

Abstract - **Biometrics in high technology sector uses an individual's unique biological traits to determine one's identity. Advances in biometric technology are focusing both on better security and cost effectiveness. Modern methods of authentication differ from traditional methods in several ways. Among the various types of biometric security system prevailing in India, the finger print is mostly used by the majority of the respondents This paper summarizes these differences along with the advantages of modern biometrics. Majority of the respondents (58.6%) are facing issues and challenges while adopting biometric security system. Most of the respondents (45.8%) are using the biometric security at office. Biometric characteristics should be as unique and permanent as possible. If compromised, it is argued that biometric characteristics could be misused and then, like a password, rendered unusable, except that a password is always exchangeable whereas a biometric characteristic isn't. The actual danger depends upon the application and the associated precautions.**

Keywords – **Biometric, Security, Perception, Recognition, Password**

1. INTRODUCTION

Biometrics in the high technology sector refers to a particular class of identification technologies. These technologies use an individual's unique biological traits to determine one's identity. The traits that are considered include fingerprints, retina and iris patterns, and facial characteristics.

The biological traits used in modern biometric applications are chosen based on our technical ability to catalogue and track them. Some traits are easier to obtain than others. Fingerprints, for example, are relatively simple to record and store in a database. They also tend to be less accurate and secure than other more complex biometrics.

Advances in biometric technology are focused on improving the accuracy and security of measurements and reducing the cost to levels appropriate for consumer applications. Simple and low cost systems available today, such as fingerprint readers, will become more reliable. High accuracy systems such as retina scanners will drop in price and will eventually supplement or replace existing systems.

2. BIOMETRICS, PAST AND PRESENT

Most people have some degree of familiarity with biometrics, thanks to television and the movies. Hollywood has portrayed biometrics as futuristic technology in science fiction movies, and as elite security technology in spy movies. This has given biometric technologies an expensive and exclusive reputation. Many business owners or executives would most likely say, "We don't need that kind of security; we are not a military facility." Some people don't even think the technology is real, convinced that it's still in the realm of science fiction. As a result, biometric systems have been unintentionally marketed as a very advanced, high-end security technology for many years.

The difference between today and twenty years ago is seen in both the effectiveness of the technology and the greatly reduced cost. What one may have only seen in the movies may soon be seen on the front door of your home. Door locks that work using fingerprints or handprints instead of keys are already available at consumer-level cost.

In the coming years a very real and very new market for biometrics will be emerging. Biometrics is truly high tech and, when utilized, gives off an image of an expensive, extremely secure technology. If you have ever had to pass through a retina scanner to get to a meeting, you already know what we mean.

Biometrics is commonly criticized for providing more glitz than security. There can be truth to this claim, depending on how biometric systems are implemented. For example, a retina scanner provides little security if an authorized person holds the door for a stranger standing behind them. Biometrics can only provide effective security when properly combined with other identification factors.

These traditional methods of the user authentication unfortunately do not authenticate the user as such. Traditional methods are based on properties that can be forgotten, disclosed, lost or stolen. Passwords often are easily accessible to colleagues and even occasional visitors and users tend to pass their tokens to or share their passwords with their colleagues to make their work easier. Biometrics, on the other hand, authenticates humans as such – in case the biometric system used is working properly and reliably, which is not so easy to achieve. Biometrics is automated methods of identity verification or identification based on the principle of measurable physiological or behavioral characteristics such as a fingerprint, an iris pattern or a voice sample. Biometric characteristics are (or rather should be) unique and not duplicable or transferable.

3. WORKING OF BIOMETRIC RECOGNITION

The biometric data subject (the person to be recognized) presents his or her biometric characteristic to the biometric capture device which generates a recognition biometric sample from it. From the recognition biometric sample the biometric feature extraction creates biometric features which are compared with one or multiple biometric templates from the biometric enrolment database. Due to the statistical nature of biometric samples there is generally no exact match possible. For that reason, the decision process will only assign the biometric data subject to a biometric template and confirm recognition if the comparison score exceeds an adjustable threshold.

What to measure?

Most significant difference between biometric and traditional Technologies lies in the answer of the biometric system to an authentication/identification request. Biometric systems do not give simple yes/no answers. While the password either is ’abcd’ or not and the card PIN 1234 either is valid or not, no biometric system can verify the identity or identify a person absolutely. The person’s signature never is absolutely identical and the position of the finger on the fingerprint reader will vary as well. Instead, we are told how similar the current biometric data is to the record stored in the database. Thus the biometric system actually says the probability that these two biometric samples come from the same person.

Biometric technologies can be divided into 2 major categories according to what they measure :

* Devices based on physiological characteristics of a person (Such as, fingerprint or hand geometry).

* Systems based on behavioral characteristics of a person (Ex: signature dynamics).

Biometric systems from the first category are usually more reliable and accurate as the physiological characteristics are easier to repeat and often are not affected by current (mental) conditions such as stress or illness.

One could build a system that requires a 100% match each time. Yet such a system would be practically useless, as only very few users (if any) could use it. Most of the users would be rejected all the time, because the measurement results never are the same. We have to allow for some variability of the biometric data in order not to reject too many authorized users. However, the greater variability we allow the greater is the probability that an impostor with a similar biometric data will be accepted as an authorized user. The variability is usually called a (security) threshold or a security

(Security) level. If the variability allowed is small then the threshold or the security level is called high and if we allow for greater variability then the security threshold or the security level is called low.

4. COMPARISON OF VARIOUS BIOMETRIC TECHNOLOGIES

It is possible to understand if a human characteristic can be used for biometrics in terms of the following parameters:

- Universality each person should have the characteristic
- Uniqueness is how well the biometric separates individually from another.
- Permanence measures how well a biometric resists aging.
- Collectability ease of acquisition for measurement.
- Performance accuracy, speed, and robustness of technology used.
- Acceptability degree of approval of a technology.
- Circumvention eases of use of a substitute.

5. ERROR RATES AND THEIR USAGE

There are two kinds of errors that biometric systems do:

* False rejection (Type 1 error) – a legitimate user is rejected (because the system does not find the user’s current biometric data similar enough to the master template stored in the database).

* False acceptance (Type 2 error) – an impostor is accepted as a legitimate user (because the system finds the impostor’s biometric data similar enough to the master template of a legitimate user).In an ideal system, there are no false rejections and no false acceptances. In a real system, however, these numbers are non-zero and depend on the security threshold. The higher the threshold the more false rejections and less false acceptances and the lower the threshold the less false rejections and more false acceptances. The number of false rejections and the number of false acceptances are inversely proportional. The decision obtained from threshold is mainly used for the entire biometric system. It is

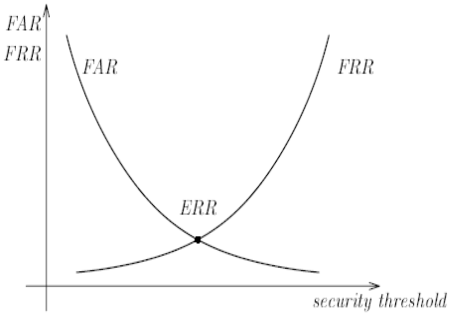
chosen as a compromise between the security and the usability of the system. The biometric system at the gate of the Disney's amusement park will typically use lower threshold than the biometric system at the gate of the NSA headquarters.

The number of false rejections/false acceptances is usually expressed as a percentage from the total number of authorized/unauthorized access attempts. These rates are called the *false rejection rate (FRR)/false acceptance rate (FAR).*

The values of the rates are bound to a certain security threshold. Most of the systems support multiple security thresholds with appropriate false acceptance and false rejection rates.

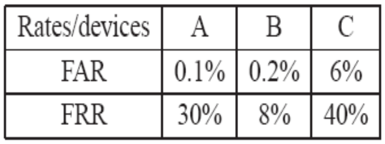
Some of the biometric devices (or the accompanying software) take the desired security threshold as a parameter of the decision process (e.g. for a high threshold only linear transformations are process allowed), the other devices return a score within a range (e.g. a difference score between 0 and 1000, where 0 means the perfect match) and the decision itself is left to the application.

If the device supports multiple security levels or returns a score we can create a graph indicating the dependence of the FAR and FRR on the threshold value. The following picture shows an example of such a graph:

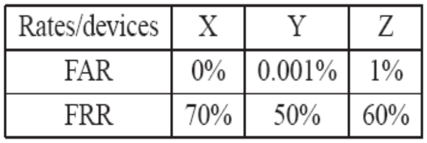


The curves of FAR and FRR cross at the point where FAR and FRR are equal. This value is called the *equal error rate (ERR)* or the *crossover accuracy*. This value does not have any practical use (we rarely want FAR and FRR to be the same), but it is an indicator how accurate the device is. If we have two devices with the equal error rates of 1% and 10% then we know that the first device is more accurate (i.e., does fewer errors) than the other. However, such comparisons are not so straightforward in the reality. First, any numbers supplied by manufacturers are incomparable because manufacturers usually do not publish exact conditions of their tests and second even if we have the supervision of the tests, the tests are very dependent on the behavior of users and other external influences.

The manufacturers often publish only the best achievable rates (e.g., FAR < 0.01% and FRR < 0.1%), but this does not mean that these rates can be achieved at the same time (i.e., at one security threshold). Moreover, not all the manufacturers use the same algorithms for calculating the rates. Especially the base for computation of the FAR often differs significantly. So one must be very careful when interpreting any such numbers. The following table shows real rounded rates (from real tests) for three devices set the lowest security level possible



Rates/devices	A	B	C
FAR	0.1%	0.2%	6%
FRR	30%	8%	40%



Rates/devices	X	Y	Z
FAR	0%	0.001%	1%
FRR	70%	50%	60%

This table shows rates (again rounded) for three devices set to the highest security level possible:

Although the error rates quoted by manufactures (typically ERR < 1%) might indicate that biometric systems are very accurate, the reality is rather different. Namely the false rejection rate is in reality very high (very often over 10%). This prevents the legitimate users to gain their access rights and stands for a significant problem of the biometric systems.

6. BIOMETRIC TECHNIQUES

There are lots of biometric techniques available nowadays. A few of them are in the stage of the research only (e.g. the odor analysis), but a significant number of technologies is already mature and commercially available (at least ten different types of biometrics are commercially available nowadays: fingerprint, finger geometry, hand geometry, palm print, iris pattern, retina pattern, facial recognition, voice comparison, signature dynamics and typing rhythm).

Issues and concerns

As with many interesting and powerful developments of technology, there are concerns about biometrics. The biggest concern is the fact that once a fingerprint or other biometric source has been compromised it is compromised for life, because users can never change their fingerprints. A theoretical example is a debit card with a personal Identification Number (PIN) or a biometric. Some argue that if a person's biometric data is stolen it might allow someone else to access personal information or financial accounts, in which case the damage could be irreversible. However, this argument ignores a key operational factor intrinsic to all biometrics-based security solutions: biometric solutions are based on matching, at the point of transaction, the information obtained by the scan of a "live" biometric sample to a pre-stored, static "match template" created when the user originally enrolled in the security system. Most of the commercially available biometric systems address the issues of ensuring that the static enrollment sample has not been tampered with (for example, by using hash codes and encryption), so the problem is effectively limited to cases where the scanned "live" biometric data is hacked. Even then, most competently designed solutions contain anti-hacking routines

7. CREATION OF MASTER CHARACTERISTICS

The biometric measurements are processed after the acquisition. The number of biometric samples necessary for further processing is based on the nature of given biometric technology. Sometimes a single sample is sufficient, but often multiple (usually 3 or 5) biometric samples are required. The biometric characteristics are most commonly neither compared nor stored in the raw format (say as a bitmap).

Storage of master characteristics

After processing the first biometric sample(s) and extracting the features, we have to store (and maintain) the newly obtained master template. Choosing proper discriminating characteristic for the categorization of records in large databases can improve identification (search) tasks later on. There are basically 4 possibilities where to store the template: in a card, in the central database on a server, on a workstation or directly in an authentication terminal. The storage in an authentication terminal cannot be used for large-scale systems, in such a case only the first two possibilities are applicable. If privacy issues need to be considered then the storage on a card (magnetic stripe, smart or 2D bar) has an advantage, because in this case no biometric data must be stored (and potentially misused) in a central database.

As soon as the user is enrolled, she can use the system for successful authentications or identifications. This process is typically fully automated and takes the following steps:

Acquisition(s)

Current biometric measurements must be obtained for the system to be able to make comparison with the master template. These subsequent acquisitions of the user’s biometric measurements are done at various places where authentication of the user is required. It is often up to the reader to check that the measurements obtained really belong to a live persons (the livens property). In many biometric techniques (e.g., fingerprinting) the further processing trusts the biometric hardware to check the livens of the person and provide genuine biometric measurements only. Some other systems (like the face recognition) check the user’s livens in software (time-phased sampling).

8. CREATION OF NEW CHARACTERISTICS

The biometric measurements obtained in the previous step are processed and new characteristics are created. Only a single biometric sample is usually available. This might mean that the number or quality of extracted features is lower than at the time of enrolment.

Comparison

Currently computed characteristics are compared with the characteristics obtained during enrolment. If the system performs (identity) verification then these newly obtained characteristics are compared only to the master template. For an identification request the new characteristics are matched against a large number of master templates.

Decision

The final step in the verification process is the yes/no decision based on a threshold. This security threshold is either a parameter of the matching process or the resulting score is compared with the threshold value. Although the error rates quoted by manufactures (typical values of equal error rate (ERR) 1 do not exceed 1%) might indicate that biometric systems are very accurate, the reality is much worse. Especially the false rejection rate is quite high (very often over 10%) in real applications. This prevents legitimate users to gain their access rights and stands for a significant problem of biometric systems.

8. WHAT ARE THE ADVANTAGES OF BIOMETRIC AUTHENTICATION?

The primary advantage of biometric authentication methods over other methods of user authentication is that they really do what they should, i.e., they authenticate the user. These methods use real human physiological or behavioral characteristics to authenticate users. These biometric characteristics are (more or less) permanent and not changeable.

It is also not easy (although in some cases not principally impossible) to change one’s fingerprint, iris or other biometric characteristics. Users cannot pass their biometric characteristics to other users as easily as they do with their cards or passwords. Biometric objects cannot be stolen as tokens, keys, cards or other objects used for the traditional user authentication, yet biometric characteristics can be stolen from computer systems and networks. Biometric characteristics are not secret and therefore the availability of a user’s fingerprint or iris pattern does not break security the same way as availability of the user’s password. Even the use of dead or artificial biometric characteristics should not let the attacker in. Most biometric techniques are based on something that cannot be lost or forgotten. This is an advantage for users as well as for system administrators because the problems and costs associated with lost, reissued or temporarily issued tokens/cards/passwords can be avoided, thus saving some costs of the system management. Another advantage of biometric authentication systems may be their speed. The authentication of a habituated user using an iris-based identification system may take 2 (or 3) seconds while finding your key ring, locating the right key and using it may take some 5 (or 10) seconds.

9. DISADVANTAGES OF BIOMETRIC AUTHENTICATION

Biometric systems still need to be improved in the terms of accuracy and speed. Biometric systems with the false rejection rate under 1% (together with a reasonably low false acceptance rate) are still rare today. Although few biometric systems are fast and accurate (in terms of low false acceptance rate) enough to allow identification (automatically recognizing the user identity), most of current systems are suitable for the verification only, as the false acceptance rate is too high. People without hands cannot use fingerprint or hand-based systems3. Visually impaired people have difficulties using iris or retina based techniques. As not all users are able to use a specific biometric system, the authentication system must be extended to handle users falling into the FTE category. This can make the resulting system more complicated, less secure or more expensive.

Even enrolled users can have difficulties using a biometric system. The FTE rate says how many of the input samples are of insufficient quality. Data acquisition must be repeated if the quality of input sample is not sufficient for further processing and this would be annoying for users. Biometric data are not considered to be secret and security of a biometric system cannot be based on the secrecy of user's biometric characteristics. The server cannot authenticate the user just after receiving her correct biometric characteristics. The user authentication can be successful only when user's characteristics are fresh and have been collected from the user being authenticated. This implies that the biometric input device must be trusted. Its authenticity should be verified (unless the device and the link are physically secure) and user's livens would be checked. The input device also should be under human supervision or tamper-resistant. The fact that biometric characteristics are not secret brings some issues that traditional authentication systems need not deal with. Many of the current biometric systems are not aware of this fact and therefore the security level they offer is limited. Some biometric sensors (particularly those having contact with users) also have a limited lifetime. While a magnetic card reader may be used for years (or even decades), the optical fingerprint reader (if heavily used) must be regularly cleaned and even then the lifetime need not exceed one year.

Biometric systems may violate user's privacy. Biometric characteristics are sensitive data that may contain a lot of personal information. The DNA (being the typical example) contains (among others) the user's preposition to diseases. This may be a very interesting piece of information for an insurance company. The body odor can provide information about user's recent activities. Biometric systems can potentially be quite troublesome for some users. These users find some biometric systems intrusive or personally invasive. Even if no biometric system is really dangerous, users are occasionally afraid of something they do not know much about. In some countries people do not like to touch something that has already been touched many times (e.g., biometric sensor), while in some countries people do not like to be photographed or their faces are completely covered. Lack of standards (or ignorance of standards) may also posses a serious problem.

10. CUSTOMER PERCEPTION AND INFLUENCE IN BIOMETRICS

To study the users' perception toward biometric security system in terms of its privacy and technology, the respondents were queried various aspects of technology and privacy involved in the existing biometric security system that they are using in their day-to-day affairs. Their valuable responses were analyzed using descriptive statistics, non-parametric tests such as chi-square and Friedman Two-Way ANOVA, mean comparison test such as one sample 't' test and independent samples 't' test. The results are tabulated in the subsequent sections of the chapter.

The type of biometric security presently used by the respondents

Type of biometric security	Frequency	Chi-Square (Sig at 5%)
Finger print	120	5.540 df=13
Face recognition	91	
Iris recognition	92	
Voice recognition	97	
Signature / handwriting recognition	100	
Others (Hand finger geometry, retina scan, ear canal, DNA, Odor, etc)	0	

Table shows the results of percentage and chi-square analysis on the type of biometric security presently used by the respondents. From the table it is apparent that, the finger print is presently used by the 24% (120) of the respondents followed by the face recognition 18.2 % (91) of the respondents, iris recognition 18.4% (92) of the respondents, voice recognition 19.4% (97) and signature/handwriting recognition 20% (100) of the respondents. Thus, among the various types of biometric security system prevailing in India, the finger print is mostly used by the majority of the respondents (24%). Since, the other types of biometric security such as hand geometry, retina scan, ear canal, DNA, Odor, etc are not practiced in India, there are no respondents using it.

Further, the type of biometric security system presently used by the respondents do not differ significantly as the chi-square value (5.540; p=0.236; df=13) is insignificant at 5% level for 4 degrees of freedom.

Reasons behind the use of biometric security by the respondents

Reasons	Frequency	Chi-Square (Sig at 5%)
Being an employee	140	55.624 df=5
Threat to theft	92	
Security conditions	74	
Privacy	73	
Avoidance of misuse	53	
Other reasons	68	

The various reasons for using biometric security such as being an employee, threat to theft, security conditions, privacy, avoidance of misuse and other reasons were analyzed using percentage and chi-square analysis. The results are tabulated in Table Perusal of the table reveals that 28% of the respondents using the biometric security for the reason as being an employee followed by 18.4% of them for threat to theft, 14.8% of them for security conditions, 14.6% of them for privacy reasons, 10.6% of them for avoidance of misuse and 13.6% of them for various other reasons such as fancy, availing new technology and minimizing the security burden. Thus, being an employee is stated as the reason for using the biometric security by the majority of the respondents (28%). Further, the chi-square value (55.624;p=0.000) is significant at 5 % level of significance at 5 degrees of freedom, which implies that the respondents differ significantly in their reasons for using biometric security system.

The place of biometric security can be used mostly by the respondents

Place	Frequency	Percent	Chi-Square (Sig at 5%)

Office	229	45.8	237.840
			df=4
			p=0.000

Bank/ATMs	90	18.0	
Malls/Shopping centres	79	15.8	
Temples/Tourism places	81	16.2	
Other places	21	4.2	

The percentage and chi-square analysis results on the places where the biometric security system will be used by the respondents are tabulated, it reveals that 45.8 % of the respondents may use the biometric security in their office, 18% of them in Bank/ATMs, 15.8% of them in Malls/Shopping centers, 16.2% of them in temples/tourism places and only 4.2% of them in other places. Thus, majority of the respondents (45.8%) are liked to use the biometric security at office.

Moreover, the Chi-Square value (237.840; p=0.000) reveals that there is a significant difference in the place where the respondents are mostly using the biometric security.

Influence of the personal factors over the time taken to adopt biometric security system

Sl No	Personal factors	Correlation co-efficient N= 500
1	Age	-0.034 (0.450)
2	Gender	-0.016 (0.728)
3.	Educational qualification	-0.299** (0.000)
4.	Occupational status	-0.325** (0.000)
5.	Monthly income	+0.044 (0.323)

To study the relationship between the personal factors of the respondents and the time taken to adopt biometric security system, Pearson correlation was performed and the results are tabulated. It is evident from the table that educational qualification has significant negative relationship with the time taken to adopt biometric security system as indicated by the correlation co-efficient, r=-0.299 (p=0.000). Hence, it can be inferred that higher the educational qualification, lesser will be the time taken to adopt biometric security system.

Similarly, occupational status has negative significant relationship with the time taken to adopt biometric security system which is revealed by the correlation co-efficient, r=-0.325 (p=0.000). This proves that the respondents who are professionally employed take lesser time to adopt biometric security system than the salaried in private/government and doing business.

However, the other personal factors such as age (r= -0.034; p=0.450), gender (r= -0.016; p=0.728)) and monthly income (r= +0.044; p=0.323)), do not have significant influence over the time taken to adopt biometric security system.

11. WHERE NOT TO USE BIOMETRICS?

False rejects – the unpleasant property of biometric systems causing authorized users to be rejected – may prevent biometric systems to spread into some specific applications, where inability of a user to authenticate herself (and run an action) may imply serious problems.

Few basic conclusions at the very end:

* Different biometric samples of the same person will never be same.
* Biometric data are not secret.
* The role of the input device is crucial, and this device must be trusted or well secured.
* The biometric system should check user's livens.
* Biometrics is good for user authentication.

They cannot be used to authenticate data or computers.

12. CONCLUSION

Biometric security has the potential to provide significant benefits to society. At the same time, the rapid growth and improvement in the technology could threaten individual privacy rights. The concern with balancing the privacy of the citizen against the government interest occurs with almost all law enforcement techniques. Current use of bio-security by law enforcement does not appear to run a foul of existing constitutional or legal protections.

Bio-authentication is by no means a perfect technology and much technical work has to be done before it becomes a truly viable tool to counter terrorism and crime. But the technology is getting better and there is no denying its tremendous potential. In the meantime, we, as a society, have time to decide how we want to use this new technology. By implementing reasonable safeguards, we can harness the power of the technology to maximize its public safety benefits while minimizing the intrusion on individual privacy.

REFERENCE

[1] M. H. Yang et al, "Detecting Faces in Images: A Survey", IEEE trans. on PAMI, 24(1), 34-59.

[2]. C. Yang et al, "Human face detection in complex background", Pattern Recognition 27(1), 345-350..

[3] Jain, A.; Bolle. R.; Pankanti; S. (Editors); "Biometrics: Personal Identification in Networked Society", Kluwer Academic Publishers, 1999.

[4] Lenz, J.-M.; Schmidt, C.; "Die elektronische Signatur", Deutscher Sparkassenverlag, ISBN 3093057051, 2004.

[5] Petermann, Thomas; Sauter, Arnold; "Biometrische Identifikationssysteme", TAB-Arbeitsbericht, 2002.] R. Kjeldsen et al, "Finding skin region in color images", Proc. Second Intel's Conf., Automatic Face and Gesture Recognition, 312-319.

[6] www.wrstech.com

[7] www.biosec.org

[8] GAO Report Aviation Security - Challenges in Using BiometricTechnologies
www.gao.gov/new.items/d04785t.pdf