GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

Increasing Accuracy in Multimodal Biometric Systems

GIAC Security Essentials Certification (GSEC)
Practical Assignment
Version 1.4c Option 1

Karine Pellerin

8 October 2004

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

CONTENTS

ABSTRACT **3**

1 AUTHENTICATION TECHNIQUES AND THEIR LIMITATIONS **3**

1.1 TRADITIONAL AUTHENTICATION TECHNIQUES 3
1.2 BIOMETRICS 4
1.3 MULTIMODAL BIOMETRICS 5

2 KEY CONCEPTS IN MULTIMODAL BIOMETRICS **5**

2.1 MAIN PROCESSES 5
2.2 ACCURACY METRICS 6
2.3 BASIC MULTIMODAL BIOMETRIC FUSION 8

3 CRITICAL FACTORS INFLUENCING ACCURACY **9**

3.1 CRITICAL DESIGN FACTORS 9
3.1.1 User acceptance and privacy *9*
3.1.2 Selection of biometric identifiers *10*
3.1.3 Initial accuracy *11*
3.1.4 Biometric fusion strategies *12*
3.2 CRITICAL IMPLEMENTATION FACTORS 14
3.2.1 Enrolment and verification processes *14*
3.3 CRITICAL SECURITY FACTORS 14
3.3.1 Spoofing attacks *15*
3.3.2 Replay attacks *15*
3.3.3 Biometric template attacks *16*
3.3.4 Trojan applications *16*

4 CONCLUSION **17**

5 FUTURE RESEARCH **17**

REFERENCES **18**

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Abstract

In computer systems, there is an urgent need for accurate authentication techniques to prevent unauthorized access. Authentication is the process of confirming the correctness of the claimed identity.[1] Many computers that store critical information are vulnerable to unauthorized access because of weak authentication. In some cases, the safety of the public can be at risk, such as in the case of a multi-billion dollar passenger-screening system defenceless against terrorists with forged security badges.[2]

Traditional authentication techniques such as the ubiquitous username / password method are inadequate for personal identity since they can only provide proof of possession and/or proof of knowledge. Only biometrics, the authentication of individuals using biological identifiers, can offer true proof of identity. Current research suggests that multimodal biometric systems, those that use more than one biological identifier, can improve the accuracy of biometric systems. This improvement in accuracy depends on critical factors in design, implementation and security. This paper explains each of these critical factors so the increase in accuracy observed in current research can be achieved in real-world applications.

1 Authentication techniques and their limitations

This section describes the traditional authentication techniques as well as biometrics and multimodal biometrics. The limitations of each of those techniques are discussed.

1.1 Traditional authentication techniques

The traditional authentication techniques are related to something that the individual has (possession based) or something that the individual remembers (knowledge based).

Possession is often related to an identity card, a smart card or a token. Possession based authentication techniques are limited in the sense that cards and tokens can be shared, stolen and forged. Knowledge is frequently associated with a password or a personal identification number (PIN). Knowledge based authentication techniques are problematic since individuals

[1] SANS Institute. "SANS Glossary of Terms Used in Security and Intrusion Detection." May 2003.

[2] IBIA. "Biometrics Advocacy Report." May 2004.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

frequently choose easy-to-guess passwords or PINs. Many organizations attempt to strengthen their knowledge-based systems by requiring users to remember more, longer, and changing passwords.[3] However, these policies often result in individuals writing down their passwords in unsecured places. The compromise of a password that is reused on different systems could have great ramifications.

A two-factor authentication method combining possession based and knowledge based techniques can increase slightly the level of confidence. Even with two-factor authentication, a fundamental problem remains in that only the card and the PIN are authenticated, not the actual individual who provides them.

1.2 Biometrics

Biometrics measures the unique physical and behavioural characteristics of individuals in order to verify their identity. Biometric systems are more convenient than traditional authentication techniques since there is no password to be forgotten or smart card to be lost. Biometric samples have to be provided in person and cannot be borrowed or poorly chosen.

Biometric authentication systems can be divided into two categories: biometric verification and biometric identification systems. Verification systems use a one-to-one matching process where a characteristic of an individual is compared to a previously stored biometric template associated with the claimed identity. Identification systems use a one-to-many matching process where the characteristic of the individual is compared with a database of possible users according to multiple matching criteria. The system needs to evaluate the suitability of the live biometric received and then search the entire database for a possible match.

Wide adoption of biometrics has been predicted for years, but has not yet happened mostly because a variety of problems associated with accuracy. Those problems include noise in the sensed data, intra-class variations, distinctiveness, non-universality and spoofing.[4] To meet accuracy requirements of today's applications, relying on a single biometric can be challenging. For example, tests conducted by the NIST suggest that approximately 2% of the population have friction ridges too damaged to be matched using current fingerprint technology.[5]

---

[3] O'Gorman. "Comparing Passwords, Tokens, and Biometrics for User Authentication." Dec. 2003.

[4] Jain, and Ross. "Multibiometric Systems." Jan. 2004.

[5] NIST. "Summary of NIST Standards for Biometric Accuracy, Tamper Resistance, and Interoperability." Nov. 2002.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

1.3 Multimodal biometrics

Multimodal biometric systems combine biometric identifiers to obtain a more accurate decision on a user's claim based on multiple sources of evidence. In a multimodal biometric system, each subsystem provides an opinion or a decision on the user's claim. A supervisor module combines the different opinions or decisions delivered by each subsystem then makes a final decision (accept/reject).

Research [6] [7]demonstrates how multimodal biometric systems can improve the accuracy of biometric systems. This increase is achievable because multimodal biometric systems use biometric identifiers that possess different strengths and weaknesses. Multimodal biometric systems are also more difficult to spoof for two major reasons: first, multiple biometric identifiers need to be forged in order to defeat the system; second, a multimodal biometric system that uses an changeable biometric trait like voice verification and keystroke recognition can participate in a challenge-response protocol diminishing the risk of replay attacks. While it is well understood that multimodal biometric systems can increase the accuracy of biometric systems, achieving the accuracy required for real-world applications is still a great research challenge.

2 Key concepts in multimodal biometrics

This section briefly describes the key concepts in multimodal biometrics. It explains the main processes, how accuracy is measured and how basic multimodal biometric fusion is achieved.

2.1 Main processes

There are three main processes involved in multimodal biometric systems: the enrolment process, storage of templates and the verification process.

The enrolment process consists of an individual providing a series of biometric identifiers. For example, during the enrolment of a multimodal biometric system using fingerprint and voice information, the user is requested to provide a series of fingerprints and a series of voice samples. The digital representations of the fingerprint samples are used to generate a fingerprint template using an averaging process. The voice samples are then used to create a voice template.

[6] Poh, and Korczak. "Hybrid Biometric Person Authentication using Face and Voice Features." 2001.

[7] Ross, and Jain. "Information Fusion in Biometrics." Sept. 2003.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Both templates together are associated with a unique identifier such as a PIN or a card number for future recall.

Templates collected in the enrolment process are stored so they can be referenced later. Typically, templates are either stored within the biometric device itself, in a central repository, or stored on a portable token carried by individuals.

The verification process requires the individual to claim an identity by providing either a PIN or by presenting a token. The individual needs to provide a live biometric sample of each biometric identifier, or a subset, that is part of the multimodal biometric system. The multimodal biometric system then compares each sample with the corresponding template. If the samples and the templates match within the predefined threshold, the multimodal biometric system returns a binary true or false message. Figure 1 describes the general operating methodology.

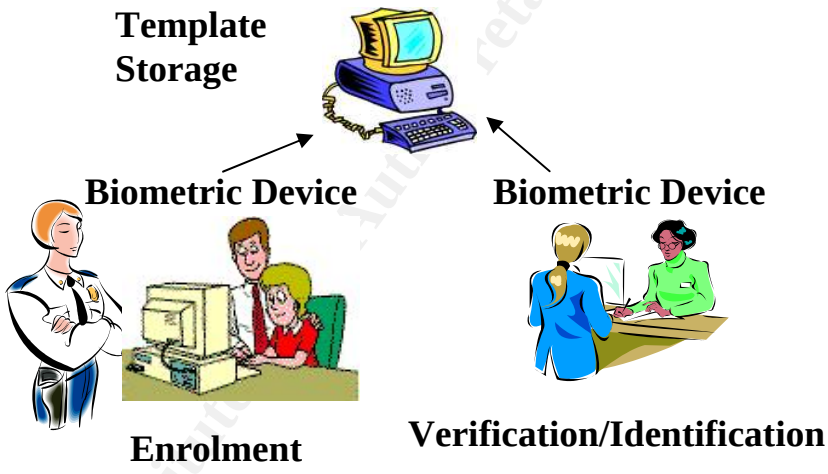


Figure 1: General operating methodology

2.2 Accuracy metrics

A password based authentication system can allow for perfect comparison of user input and the stored password hash. However, in a multimodal biometric system, limitations of the feature extractors, matching algorithms, plus noise from the biometric sensors and the environment do not allow a perfect comparison. Instead, algorithms that attempt to compensate for variations are used.

The accuracy of a multimodal biometric system is usually measured in terms of matching errors and image acquisition errors. Matching errors consist of false match rate (FMR) where an impostor is accepted and false non-match rate (FNMR) where a genuine user is denied access. Image acquisition errors

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

comprise of failure-to-enrol (FTE) and failure-to-acquire (FTA). A summary of the different biometric errors is provided in Table 1.

Table 1: Biometric errors

	Sometimes referred as	Refers to
1) Matching Errors		
False Match Rate (FMR)	False Positive Rate (FPR)	An impostor's sample matches a legitimate user's template
False Non Match Rate (FNMR)	False Negative Rate (FNR)	A legitimate user's sample does not match his/her own template
2) Image Acquisition Errors		
Failure-to-enrol (FTE)	Failure to Enrol Rate (FER)	A user that is unable to successfully enrol in a biometric system
Failure-to-acquire (FTA)		A user that is unable to provide a good quality biometric trait at verification

The summarized accuracy of a multimodal biometric system is depicted using the Detection error trade-off (DET) curve, which plots FNMR against FMR directly using logarithmic axes. The DET curve is obtained by ordering the genuine and impostor scores. As the score varies over all possible values, each point on the DET curve represents the false match and false non-match rate using that score as the decision threshold.[8] Figure 2 provides an example of the DET curve of a fingerprint subsystem. In order to obtain a high overall accuracy, a multimodal biometric system must be able to achieve a low FMR and a low FNMR.

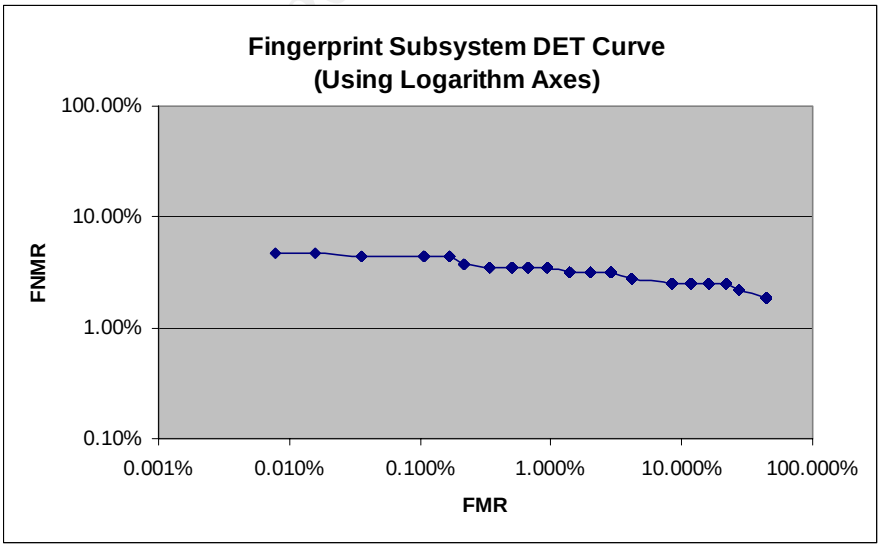


Figure 2: Example of a Fingerprint Subsystem DET Curve

[8] Mansfield, and Wayman. "Best Practices in Testing and Reporting Performance of Biometric Devices." Aug. 2002.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

2.3 Basic multimodal biometric fusion

In a multimodal biometric system, each subsystem provides an opinion or a decision on the user's claim. The supervisor module uses different fusion strategies to combine each subsystem opinion or decision and make a final decision. Fusion can use multiple representations of a single biometric, a single biometric with multiple matchers or multiple biometric identifiers.[9] Fusion can be performed at different levels: sensor level, feature level, confidence level and abstract level. Figure 3 illustrates the different levels of fusion for a multimodal biometric system using a fingerprint and a voice subsystem. Table 2 describes the basic multimodal biometric fusion techniques.

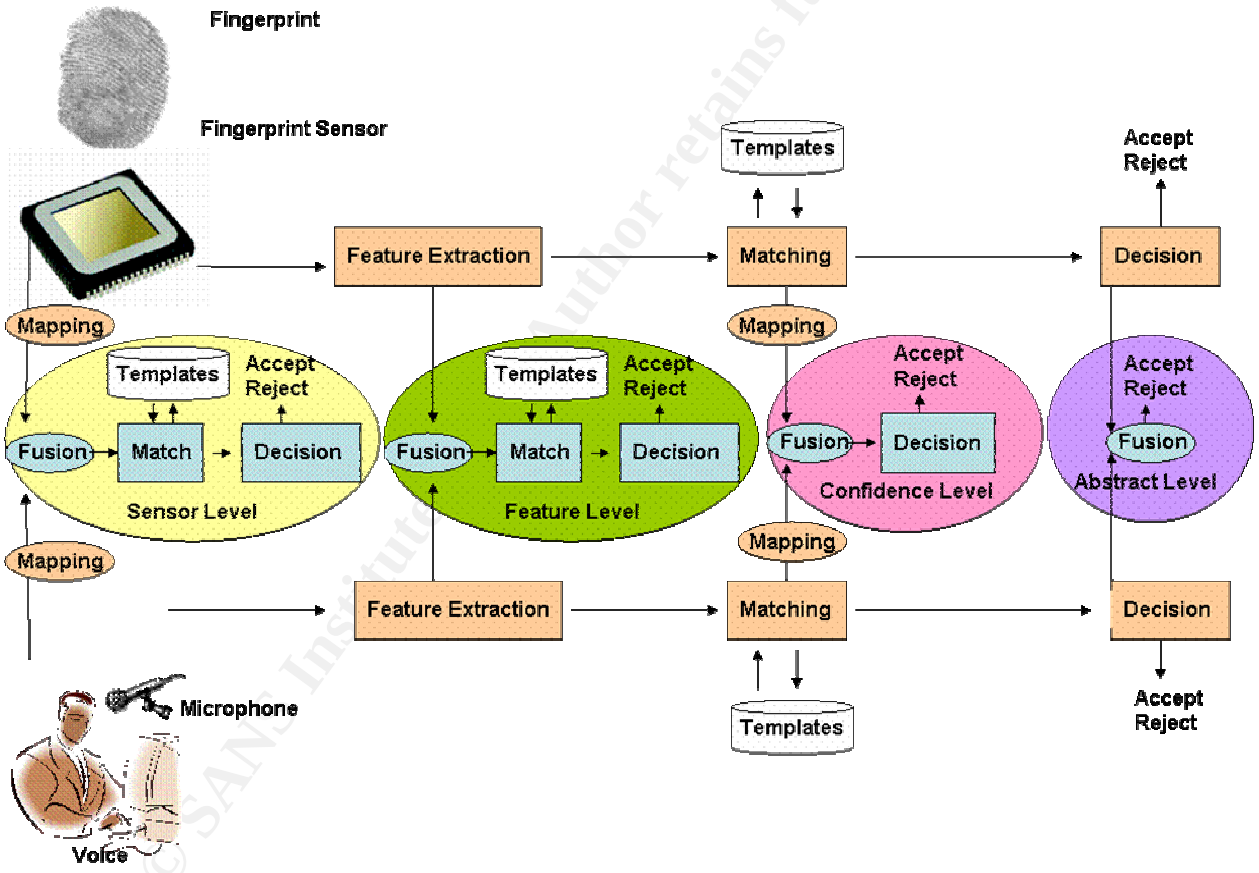


Figure 3: Levels of fusion for a multimodal biometric system

[9] Ross, and Jain. "Information Fusion in Biometrics." Sept. 2003.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Table 2: Multimodal biometric fusion techniques

Fusion Level	*Sometimes referred as*	*Refers to*
Sensor Level		The raw data of the sensors are combined.
Feature Level	Representation level fusion	The features extracted from the different sensors are concatenated to create a joint feature vector.
Confidence Level	Score level integration Measurement level integration Opinion fusion Soft decision fusion	The matching scores of each subsystem are combined using techniques such as weighted sum rule, weighted product, linear discriminant, decision tree and the Bayesian Rule.
Abstract Level	Decision fusion	The decision of the subsystems are combined using techniques such as an AND rule, OR rule and Majority Voting.

3 Critical factors influencing accuracy

This section describes the critical design, implementation and security factors influencing the accuracy of multimodal biometric systems.

3.1 Critical design factors

User acceptance, privacy, selection of biometric identifiers, initial accuracy and the fusion strategy used are critical design factors.

3.1.1 User acceptance and privacy

Care must be taken when designing a multimodal biometric verification system to ensure that desired increase in accuracy is not obtained to the detriment of other critical factors like user acceptance and privacy.

The user's interaction with the acquisition sensors greatly affects all biometric technologies. The consistency in which the biometric identifiers are presented to the sensors and the changes related to wear and tear or injuries to the identifiers will greatly affect accuracy. User familiarity, motivation, stress, tension and mood can also significantly affect the accuracy of the system.[10]

Privacy is a vital aspect of any multimodal biometric system deployment. The design of the multimodal biometric system must ensure that it does not threaten

[10] Ashbourn. Biometrics: Advanced Identity Verification, The Complete Guide. 2000.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

personal or informational privacy. Informational privacy, the right of an individual to exercise consent and control over the collection, storage, usage and disclosure of data relating to him or her,[11] can be threatened by the unauthorized collection, use and disclosure of biometric information. This includes unauthorized linkage of independent databases. Personal information should be collected only under specific conditions and for specific reasons and only be used for the purpose it was collected. Privacy is also threatened when a biometric measurement makes it possible to uncover medical conditions of individuals.[12]

3.1.2 Selection of biometric identifiers

Multimodal biometric systems are more accurate because they use identifiers with different strengths and weaknesses. "The match between a specific biometric and an application is determined depending upon the requirements of the application and the properties of the biometric characteristics."[13] By evaluating the required/desired strengths and undesirable weaknesses, one can determine a combination of biometric identifiers that will satisfy the requirements of the application. Table 3, which is adapted from "Trusted User Authentication Using Biometrics",[14] provides the strengths and weaknesses of some of the different biometric techniques. The cost described in Table 3 is related only to the equipment cost. Actual costs associated with deploying a multimodal biometric system are far greater and include equipment cost, administration, installation, training, template updates, software and testing.[15]

© SANS Institute 2004, Author retains full rights.

[11] Nanavati, et al. Biometrics: Identity Verification in a Network World. A Wiley Tech Brief, 2002.

[12] Jain, et al. "Biometrics Systems: Anatomy of Performance." Jan. 2001.

[13] Uludag, et al. "Biometric Cryptosystems: Issues and Challenges." June 2004.

[14] Xiao. "Trusted User Authentication Using Biometrics." Nov. 2002.

[15] Polemi. "Review and Evaluation of Biometric Techniques for Identification and Authentication." Apr. 1997.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Table 3: Advantages and disadvantages of the different biometric techniques

TECHNIQUE	ADVANTAGES	DISADVANTAGES	USAGE	COST
Fingerprint Scanning	• Better security • Can accommodate cuts • Less Expensive • Small • Easy to adapt • Widely accepted	• Each finger only has 50 discriminators • 2% of the population have poor fingerprints	•Law enforcement •Corporate database	$50-$1,200
Facial Recognition	• Video camera equipment is inexpensive • Unobtrusive/Passive • Allow for audits from stored face images	• Awkward lighting in the image can affect authentication • Subject to spoofing attempts	•General	$200-$3,000
Iris	• The iris remains unchanged throughout a person's life • The left and the right irises are different • Each iris has 170 discriminators • Very accurate • The iris's image can be captures from a distance	• More expensive • Subject to user motion • Large template • 15% of the population cannot have their iris scanned	•Access control •ATM •Airport	$200-$3,000
Voice Print	• Less expensive • Can be used remotely • PCs already have the necessary hardware	• Less accurate • Susceptible to rejections • Susceptible to forgery	•Industrial	$120-$1,000

3.1.3 Initial accuracy

When selecting biometric identifiers in a multimodal biometric system, the initial accuracy of the subsystems must be taken into account. Some research[16] [17] suggest that when the initial accuracy of the subsystems are significantly different, the accuracy of the multimodal biometric system as a whole can be higher than the less reliable subsystem but also lower than the more reliable one. One should also be very careful when looking at published accuracy data for the different technologies. To correctly establish accuracy, large databases of samples are required. However, large-scale databases are currently available only for fingerprint impressions and facial images. In addition, FTE and FTA accuracy metrics are rarely published. A multimodal biometric system should be able to minimize FTE and FTA. For example, if your multimodal biometric

[16] Daugman. "Combining Multiple Biometrics." No Date.

[17] Pellerin. "The Accuracy Performance of a Fingerprint/Voice Multimodal Biometric System." Oct. 2004.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

system has a high FTE, some users may not be able to enrol. Those users will need to be provided with traditional authentication techniques such as username / password. Those accounts are now vulnerable to the numerous attacks on traditional authentication techniques. Since the resources protected by those vulnerable accounts are the same as those protected by your biometric authentication system, a hole has been created in your authentication process.

3.1.4 Biometric fusion strategies

The effectiveness of the fusion scheme greatly influences the accuracy of a multimodal biometric system.

Fusion at the sensor level is very complex and fusion at the feature level may not always be feasible. It is difficult to combine the minutia feature of a fingerprint image with the eigen-coefficients of a face image. [18] There is currently very little published about those fusion techniques. Fusion at the confidence level is often the preferred fusion technique since it is relatively easy to combine the opinions of the different subsystems.

Fusion at the confidence level can adjust the weight assigned to each subsystem to arrive at a more accurate decision. This can be achieved using a non-adaptive approach or an adaptive approach. In a non-adaptive approach, the weight of each subsystem is based on the subsystem's bias. In a multimodal biometric system with a fingerprint and voice subsystems, the initial accuracy of the fingerprint subsystem could be higher than the voice subsystem. Therefore, a higher weight can be assigned to the fingerprint subsystem.

An adaptive approach is where the contribution of at least one subsystem varies on the user's identity claim or the environment. Research clearly demonstrates the benefits of assigning weight to subsystems depending on user-specific parameters as opposed to parameters common to all.[19] By computing a matching threshold for each user using cumulative histograms of impostor's scores for each biometric trait, an increase in accuracy was observed when using a user-specific threshold versus a common threshold. Also, by learning user-specific weight for each trait, a low weight could be assign to a less reliable trait and a higher weight to a more reliable one. It was demonstrated that the error rates were reduced for that particular individual. The weight of each subsystem can also be assigned depending on the environment. For a multimodal biometric system combing fingerprint and speech information, the system can lower the weight associated to the speech subsystem when the signal to noise ratio is low.

[18] Jain, and Ross. "Multibiometric Systems." Jan. 2004.

[19] Jain, and Ross. "Learning User-specific Parameters in a Multibiometric System." Sept. 2002.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

A secure and user-friendly multimodal biometric system was proposed in September 2004.[20] It uses a sequential fusion based on the sequential probability ratio test (SPRT). The sequential fusion stops when the verification process has enough evidence to accept or reject an individual. Each time a biometric identifier is presented, a probability ratio is calculated. The system will accept the user when the probability ratio is equal or below the threshold. When the number of inputs reaches the maximum allowed and the probability ratio is still above the threshold, the user is rejected.

New methods are currently being researched. A fuzzy logic decision fusion will be presented in October 2004. [21] This new method accounts for external conditions that affect accuracy. The fuzzy interference system uses input variables that can assign a confidence value when allocated to defined fuzzy sets. For example, a fingerprint impression (input variable) can be assigned a confidence value for each of the defined fuzzy set it belongs to. Examples of fuzzy sets for fingerprint impressions are CorePosX, CorePosY, Darkness and Low-clarity. If the x-coordinate (CorePosX) of the provided fingerprint impression falls in the preferred external condition of the Gaussian distribution for the CorePosX fuzzy set, then a high confidence value can be set for that fingerprint impression. The fuzzy rule is achieved by a set of IF-THEN rules. Initial research suggests that the fuzzy logic decision fusion can adapt well to external conditions and achieve an improvement in accuracy.

Another key aspect of fusion is normalization. When the different subsystem's opinions are fused at the confidence level, normalization or mapping to a common interval is required before the opinions can be combined. Various normalization techniques have been researched. Using a simple summation fusion, the min-max normalization technique obtained the best accuracy.[22] A new method called adaptive normalization has been proposed.[23] This adaptive normalization approach uses the Quadric-Line-Quadric (QLQ) mapping function. It does not modify the overlapped zone where errors occur but map the region of genuine and impostor distributions with two quadratic function segments. The experiment shows that for application that deals with closed populations this adaptive normalization approach obtains the best results when used with a user weight fusion approach.

[20] Systems Development Laboratory. "A Secure and User-friendly Multi-Modal Biometric System." Apr. 2004.

[21] Lau, et al. "Fuzzy Logic Decision Fusion in a Multimodal Biometric System." Oct. 2004.

[22] Snelick, et al. "Multimodal Biometrics: Issues in Design and Testing." Nov. 2003.

[23] Indovina, et al. "Multimodal Biometric Authentication Methods: A COTS Approach." Dec. 2003.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

3.2 Critical implementation factors

The best multimodal biometric system can be extremely inaccurate if the critical implementation factors are not taken into account. The enrolment and verification processes play a critical role in the accuracy of a multimodal biometric system.

3.2.1 Enrolment and verification processes

Even with a highly accurate multimodal biometric system in theory, the accuracy of a real-life scenario may be very poor if the enrolment and verification processes are not carefully conducted. During enrolment, the identity of the individual must be confirmed to avoid identity theft. A highly trusted authentication document must be required to enrol an individual into a multimodal biometric system. Since the biometric live samples taken at enrolment will be the basis for templates creation, their quality is vital. Without good quality templates, the accuracy of subsequent verifications will be greatly reduced. To ensure good templates quality, the enrolment process must include a training session on how to present the live samples to the different biometric sensors. The application should also have a process that allows poor quality live samples to be rejected.

The quality of the live samples captured during verification is also important. Noisy inputs, different environmental factors like background noise, lighting conditions could have a great impact on accuracy. One area that has not been researched until now is sensor interoperability. When the sensors used for enrolment are different then the sensors used for verification, the accuracy can be significantly affected.[24] The cost associated with re-enrolling all your users because the sensors used during enrolment are not available on the market anymore could be prohibitive.

3.3 Critical security factors

A multimodal biometric system will only be as good as its weakest link. The accuracy of a multimodal biometric system is highly dependant on each of its components' security. The vulnerabilities associated with multimodal biometric authentication must be well understood to ensure that impostors cannot circumvent the system. The remainder of this section discusses some of the most common attacks on multimodal biometric systems.

[24] Ross, and Jain. "Biometric Sensor Interoperability: A Case Study in Fingerprints." May 2004.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

3.3.1 Spoofing attacks

Spoofing is the biggest threat to authentication systems. Multimodal biometric systems are vulnerable to spoofing. Spoofing occurs when an unauthorized user is able to masquerade as an authorized user. Research evaluated eleven biometric applications including capacitive, optical and thermal fingerprint technologies, iris-scan technology and face recognition.[25] Using different attacks, they were able to outwit all the systems tested with simple means.

The potential threats caused by fake or artificial fingers were also evaluated.[26] The experiment demonstrated that artificial fingers cloned with plastic molds could enrol in the 11 tested fingerprint systems and were accepted in the verification procedures with the probability of 68-100% depending on the system. Artificial fingers cloned from residual fingerprints could also enrol in all the systems and were accepted in the verification procedures with a probability higher than 67%. The "gummy" fingers were created with cheap and readily available gelatine.

Using biometric sensors that provide "liveness" detection can minimize spoofing. "Liveness" refers to the ability of a multimodal biometric system to differentiate between a living and a fake sample and is usually done by measuring biometric features like pulse, humidity, temperature etc. Multimodal biometric systems are more difficult to spoof than biometric system since multiple biometric identifiers need to be forged in order to defeat the system.

3.3.2 Replay attacks

Biometric information must be converted to digital data to be processed by the multimodal biometric system. The data transmitted over the network is susceptible to eavesdropping. An attacker could potentially obtain the biometric information between the verification device and the multimodal biometric system. This stolen biometric information can be electronically injected later to fool the system. Encrypting the information between the verification device and the system solve the confidentiality issue but does not prevent replay attack as an attacker can replay the encrypted information. To prevent replay attacks, a nonce can be combined with the biometric templates before it is encrypted and sent to the multimodal biometric system. Access to resources should only be provided if the nonce is the same and if the similarity between the templates provided and the templates stored in the central repository is within acceptable range. Multimodal biometric systems are better than biometric systems since

[25] Thalheim, et al. "Body check: Biometric access protection devices and their programs put to the test." 22 May 2002.

[26] Matsumoto, et al. "Impact of artificial "gummy" fingers on fingerprint systems." 2002.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

they can participate in a challenge-response protocol diminishing the risk of replay attacks. Biometric sensors that are not cleaned on a regular basis are vulnerable to residual image attacks. Physical residual biometric images can sometime be reactived and provide access to resources.

3.3.3 Biometric template attacks

The integrity and confidentiality of the biometric templates stored in the central repository is critical. If biometric templates are compromised, they are not as easily replaceable as password and tokens. In traditional authentication systems, passwords are often hashed using a cryptographic hash function before they are store in a database. Since cryptographic hash functions are irreversible, it prevents an attacker from obtaining the original passwords directly from hash values. In multimodal biometric systems, it is not possible for the hash value of a live biometric sample provided at verification to equal the hash value of the template store in the database. Once again, this is due to the fact that biometrics relies on "closeness" between the template and the live biometric sample, not an exact match. Biometric templates stored in a central repository can therefore only be encrypted using a reversible algorithm. If an attacker is able to obtain a database of encrypted biometric templates and the decryption key, biometric templates can be retrieved. Security mechanisms must also ensure that an attacker cannot inject their own template in the database or replace templates already stored in the central repository. If an attacker is able to inject his own biometric template, future authentications will be successful. Digitally signing the biometric templates at enrolment can ensure the integrity and the authenticity of the biometric templates stored in the central repository.

3.3.4 Trojan applications

A Trojan horse application installed in the capturing device could yield an accept decision to all attempts. Client security must ensure that no rogue application can be installed. Having the capturing device authenticate itself to the multimodal biometric system could minimize this type of attack.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

4 Conclusion

Traditional authentication techniques are inadequate for user authentication. The insufficient accuracy of biometric systems has lead researchers to multimodal biometric systems to provide highly accurate authentication. The accuracy obtained in research can only be achievable in real-world applications if several critical factors are considered.

In designing a multimodal biometric system, biometric identifiers must be selected based on the application requirements, user acceptance and privacy. The initial accuracy of the subsystems is critical since a subsystem with poor accuracy can negate the benefits obtained from multimodal biometrics. Fusion at the confidence level is often the favourite fusion technique since the weight of each subsystem can be adjusted using user-specific or/and environment parameters. New promising biometric fusion techniques and adaptive normalization techniques are currently being researched. The enrolment and verification processes are key implementation factors. Multimodal biometric systems are vulnerable to several attacks. Understanding those vulnerabilities and potential safeguards will minimize the risks to resources protected by multimodal biometric systems.

5 Future research

More research is needed to understand how one biometric measurement from an individual is related to another biometric measurement of the same person. Research assumes that they are statistically independent but it has yet been confirmed.[27] [28] [29] If they are statistically dependent, randomly combining biometric identifiers to obtain virtual subjects for testing may not be appropriate.

Very little research has been conducted on biometric sensor interoperability.[30] More research is needed to clearly understand how the use of different sensors for enrolment and verification affects system accuracy.

Finding the most effective way to fuse independent subsystem opinions into a more accurate decision to improve system accuracy is a significant research challenge.

---

[27] Ross, and Jain. "Information Fusion in Biometrics." Sept. 2003.

[28] Jain, et al. "Biometrics Systems: Anatomy of Performance." Jan. 2001.

[29] Snelick, et al. “Multimodal Biometrics: Issues in Design and Testing.” Nov. 2003.

[30] Ross, and Jain. “Biometric Sensor Interoperability: A Case Study in Fingerprints.” May 2004.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

References

Ashbourn, Julian. Biometrics: Advanced Identity Verification, The Complete Guide. London: Springer, 2000. 73-78.

Daugman, John. “Combining Multiple Biometrics.” No Date.
URL: http://www.cl.cam.ac.uk/users/jgd1000/combine/combine.html (23 Sept. 2004).

Indovina, Michael, Umut Uludag, Robert Snelick, Alan Mink, and Anil K. Jain. “Multimodal Biometric Authentication Methods: A COTS Approach." Proceedings of the MMUA 2003. 11-12 December 2003.
URL: http://biometrics.cse.msu.edu/Multimodal-Biometric-MMUA-CONF.pdf (23 Sept. 2004).

International Biometric Industry Association. “Biometrics Advocacy Report.” Vol. VI, No. 9. 21 May 2004. URL: http://www.ibia.org/newslett040521.htm (23 Sept. 2004).

Jain, K. Anil, and Arun Ross. “Learning User-specific Parameters in a Multibiometric System.” Proceedings of the International Conference on Image Processing. September 2002.
URL: http://biometrics.cse.msu.edu/JainRossICIP2002.pdf (23 Sept. 2003).

Jain, K. Anil, and Arun Ross. "Multibiometric Systems." Communications of the ACM, Special Issue on Multimodal Interfaces, Vol. 47, No. 1. January 2004.
URL: http://biometrics.cse.msu.edu/RossMultibiometric_CACM04.pdf (23 Sept. 2004).

Jain, K. Anil, Arun Ross, and Sharath Pankanti. "Biometrics Systems: Anatomy of Performance." IEICE Transactions Fundamentals, Vol. E00-A, No. 1. January 2001. URL: http://researchweb.watson.ibm.com/ecvg/pubs/sharat-ieice.pdf (23 Sept. 2004).

Lau, Chun Wai, Bin Ma, M. Helen Meng, Y.S Moon, and Yeung Yam, “Fuzzy Logic Decision Fusion in a Multimodal Biometric System.” To appear in the Proceedings of the 8th International Conference on Spoken Language Processing. October 2004.
URL: http://www.se.cuhk.edu.hk/hccl/publications/pub/lau_icslp2004.pdf (23 Sept. 2004).

Mansfield, Tony, and L. James Wayman. “Best Practices in Testing and Reporting Performance of Biometric Devices.” August 2002.
URL: http://www.cesg.gov.uk/site/ast/biometrics/media/BestPractice.pdf (25 Sept. 2004).

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Matsumoto, Tsutomu, Hiroyuki Matsumoto, Koji Yamada, and Satoshi Hoshino. "Impact of artificial "gummy" fingers on fingerprint systems." Proceedings of SPIE, Vol. 4677. 2002.
URL: http://www.totse.com/en/bad_ideas/locks_and_security/164704.html 28 Sept. 2004).

Nanavati, Samir, Micheal Thieme, and Raj Nanavati. Biometrics: Identity Verification in a Network World. A Wiley Tech Brief, New-York: Wiley Computer Publishing, 2002.

National Institute of Standards and Technology. "Summary of NIST Standards for Biometric Accuracy, Tamper Resistance, and Interoperability." 13 November 2002.
URL: ftp://sequoyah.nist.gov/pub/nist_internal_reports/NISTAPP_Nov02.pdf (23 Sept. 2004).

O'Gorman, Lawrence. "Comparing Passwords, Tokens, and Biometrics for User Authentication." Proceedings of the IEEE, Vol. 91, No. 12. December 2003.
URL: http://www.research.avayalabs.com/user/logorman/compareAuthent.pdf (24 Sept. 2004).

Pellerin, Karine. "The Accuracy Performance of a Fingerprint/Voice Multimodal Biometric System." To appear in the Proceedings of the 1st NATO Biometric Workshop. Oct. 2004.

Poh, Norman, and Jerzy Korczak. "Hybrid Biometric Person Authentication using Face and Voice Features." Proceedings of the Audio and Video-based Person Authentication. 2001.
URL: http://www.idiap.ch/~norman/myphp/data/avbpa01_poh.pdf (25 Sept. 2004).

Polemi, Despina. "Review and Evaluation of Biometric Techniques for Identification and Authentication." April 1997.
URL: http://www.cordis.lu/infosec/src/stud5fr.htm (25 Sept. 2004).

Ross, Arun, and Anil K. Jain. "Biometric Sensor Interoperability: A Case Study in Fingerprints." Proceedings of the International ECCV Workshop on Biometric Authentication, Vol. 3087. May 2004.
URL: http://biometrics.cse.msu.edu/RossInter_BIOAW04.pdf (23 Sept. 2004).

Ross, Arun, and Anil K. Jain. "Information Fusion in Biometrics." Pattern Recognition Letters, Vol. 24, Issue 13. September 2003.
URL: http://biometrics.cse.msu.edu/RossFusion_PRL03.pdf (23 Sept.2004).

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Snelick, Robert, Mike Indovina, James Yen, and Alan Mink. “Multimodal Biometrics: Issues in Design and Testing.” Proceedings of Fifth International Conference on Multimodal Interfaces. November 2003.
URL: http://w3.antd.nist.gov/pubs/ICMI_submit_4_23_03.pdf (24 Sept. 2004).

SysAdmin, Audit, Network, Security (SANS) Institute. “SANS Glossary of Terms Used in Security and Intrusion Detection.” May 2003.
URL**:** http://www.sans.org/resources/glossary.php (23 Sept. 2004).

Systems Development Laboratory. “A Secure and User-friendly Multi-Modal Biometric System.” SPIE Defense and Security Symposium. April 2004.
URL: http://www.sdl.hitachi.co.jp/english/news/04/dss04/ (23 Sept. 2004).

Thalheim, Lisa, Jan Krissler, and Peter-Micheal Ziegler. “Body check: Biometric access protection devices and their programs put to the test.” 22 May 2002.
URL: http://www.heise.de/ct/english/02/11/114/ (28 Sept. 2004).

Uludag, Umut, Sharath Pankanti, Salil Prabhakar, and Anil K. Jain. "Biometric Cryptosystems: Issues and Challenges." Proceedings of the IEEE, Vol. 92, No. 6. June 2004.
URL: http://biometrics.cse.msu.edu/Uludagetal_Cryptosystems_ProcIEEE04.pdf (23 Sept. 2004).

Xiao, Qinghan. “Trusted User Authentication Using Biometrics.” November 2002.
URL : http://cradpdf.drdc-rddc.dnd.ca/PDFS/CAN1/p518641.pdf (23 Sept. 2003).

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.