A Perceptual Study of Biometric Authentication and its Implementation

***Dr. G. Gokulkumari**

*Associate Professor, MIS Department, Ibn Rushd College for Management Sciences, King Abdul Aziz Road - P. O. Box 447 ABHA 61411 Saudi Arabia.

Abstract

A common use of biometric systems is to authenticate users desiring access to a system or resource. Universal Access can be promoted with biometrics. Biometrics provides a secure way to access information technology, although the use of biometrics presents challenges and opportunities unique to other authentication methods. 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: Biometrics, Security system, Rendered unusable.

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.

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.

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:

1. Universality each person should have the characteristic
2. Uniqueness is how well the biometric separates individually from another.
3. Permanence measures how well a biometric resists aging.
4. Collectability eases of acquisition for measurement.

5. Performance accuracy, speed, and robustness of technology used.
6. Acceptability degree of approval of a technology.
7. Circumvention eases of use of a substitute.

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

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:

1. 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).

2. 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.

3. 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.

4. 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.

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		
Face recognition	91		
Iris recognition	92	5.540	
Voice recognition	97	df=13	
Signature / handwriting Recognition	100		
Others(Hand finger geometry, retina scan, ear canal, 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	
Threat to theft	92	df=5	
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	
Bank/ATM	90	18.0	df=4 p=0.000	
Malls/Shopping centres	79	15.8		
Temples/ Tourism places	81	16.2		
Others	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.

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 afoul 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.

References

Websites

1. Boroshok, J. (2005, January 14). Pointing the finger at biometrics *SearchSecurity.com*. Retrieved February 4, 2005 from http://www.searchsecuritytechtarget.com.

2. Chapple, M. (2003, September 30). Practical biometrics. *SearchSecurity.com*. Retrieved February 4, 2005 from http://www.searchsecuritytechtarget.com.

3. USTreasury. (2005). "The use of technology to combat Identity Theft - Report on the study conducted pursuant to section 157 of the Fair and 0.1.

Books

1. Maher, K. (2003, November 4). Big employer is watching: Companies monitor workers with high-tech systems: Did lunch take too long? *Wall Street Journal*, B1.

2. Matyáš, V. & Riha, Z. (2003, May/June). Toward reliable user authentication through biometrics. *IEEE Security & Privacy*, 45-49.

3. Uludag, U., Pankanti, S., Prabhakar, S, and A.K. Jain (2004),Biometric cryptosystems: issues and challenges, *Proceedings of the IEEE*, vol. 92, no. 6, pp. 948-960.

4. Vijayan, J. (2004, August 9). Corporate America slows to adopt biometric technologies. *Computerworld*, *38*(32), 1, 45.

5. Li S. Z. and Jain A. K., Eds., (2004) Handbook of Face Recognition. New York: Springer Verlag.

6. Ashbourn, J. (2004). *Practical biometrics: From aspiration to implementation*. London: Springer-Verlag.

7. Bolle, R.M., Connell, J.H., Pankanti, S., Ratha, N.K., & Senior, A.W. (2004). *Guide to biometrics*. New York: Springer-Verlag

8. Nixon, M.S., Carter, J.N., Grant, M.G., Gordon, L., & Hayfron-Acquah, J.B. (2003). Automatic recognition by gait: Progress and prospects. *Sensor Review, 23*(4), 323-331.

9. O'Gorman, L. (2003). Comparing passwords, tokens, and biometrics for user authentication. *Proceedings of the IEEE, 91*(12), 2021-2040.