Security of Biometric Authentication Systems

Parvathi Ambalakat

ABSTRACT

Biometric based authentication, the science of using physical or behavioral characteristics for identity verification is becoming a security mainstay in many areas. Their utilization as an authentication technology has become widespread from door access to e-commerce especially after the September 11th terrorist attacks. This paper examines the major forms of known attacks against biometric systems such as Spoofing, Replay attacks and Biometric template database attacks. Biometric systems that use face, fingerprints, iris and retina are used for the study. A literature study of the attack points in each of the biometric system and the various methods to combat the attacks at these points is conducted and analyzed in this paper. The methods covered are Liveness detection mechanisms, Challenge-Response systems, Steganographic and Watermarking techniques, Multimodal biometrics, Soft biometrics and Cancelable biometrics. Each mechanism is explained in detail. Potentials and weaknesses of the methods are shown and discussed. The effectiveness of the solutions is measured in terms of the various security metrics like cost, amount of effort, practicality, etc. The results of the study indicate that spoofing attacks are a still a major threat to the biometric systems. Liveness detection mechanisms are easily defeated in the case of face and fingerprints, while iris and retina systems are very resistant to spoofing attacks. The systems that use watermarking techniques suffer from the lack of algorithms to deal with image degradation introduced by the watermarks. Although soft biometrics like gender, age color, race etc can be used to improve the speed of biometric matching through efficient filtering of the database for candidate templates, there exists no real accepted mechanisms for automatic extraction of soft biometric characteristics.

1. INTRODUCTION

Biometrics comes from the Greek words bios (Life) and metricos (Measure) [11]. It is basically a pattern-recognition system that is used to identify or verify users based on his on her unique physical characteristics.

Biometric systems offer several advantages over traditional authentication methods. Biometric information cannot be acquired by direct covert observation. It is impossible to share and difficult to reproduce. It enhances user convenience by alleviating the need to memorize long and random passwords. It protects against repudiation by the user. Biometrics provides the same level of security to all users unlike passwords and is highly resistant to brute force attacks. Moreover, biometrics is one of the few techniques that can be used for negative recognition where the system determines whether the person is who he or she denies to be. Using biometrics with password protected smart cards introduces all three factors of authentication simultaneously (something you know, something you have and something you are).

1.1 Basic structure of a biometric system

Every biometric system consists of four basic modules:

1.1.1 Enrollment Unit

The enrollment module registers individuals into the biometric system database. During this phase, a biometric reader scans the individual's biometric characteristic to produce its digital representation.

1.1.2 Feature Extraction Unit

This module processes the input sample to generate a compact representation called the template, which is then stored in a central database or a smartcard issued to the individual.

1.1.3 Matching Unit

This module compares the current input with the template. If the system performs identity verification, it compares the new characteristics to the user's master template and produces a score or match value (one to one matching). A system performing identification matches the new characteristics against the master templates of many users resulting in multiple match values (one to many matching).

1.1.4 Decision Maker

This module accepts or rejects the user based on a security threshold and matching score.

1.2 Biometric System Performance

The performance evaluation of a biometric system depends on two types of errors – matching errors and acquisition errors. The matching errors consist of the following:

1.2.1 False Acceptance Rate (FAR)

Mistaking biometric measurements from two different persons to be from the same person.

1.2.2 False Rejection Rate (FRR)

Mistaking biometric measurements from the same person to be from two different persons.

The acquisition errors consist of the following:

1.2.3 Failure to Capture Rate (FTC)

Proportion of attempts for which a biometric system is unable to capture a sample of sufficient quality.

1.2.4 Failure to Enroll Rate (FTE)

Proportion of the user population for which the biometric system is unable to generate reference templates of sufficient quality. This includes those who, for physical or behavioral reasons, are unable to present the required biometric feature.

All of the above are used to calculate the accuracy and performance of a biometric system.

Biometric systems like any authentication system are not completely foolproof. It has its own drawbacks. While a biometric

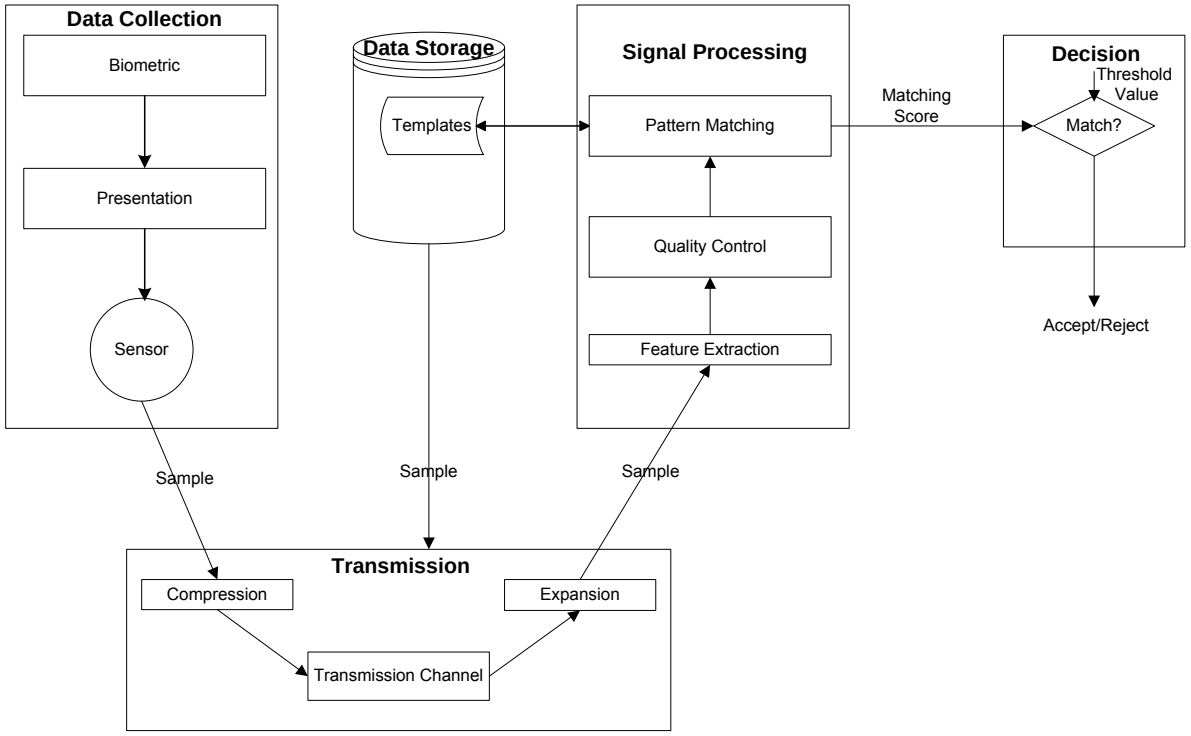

Figure 1: Basic Structure of a Biometric Authentication System. [6]

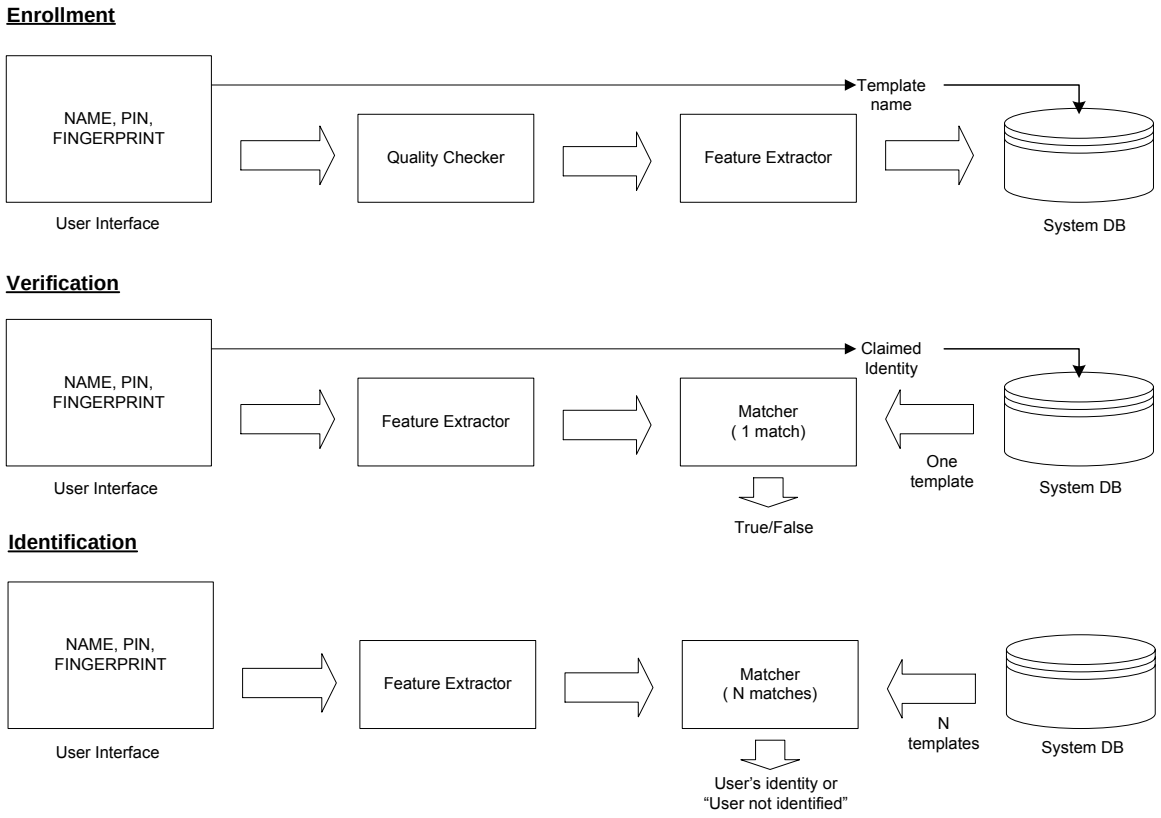

Figure 2: Enrollment, Identification and Verification in a Biometric System. [4]

is a unique identifier, it is not a secret and biometrics, once lost is lost forever (Lack of secrecy and non-replaceability).

In this paper, the known attacks against biometric systems that are based on fingerprints, face, iris and retina are discussed and several solutions are proposed. In the next section, "Known attacks on biometric systems" the vulnerable points in a biometric system and all forms of attacks are discussed in detail. In the following section, "Known technologies to resist the attacks" different solutions to resist attacks are presented. The section "Comparative evaluation" discusses the advantages and disadvantages of each of the techniques presented in the previous section. The final section, Conclusion recapitulates the issues discussed and summarizes the proposed new approaches.

2. Known Attacks on a Biometric System

Biometrics work well only if the verifier can verify two things:

- The biometric came from the genuine person at the time of verification.
- The biometric matches the master biometric on file [11].

But a variety of problems hinder the ability to verify the above [8].

- Noise in acquired data – Noisy biometric data caused by defective sensors, defective physical characteristics and unfavorable ambient conditions. This causes the data to be incorrectly matched or incorrectly rejected.
- Intra-class variations – The data acquired during authentication may be different from the data used to generate the template during enrollment, affecting the matching process.
- Distinctiveness – Every biometric trait has an upper bound in terms of its discrimination capabilities.
- Non-universality – A subset of the users not possessing a particular biometric.

The above-mentioned problems form the basis for many types of attacks against biometric systems.

There are 8 points in a generic biometric system which can be attacked [9].

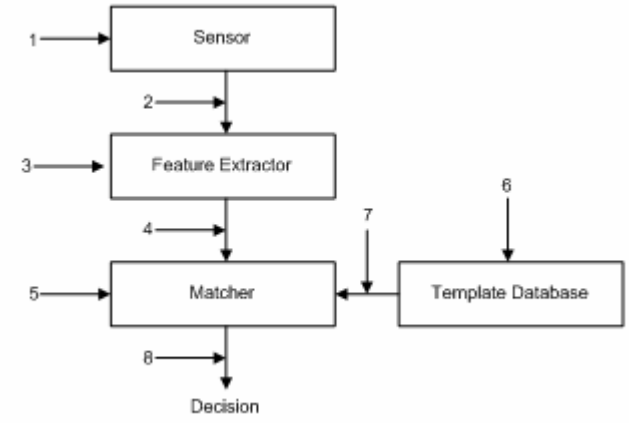

Figure 3: Attack Points in a Biometric System. [5]

2.1 Attacking the Sensor

In this type of attack a fake biometric such as a fake finger or image of the face is presented at the sensor.

2.2 Resubmitting Previously Stored Digitized Biometric Signals

In this mode of attack a recorded signal is replayed to the system bypassing to the sensor.

2.3 Overriding the Feature Extractor

The feature extractor is forced to produce feature sets chosen by the attacker, instead of the actual values generated from the data obtained from the sensor.

2.4 Tampering With the Biometric Feature Representation

The features extracted using the data obtained from the sensor is replaced with a different fraudulent feature set.

2.5 Corrupting the Matcher

The matcher component is attacked to produce pre-selected match scores regardless of the input feature set.

2.6 Tampering With the Stored Templates

Modifying one or more templates in the database, which could result either in authorizing a fraud or denying service to the person, associated with the corrupted template. A smart card based system where the template is stored in the smart card is also vulnerable to this form of attack.

2.7 Attacking the Channel Between the Stored Template and the Matcher

Data traveling from the stored template to the matcher is intercepted and modified in this form of attack.

2.8 Overriding the Final Decision

Here the final match decision is overridden by the hacker disabling the entire authentication system.

3. Known Technologies To Resist the Attacks

3.1 Liveness Detection Mechanisms

Liveness detection can be used to thwart the attacks at attack point: 1(attacking the sensor). Liveness detection refers to the ability of the system to distinguish between a sample feature provided by a live human being and a copy of a feature provided by an artifact. Liveness detection can be implemented using software or hardware means.

- Using extra hardware to acquire life signs like temperature, pulse detection, blood pressure etc for fingerprints and movements of the face for face recognition. Iris recognition devices can measure the involuntary papillary hippos (Constant small constrictions and dilations of the pupil caused by spontaneous movements of the Iris). The drawback is that extra hardware makes the system expensive and bulky.

- Using the information already captured to detect life signs. The only researched method is using information about sweat pores. For this a sensor that can acquire a high-resolution image is required. It is difficult to reproduce the exact size and position of the pores on an artificial mold.
- Using liveness information inherent to the biometric being obtained. For fingerprints, using a side impression near the nail, which has been enrolled earlier, can do this. The advantage is that people do not leave side impressions as latent prints and no major changes in the scanner is needed to acquire this additional information.

  A system that uses multiple instances of the same biometric can be used for liveness detection by asking the user to provide a random subset of biometric measurements, for e.g. left index finger followed by right middle finger [4].

Liveness detection can also be done through challenge-response like passing a small impulse current to the finger and capturing the fingers, response. Also, a new research is being done by the biomedical signal analysis laboratory at West Virginia University on an algorithm based on the detection of perspiration in a time progression of fingerprint images. Liveness detection through perspiration patterns is based on the fact that the perspiration changes the fingerprint image darkness over time. In addition to the technical procedures, procedural techniques like supervision are highly efficient for liveness detection.

3.2 Steganographic and Watermarking Techniques

Steganographic and Watermarking techniques are used to resist attacks at the attack points 2 and 7 (Channel between the sensor and feature extractor and also the channel between the stored template and the matcher). Steganography meaning secret communication, it involves hiding critical information in unsuspected carrier data. Steganography based techniques can be suitable for transferring critical biometric information from a client to a server. There are two application scenarios where hiding method is the same, but differs in the characteristics of the embedded data, host image and medium of data transfer [5].

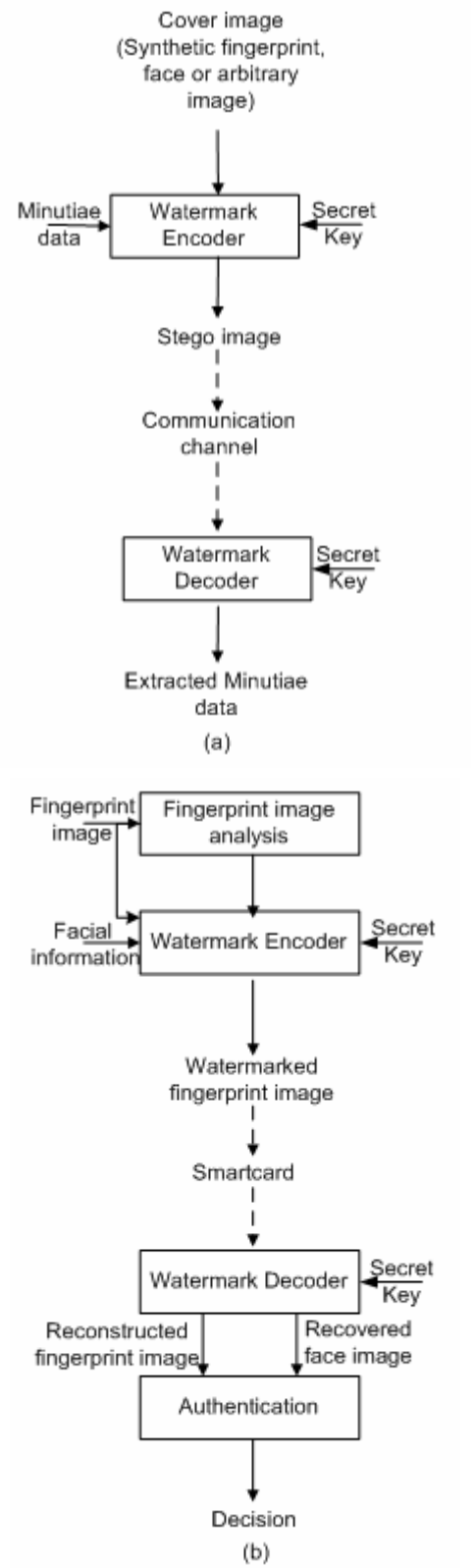

Figure 4: Steganographic (a) and Watermarking (b) techniques. [5]

In the first scenario the biometric data that need to be transmitted is hidden in a host or carrier image whose only function is to carry the data. The carrier image can be a synthetic fingerprint image, a face image or any arbitrary image. Using such a synthetic image to carry actual fingerprint data provides good security since the person who intercepts the carrier image might treat that image as the real fingerprint image. The security of transmission can be further increased by encrypting the stego image before transmission.

In the second scenario an additional biometric (e.g. Face) is embedded into another biometric (e.g. Fingerprint) in order to increase the security of the latter and stored on a smart card. At the access control site, the fingerprint of the person is compared to the fingerprint on the smart card. Then the face information hidden in the fingerprint is recovered and used as a second source of authenticity either automatically or by a human in a supervised biometric application.

Ratha [9] proposes a water marking technique applicable to fingerprinting images compressed with WSQ wavelet-based scheme. The discrete wavelet transform coefficients are changed during WSQ encoding by taking into consideration possible image degradation. This method is used to secure biometric authentication systems for commercial transactions against replay attacks. To achieve this, the service provider issues a different verification string for each transaction. The string is mixed with the fingerprint image before transmission. When the image is received by the service provider it is decompressed and the image is checked for a one-time verification string. Here, the message is not hidden in a fixed location, but is deposited in different places on the structure of the image so that it cannot be easily recovered.

Spatial domain water marking methods for fingerprint images and utilizing verification keys are also available. Water-marking the information in the biometric template database allows for the integrity of the contents to be verified when retrieved for matching.

3.3 Challenge-Response Systems

Challenge-Response systems can be used to prevent replay attacks at attack points 2 and 7. One approach is the image based challenge-response method where the challenge is presented to the sensor and the response string computed depends on the challenge string and the content of the input image acquired [9].

In another approach the verification data to be transferred to the smart card for on-card matching is protected with a cryptographic checksum that is calculated within a security module controlled by a tamper resistant card terminal with integrated biometric sensor [14].

3.4 Multi-modal Biometric Systems

Multi-modal biometric systems can be used to resist spoofing attacks (attacks at point 1). Multi-modal Biometric systems use multiple representations of a single biometric, a single biometric with multiple matchers or multiple biometric identifiers [4]. These systems can address the problem of non-universality since multiple traits can ensure sufficient population coverage. They can be used to counteract spoofing attacks, since it is difficult for a hacker to simultaneously spoof multiple biometric traits of a legitimate user. The choice and the number of biometric traits is decided by the nature of the application, the computational demands and costs introduced, and the correlation between the traits considered. The fusion of the multiple traits can be done at the feature extraction level, the matching score level or the decision level. At the feature extraction level, the feature sets of multiple bimodalities are combined to generate a new one, which is then used in matching and decision-making. At the matching level, the scores produced by each biometric subsystem are integrated using different techniques like weighted averaging to generate a new score which is then compared with the threshold to make the accept or reject decision. At the decision level each biometric system makes its own decision and a majority-voting scheme is used to make the final decision. Usually fusion at the matching score level is preferred because different biometric traits can be given varying degrees of importance based on their strength and weaknesses for different users. The problem of noise in the acquired data can be reduced by using multi-modal biometrics and assigning different degrees of importance for the different traits. This, in turn, results in improved matching performance and accuracy that makes spoofing attacks more difficult. Since the multi-modal biometric system introduces computational and cost overheads, the cost versus performance trade-off should be studied before deploying these systems.

3.5 Soft Biometrics

Soft biometrics can be used to thwart attacks at the attack points 1 and 8 (attacks on the sensor and decision maker). Soft Biometric traits are those characteristics that provide some information about the individual, but lack the distinctiveness or permanence to sufficiently differentiate any two individuals (gender, ethnicity, age, height, weight etc) [3]. Most of the biometric systems collect ancillary information about the users during enrollment, which is stored either in the database or in the smart card possessed by the user. The ancillary information collected together with the matching scores will lead to the correct identification of the user, which in turn prevents spoofing. The factors like age, gender, color, etc can affect the performance of a biometric system. The use of soft biometric traits helps to filter a large biometric database to get a reduced number of templates to do the comparison with, which in turn, will improve the speed and efficiency of the biometric system.

Soft biometric traits can also be used for tuning the parameters of a biometric system like the threshold on the matching score in a unimodal system, and the thresholds and weighing of different modalities in a multi-modal biometric system to obtain the optimum performance for a particular user or class of users. Incorporating soft biometrics will reduce FAR and FRR errors which in turn prevents spoofing.

3.6 Cancelable Biometrics

Cancelable biometrics can be used to resist attacks at point 6 (template database). Cancelable biometrics involves an intentional repeatable distortion of a biometric signal based on a chosen non-invertible transform [9]. This reduces the stored template compromise by using the legitimate substitution of a transformed version of a template for matching against a similarly transformed vector. Cancelable biometrics also addresses the issue of non-replaceability of biometric systems. Here, cancellation simply requires the specification of a new distortion transform.

The distortion transforms selected are non-invertible so that the original biometric cannot be recovered even if the transform function and the transformed biometric data are known. The transform can be applied to the acquired signal or the features

extracted from it. Signal level transforms include grid morphing and block permutation. Feature level transform is usually a set of random, repeatable permutations of feature points. Cancelable biometrics is especially useful when an individual user is subscribed to multiple services. Here, privacy and security are enhanced because different distortions can be used for different services and true biometrics are never stored or revealed to the authentication server.

4. Comparative Evaluation

There are three major criteria for the evaluation of biometric systems:

- Performance: This is measured by the achievable identification accuracy, which depends on the FAR and FRR, speed and robustness.
- Acceptability: Extend to which people are willing to accept the method in their daily lives.
- Circumvention: This is measured based on, how easy it is to fool the system.

The other factors are universality (Do all people have it?), distinctiveness (How well people can be distinguished using the biometric), permanence (How much does the biometric vary over time), and collectabiltiy (How well can the biometric identifier be captured and quantified) [5].

For fingerprints, universality is medium compared to iris, retina and face because there are a significant number of people without fingers in the world. The acceptability is high for face recognition systems because people can be easily photographed without requiring them to look into infrared light while remaining in a specific position as required in the case of systems using retina and iris. The circumvention is high for face and fingerprints because these systems can be easily spoofed. Biometric systems using iris and retina have the best performance since the FRR and FAR rates are very low for these identifiers.

The following table will provide a comparison of various biometric systems.

Table 1: Comparison of biometric characteristics. (H=high, M=medium, L=low)

Biometric Identifier	Universality	Distinctiveness	Permanence	Collectabilty	Performance	Acceptability	Circumvention
Fingerprint	M	H	H	M	M	M	H
Face	H	L	L	H	L	H	H
Iris	H	H	H	M	H	L	L
Retina	H	H	H	L	H	L	L

The next table gives a comparison of the advantages and drawbacks of the different techniques to prevent attacks discussed in this paper.

Table 2: Advantages and drawbacks of the different protection techniques.

Technique	Advantages	Drawbacks
Liveness Detection	Resists spoofing attacks.	Increased cost for the extra hardware and software, user inconvenience and increased acquisition time.
Watermarking	Prevents replay attacks and provide integrity of the stored templates.	Problem of image degradation and lack of algorithms to deal with it.
Soft Biometrics	Provides improved performance through filtering and tuning of parameters.	Lack of techniques for automatic extraction of soft biometric techniques.
Multi-modal Biometrics	Improves performance, resists spoofing and replay attacks and provides high population coverage.	Increased system complexity, computational demands and costs.

5. Conclusion

There is no security system that is completely foolproof. Every system is breakable with an appropriate amount of time and money. The techniques used to prevent the attacks help to increase the time, and cost of money. Fingerprints can be easily discovered from touched surfaces and can be copied in a small amount of time using readily available materials. All the liveness detection mechanisms in fingerprint systems can be easily defeated using wafer thin gelatin and silicon artificial fingerprints as illustrated by the Japanese cryptographer, Matsumoto [7] and a student thesis in Linkoping University, Sweden [10]. The liveness detection in face recognition systems can also be defeated using video clips of faces and playing them back. But it is very difficult to fake the iris and retina systems because they use physiological reactions to changing illumination conditions for liveness detection. A physical modeling of the eye or implanted iris device will be needed to defeat them which are very hard and expensive. Also a fake iris printed on a contact lens can be easily detected using a check to see special properties introduced by the printing. So iris and retina systems can be used for high security applications and network security. But iris and retina systems are very expensive and their user acceptability is low compared to face and fingerprint recognition systems. This makes them a bad choice for common applications. Biometric systems using fingerprints and face are sufficiently robust to be used as an authentication system for time and attendance and access control for low security systems. In my opinion, biometric systems can be used to supplement the existing technologies rather than replacing them completely, to provide a highly secure user authentication. No biometric system is optimal. The decision to which biometric is to be used should be made on the basis of the type of application and the level of security needed.

6. ACKNOWLEDGMENTS

My thanks to Professor Roger Brown and Professor Lynn DeNoia for providing support and guidance for completing this paper.

7. REFERENCES

[1] Ailisto, Heikki, Mikko Lindholm, Satu-Marja Mäkelä, Elena Vildjiounaite, "*Unobtrusive user identification with light biometrics*", Proceedings of the third Nordic conference on Human-computer interaction, October 2004.

[2] Arndt, Craig M., "*Biometric template revocation*", Proceedings of SPIE -- Volume 5404, August 2004.

[3] Jain, Anil K., Sarat C. Dass, and Karthik Nandakumar, "*Can soft biometric traits assist user recognition?*" Proceedings of SPIE -- Volume 5404, August 2004.

[4] Jain, Anil K. and Arun Ross, "*Multibiometric systems,*" Communications of the ACM," January 2004, Volume 47, Number 1 (2004).

[5] Jain, A.K.; Uludag, U., "*Hiding biometric data*", Pattern Analysis and Machine Intelligence, IEEE Transactions on, Volume: 25, Issue: 11, Nov. 2003.

[6] Leniski, *A.C., Skinner, R.C., McGann, S.F. and Elliott, S.J*, "*Securing the biometric model,*" Security Technology, 2003. Proceedings. IEEE 37th Annual 2003 International Carnahan Conference on, 14-16 Oct. 2003.

[7] Matsumoto, Tsutomu, Hiroyuki Matsumoto, Koji Yamada, and Satoshi Hoshino, "*Impact of artificial "gummy" fingers on fingerprint systems*", Proceedings of SPIE -- Volume 4677, Optical Security and Counterfeit Deterrence Techniques IV, April 2002.

[8] Matyas, V and Riha, Z, "*Toward reliable user authentication through biometrics,*" Security & Privacy Magazine, IEEE, Volume: 1, Issue: 3, May-June 2003.

[9] Ratha, N.K., J.H. Connell, and R.M. Bolle, "Enhancing security and privacy in biometrics-based authentication systems", IBM Systems Journal, vol. 40, no. 3.

[10] Sandstrom, Marie, "*Liveness Detection in fingerprint recognition systems,"*, Linkoping University Electronic Press-Student Thesis, http://www.ep.liu.se/exjobb/isy/2004/3557/

[11] Schneier, Bruce, "*Inside risks: the uses and abuses of biometrics,*" August 1999 Communications of the ACM, Volume 42 Issue 8.

[12] Shenglin Yang, Ingrid M. Verbauwhede, "*A secure fingerprint matching technique,*" Proceedings of the 2003 ACM SIGMM workshop on Biometrics methods and applications, September 2002.

[13] Uludag. U, Pankanti. S, Prabhakar. S and Jain. A.K, "Biometric Cryptosystems: issues and challenges," Proceedings of the IEEE, Volume: 92, Issue: 6, June 2004.

[14] Waldmann, Ulrich, Dirk Scheuermann, and Claudia Eckert, "*Protected transmission of biometric user authentication data for oncard-matching,*" Proceedings of the 2004 ACM symposium on Applied computing March 2004.

[15] Williams, John Michael," *Assurance in life/nation critical endeavours: Biometrics or ... biohazards?*" Proceedings of the 2002 workshop on New security paradigms, ACM Press.

[16] "*Iris Recognition: Counterfeit and Countermeasures*". http://www.iris-recognition.org/counterfeit.htm.