Biometric Security Systems

A. M. Bojamma, B. Nithya, Prasad C. N., M. N. Nachappa

Abstract- The modern information technology evolution demands the use of computer networks with strict security performance. The password-based authentication system and the token-based systems that are currently deployed are not able to meet this performance Verification using biometrics has become in the last few years a key issue in security and privacy .The problems of traditional personal authentication systems may be solved by biometric systems. Information security has gained more and more attention from researchers because it plays an important role in our daily life. Biometrics-based authentication offers several advantages over other authentication methods; hence there has been a significant rise in the use of biometrics for user authentication in recent years. It is important that such biometrics-based authentication systems be designed to withstand attacks when employed in critical applications, especially in remote applications which are unattended such as ecommerce environment. In this paper we outline the strengths and weakness of biometrics-based authentication, and techniques to enhance the strength of the biometric system with new solutions for eliminating some of the weak links with techniques like steganography , watermarking, cryptosystems. For illustration purpose, finger print authentication, facial recognition has been considered.

Index Terms: steganography , watermarking, cryptosystem.

I. INTRODUCTION

The term biometric comes from the Greek words ***bios*** meaning life and ***metric*** means measure. Therefore biometrics is automatic recognition of individuals based on their biometric templates like physiological and behavioral characteristics.

Biometrics systems are commonly classified into two categories: ***physiological biometrics*** and ***behavioral biometrics***. Physiological biometrics (fingerprint, iris, retina, hand geometry, face, etc) use measurements from the human body. Behavioral biometrics (signature, keystrokes, voice, etc) use dynamics measurements based on human actions. These systems are based on pattern recognition methodology, which follows the acquisition of the biometric data by building a biometric feature set, and comparing the input template pattern against a pre-stored template pattern.

Biometric systems are more reliable and user friendly when compared to the traditional techniques used for identification. However in spite of these advantages the biometric system has many unresolved issues of integrity and robustness these problems generally emerge from the security characteristics of the system. In this paper we have attempted to discuss the various techniques used for securing a biometric system from both internal and external threats like *circumvention*(attacker accesses unauthorized data), *repudiation*(alteration of sensitive information by the attacker), *contamination*(misuse of biometrics data intended for one system to access other system use by the attacker), *collusion*(the legitimate user becomes an attacker of the biometric system), *coercion*(use of threat or force to access biometric information from the user). The techniques of securing biometric data like ***digital watermarking, Steganography, Cryptography*** are discussed below.

II. VULNERABILITIES OF BIOMETRIC SYSTEM

As the size of the population that use biometric security systems both physiological (e.g., fingerprint, face, iris) and behavioral (e.g., speech, handwriting) traits at various organizations both commercial and government sectors increases, there is an increased number of attacks on biometrics systems. Biometric systems are prone to attacks by various factors; Ratha et al.[1]analyzed these attacks and grouped them into eight classes.

They are:

Type 1 attack: Fake biometric data presented at the sensor

Type 2 attack: Illegally intercepted data is resubmitted for authorization

Type 3 attack: Feature extractor module is replaced by a Trojan horse program.

Type 4 attack: Legitimate features are replaced by fake synthetic features.

Type 5 attack: Matcher is replaced by Trojan horse program.

Type 6 attack: Attacks on the template database.

Type 7 attack: The templates are tampered with (stolen, replaced, or altered) in the transmission medium between the template database and matcher

Type 8 attack: Matching results (e.g. accept/reject) is overridden.

Manuscript received February 23, 2013.

A.M. Bojamma: Department Of Computer Science, St. Joseph's College (Autonomous), Langford Road, Shanthinagar, Bangalore – 560027.

B. Nithya: Department Of Computer Science, St. Joseph's College (Autonomous), Langford Road, Shanthinagar, Bangalore – 560027.

Prasad .C.N.: Department Of Computer Science, St. Joseph's College (Autonomous), Langford Road, Shanthinagar, Bangalore – 560027.

M.N. Nachappa: Department Of Computer Science, St. Joseph's College (Autonomous), Langford Road, Shanthinagar, Bangalore – 560027.

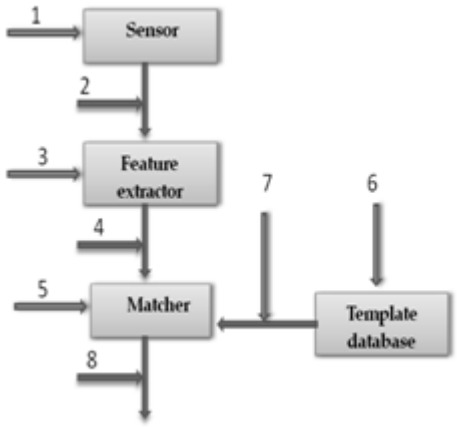


Figure-1 Locations of possible attacks in a biometric system

III. VARIOUS TECHNIQUES USED BY THE ATTACKER TO ATTACK A BIOMETRIC SYSTEM :

a. Circumvention: The attacker gains access to parts of the biometrics system protected by authentication application, here the attacker accesses some part of the data which he/she is not authorized to access. He can also launch an subversive attack where an attacker manipulates the data (e.g. changing records, false insurance claims, compensations etc).

b. Repudiation: The attacker denies accessing the system. The attacker (an employee working the organization) can alter some sensitive information like the financial records etc and claim that his /her biometric data was "stolen". He can also argue that the false accept rate (FAR) of the biometric system allowed some other user to access his account and manipulate them.

c. Contamination: The attacker surreptitiously obtains biometric data of the legitimate users in a covert acquisition (e.g. lifting a fingerprint and constructing a three dimensional mould of the finger) and use it to access the system. Misuse of biometrics data intended for one system to access other system used by the same user (e.g. finger print used to open office doors is used to access the bank account of the user by the attacker).

d. Collusion: In this scenario a legitimate user who has additional user privileges (e.g. system administrator) is an attacker, he illegally modifies the system.

e. Coercion: Here the attacker forces the user to access the system using threat (e.g. accessing bank accounts and ATM's at gunpoint).

IV. HOW ATTACKS ON BIOMETRIC SYSTEM HAPPEN

A few Classic examples of attacks on biometric systems are discussed in this section. We have taken into consideration two commonly used types of biometric features (fingerprint and iris) for which attacks are explained.

a. Direct attacks on fingerprint verification systems:

The success of fake biometric submission to sensors (type 1 attack) has been demonstrated by several researchers. This type of attack does not need any other input more than a fake biometric data. In this case no knowledge of the matcher, template specification, or template database access privileges is necessary. Also, this attack operates in the analog domain, outside the digital limits of the biometric system.

Fingerprints are one of the most commonly used type of biometric data, as they are highly acceptable by the user and can be easily embedded in the electronic devices such as mobile phones, keyboards, etc . This has given rise to the high rate of research happening in this sector by the researchers on topics like their robustness and their vulnerability.

Researchers Putte and Keuining [5] tested various biometric fingerprint sensors to check the acceptability of fake fingerprints instead of the real ones and they concluded that the fake fingers were as acceptable as the real ones. They described the methods of making fake fingerprints with or without the owner's cooperation. It was also found that the quality of fake fingerprints produced with cooperation of the owner is better than the one created without owner's cooperation. In most cases fingerprints were created using inexpensive and easily accessible material for creating dummy fingers.

b. Indirect attack on fingerprint verification system:

Most variants of Indirect attacks are based on the hill climbing technique Uludag and Jain [1] introduced a hill climbing algorithm to demonstrate an attack on a fingerprint verification system In these attacks a synthetic random minutia template is presented to the input of the matcher and, according to the score generated, it is iteratively changed until the system returns a positive verification. The minutiae in the template are modified one at a time and the change is only stored if the score returned by the matcher improves the previous one, otherwise it is discarded.

Thus, to carry out this type of attack we need:

i) The resolution and size of the images captured by the sensor (which is usually a parameter specified by the vendor).
ii) The template format.
iii) Access to the matcher input (to present the synthetic templates) and output (to get the necessary feedback from the scores).

Capelli [2] has described a fast and reliable method to generate synthetic finger print images which look realistic, which is implemented using synthetic finger print generator tool.

With this application, a type 4 attack (to the input of the matcher) using synthetic generated templates could easily be converted to a type 2 attack (to the input of the feature extractor) using the corresponding synthetic fingerprint images. Thus, the attack would be simplified as the intruder would not need to know the storage format used in the system. In the recent past various other methods of indirect methods of attack on fingerprint recognition system have been developed.

c. Direct attack on iris recognition system:

Iris is one of the most rapidly emerging biometric traits in the recent market, high accuracy algorithms are used in its recognition. The iris of the eye is used an optical fingerprint, having a highly detailed pattern that is

unique for each individual and stable over many years. In normal operation conditions, Iris-based verification systems have shown a remarkable performance. However, several works have pointed out their vulnerabilities to very simple direct attacks carried out with a printed iris, an artificial eye, and a fake contact lens [12]. Thalheim and Krissler were the pioneers who conducted a vulnerability study on iris verification system. In this work an iris image of a legitimate user was printed with a high resolution inkjet printer to fraudulently access the system. The trick was only successful if the pupil in the image was cut and the eye of the impostor placed behind the paper to give the impression to the system of a real eye. Only one commercial system (the Panasonic's Authenticam BM-ET100) was tested in the experiments showing high vulnerability to this type of attacks. It not only permitted the access with vulnerabilities in Biometric Systems with the fake iris, but also allowed the attacker to log on to the system using the iris picture.

Matsumoto et al. [13] carried out the first systematic experiment of iris spoofing. Three different iris verification systems were tested, two portable, and the remaining system being a hard-core device for gate control .Two different devices were used in the experiments to acquire the images for the fake irises, the camera embedded in the Iris Pass-h system and a digital microscope with infrared lighting. As explained in Thalheim's [12] experiments, the images were then printed using a high resolution inkjet printer and the pupil removed from the picture in order to place the impostor's eye behind the fake iris. When using the images taken with the IrisPass camera, all three systems accepted the fake irises as real with a probability of over 50%.

V. ENHANCING SECURITY IN BIOMETRIC SYSTEM

Biometric readings, which range from several hundred bytes to over a megabyte, have the advantage when compared to passwords or a pass phrase. It is unreasonable to extend the length of the password to attain the equivalent bit strength as it leads to usability problems.

Fortunately, automated biometrics can provide the security advantages of long passwords while retaining the speed and characteristic simplicity of short passwords.

Even though automated biometrics can help reduce the problems associated with the existing methods of user authentication, hackers will still find that there are weak points in the system, vulnerable to attack. For example Password systems are prone to frequent attacks whereas biometric system needs substantial effort to hack a biometric system.

Yet several new types of attacks are possible on biometric system domain. In remote unattended applications or applications running on the web there arises many opportunities and ample time for the hackers to hack into the biometric security system or even physically violate the integrity of the system before being detected.

Various techniques used by biometric researchers in order to enhance the security of the biometric system have been listed below.

They are

- **Digital Watermarking**
- **Steganography**
- **Cryptography**

Digital Watermarking technique involves use of proprietary information such as company logo, signature etc that are embedded in the host data to protect the intellectual rights of the data.

Steganography the word is derived from Greek language, meaning secret communication, this technique involves hiding of critical information in unsuspected carrier data. Steganography is based on concealing the information itself. This technique reduces the chances of illegal modification of data.

Cryptography is the science and art to transform message to make them secure and immune to attacks. While cryptography focuses on methods to make encrypted information meaningless to unauthorized parties, Encryption is the encoding of the data by special algorithm that renders the data unreadable by any program without decryption key.

VI. DIGITAL WATERMARKING

Watermarking is one of the techniques used for *hiding information in digital content for protecting the data's integrity*. A number of watermarking techniques are available for embedding information securely in an image. These can be broadly classified as

- **Transformation domain techniques.**
- **Spatial domain techniques.**

A biometric water marking system generates a biometrically encoded bit stream from the given biometric data and from the electronic data to be transmitted to the user. This encoded biometric data has the biometric data as biometric watermark. This data is then sent to the user's decoder. The decoder utilizes the biometric data of the user to decode the biometrically encoded bit stream, to extract the biometric watermark and retrieve the electronic data.

Finger print is one of the biometric identifier that is extensively used for personal identification. Ratha [1], Connell and Bolle proposed a blind data hiding method applicable to fingerprint images. The watermark message is assumed to be very small compared to the fingerprint image. The quantizer integer indices are randomly selected and each watermark bit replaces the LSB of the selected coefficient. At the decoder, the LSB's of these coefficients are collected in the same random order to construct the watermark to the fingerprint image. Jain, Uludag, and Hsu [11] used the facial information as watermark to authenticate the fingerprint image.

A bit stream of eigen face coefficients is embedded into selected fingerprint image pixels using a randomly generated secret key. The embedding process is in spatial domain and does not require the original image for extracting the watermark [8].

An example of how host image pixels can be watermarked is given below

➢ ***Hiding Facial Information into Fingerprint Images:***

The amplitude modulation-based watermarking method described below.

This Method includes image adaptivity, watermark strength controller, and host image feature analysis.

- In the first step, the data to be hidden in the host image is converted to a binary stream.
- In this scenario, every field of individual minutia is converted to a 9-bit binary representation.
- This range is adequate for x-coordinate ([0, N-1]).
- This range is adequate for y-coordinate ([0, M-1]).
- N and M are the number of rows and columns.
- Eigen-face coefficients are converted into a binary stream using 4-bytes per coefficient.

➢ ***How host image pixels are watermarked?***

- A random number generator initialized with the secret key generates locations of the given image pixel.
- First, a sequence of random numbers between 0 and 1 is generated using uniform distribution.
- Every number with odd indices is linearly mapped to [0,x-1].
- Every number with even indices is linearly mapped to [0,Y-1]. X and Y are the number of rows and columns of the host image.
- During watermark embedding, a pixel is not changed more than once, which will lead to incorrect bit decoding.
- If at any step in embedding, the candidate pixel cannot be marked due to one of these reasons, the next pixel location is considered.

➢ **How next pixel location is considered?**

The (i,j)th pixel is changed according to the following equation:

$$P_{WM}(I,J) = P(I,J) + (2S-1)\, P_{AV}(I,J)\, Q * (1 + P_{SD}(I,J) / A) (1 + P_{GM}(I,J) / B)\, B(I,J).$$

P(I, j) : Are values of original pixels at location (I, j).

s: The value of the watermark bit.

q : The value of watermark embedding strength.

P_{WM}(I, j) : Are values of the watermarked.

P(I, j) : Are values of original pixels at location (I, j).

P_{AV} (I, j) : Denote the average.

P_{SD} (I, j) : Standard deviation of pixel values in the neighborhood of pixel (I, j).

P_{GM} (I, j) : Denotes the gradient magnitude.

A and B : Are parameters weights for the standard deviation and the gradient magnitude.

The minimum values for P_{SD} (I,j) and P_{GM} (I,j) are both 0.

The maximum value for P_{SD} (I, j) is around 127.

The maximum value for P_{GM} (I, j) is around 1,082.

P_{AV} (I, j) : Denote the average.

P_{SD} (I, j) : Standard deviation of pixel values in the neighborhood of pixel (I, j).

P_{GM} (I, j) : Denotes the gradient magnitude.

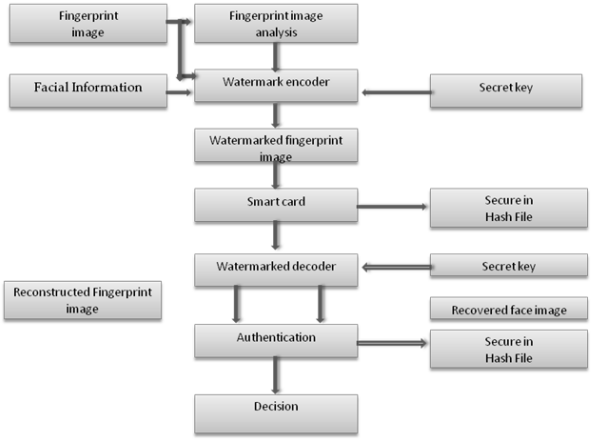
A and B : Are parameters weights for the standard deviation and the gradient magnitude.

The minimum values for P_{SD} (I,j) and P_{GM} (I,j) are both 0.

The maximum value for PSD (I, j) is around 127.

The maximum value for PGM (I, j) is around 1,082.

Figure-2 Schematics for hiding facial information into fingerprint images



In this diagram a scenario of one biometric template (e.g., face) being embedded into another (e.g., fingerprint), in order to increase the security of the latter is depicted.

➢ **How to decode watermarked information (image)**

- For every bit embedding location (I, j), its value during decoding is estimated as the linear combination of pixel values in a 5x5 cross-shaped neighborhood of the watermarked pixels as shown

$$P(I,j) = 1/8(\Sigma P_{WM}(I+k,j) + \Sigma P_{WM}(I,j+k) - 2 P_{WM}(I,j))$$

The difference between the estimated and the watermarked pixel values is calculated as $\delta = P_{WM}(I,j) - P'(I,j)$

- For finding an adaptive threshold, these averages are calculated separately for the reference bits 0 & 1.

VII. STEGANOGRAPHY

Steganography is the art of hiding the existence of data in another transmission medium to achieve secrecy of communication. Biometrics uses the *stegano* technique frequently to hide data and the biometric feature used to implement steganography is skin tone region of images. Here secret data is embedded within skin region of image that will provide an excellent secure location for data hiding. For this skin tone detection is performed using HSV (Hue,

Saturation and Value) color space.

A scenario where Biometric data (fingerprint minutiae) that need to be transmitted (possibly via a non-secure communication channel) are hidden in a host (also called cover or carrier) image, whose only function is to carry the data, is as explained below.

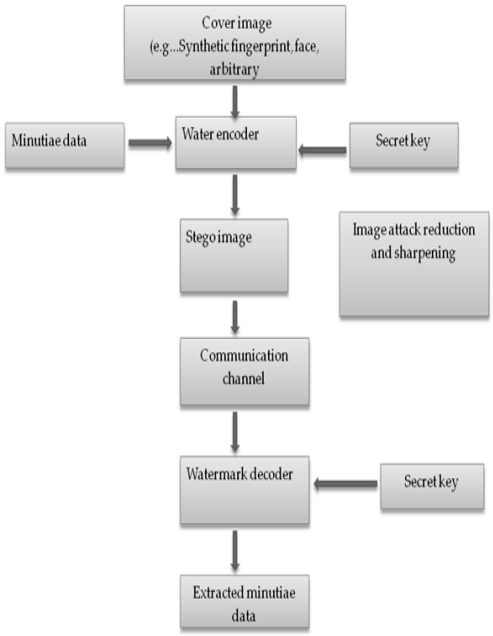


Figure-3 Steganography technique used for transmission of biometric data using non secure communication channel

The security of the biometric system in this scenario is based on the secrecy of the communication.

- To implement this scenario three different types of cover images are considered they are-a fingerprint image, a face image, and an arbitrary image.
- The synthetic fingerprint image is generated using the algorithm.
- This synthetic fingerprint image is used to carry the original fingerprint minutae data, which in turn increases the level of security.
- This application is used to counter attack the 7th type of attack i.e., The templates are tampered with (stolen, replaced, or altered) in the transmission medium between the template database and matcher.
- Key encryption algorithms like symmetric and asymmetric can be used depending on the requirement of the application.
- After encryption the *stego* image is sent through a channel that may be subjected to interceptions.
- After the reception of data decoding technique is used to decode where the same key used for encoding needs to be used to recover the hidden data from the *stego* image
- *Transmission keys* can be different for every transmission
- Parameters like *receiver, sender, and fingerprinted subject identities* can be used in tuning the *key assignment.*

VIII. BIOMETRIC CRYPTOSYSTEMS

Traditional Cryptographic systems use one or more keys to convert plain text to cipher text(encrypted data) .The encrypting key(s) maps the plain text to essentially a sequence of pseudo random bits , that can only be mapped back to the plain text using the appropriate decrypting key(s) [9].

Symmetric and asymmetric cryptographic key techniques can be used to encrypt and decrypt data.

In symmetric system decrypting key is the same as the encrypting key.

In asymmetric system both decrypting and encrypting keys are unique.

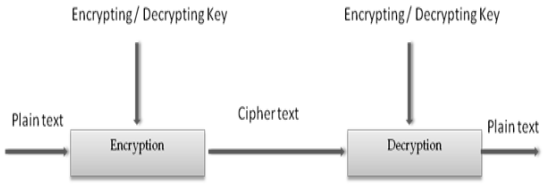


Figure-4 Symmetric encryption system

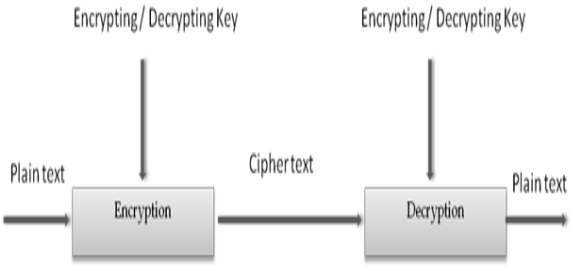


Figure-5 Asymmetric encryption system

Biometric cryptosystems combine cryptography and biometrics to benefit from the strengths of both fields. In such systems, while cryptography provides high and adjustable security levels, biometrics brings in non-repudiation and eliminates the need to remember passwords or to carry tokens etc [10]. In biometric cryptosystems, a cryptographic key is generated from the biometric template of a user stored in the database in such a way that the key cannot be revealed without a successful biometric authentication.

Fingerprint patterns are taken as example to illustrate cryptosystems:

We have selected fingerprint as the biometrics feature for generating cryptographic key. We have extracted minutiae points from the fingerprint and used that point set for generating cryptographic key [9].

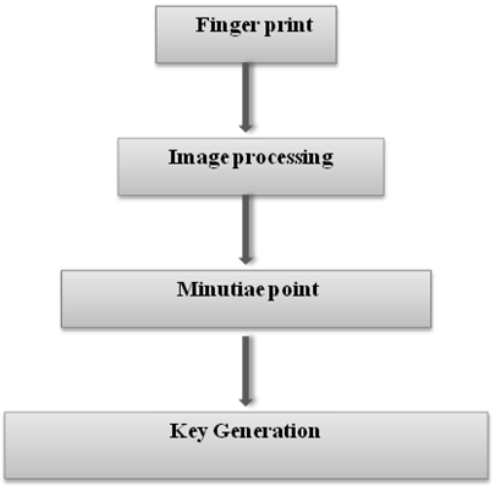


Figure-6 Stages in cryptosystem

a. Image preprocessing stage :

Histogram Equalization and Filters are used to enhance the image.

Binarization is applied on fingerprint image. Then Morphological operation is used to extract Region of Interest.

Histogram equalization increases the contrast of images, especially when usable data of the image represented by close contrast values.

Perceptional information of the image is increased through Histogram equalization.

Morphological operations are used to understand the structure or form of an image. This usually means identifying objects or boundaries within an image. There are three primary morphological functions: *erosion*, *dilation*, and *hit-or-miss*.

b. Minutiae Points Extraction stage

Thinning eliminates the redundant pixels of ridges till the ridges are just one pixel wide. Ridge thinning algorithm is applied and in each scan of full fingerprint image, the algorithm marks down redundant pixels in each small window and finally removes all those marked pixels after several scans. After fingerprint ridge thinning minutiae points are marked easily.

c. The key generation stage algorithm is as follows:

Extracted minutiae points co-ordinates are maintained in a vector

$\mathbf{M_p}$- Minutiae points set

$\mathbf{S_p}$ - Size of Mp

KL=key length

$\mathbf{K_v}$ -Key Vector

$\mathbf{L_k}$ -Length of key vector

$\mathbf{Z}_{-(X, Y)}$ co-ordinate of a minutiae point

Step 1: Read the Minutiae points

Step 2: Find the point H with highest x+y

Step 3: Draw a line from origin (0, 0) to the H and call it as L

Step 4: Sort the Minutiae points and Store in an array A

Step 5: Value= KL / Np

Vector=KL % Np

Step 6: For i=1 to value

For j=1 to Sp

Read point X from Array A and Check the point whether it is above or below the line L.

If it is above the line or on the line put value as „0" else value is „1".Store them in array K.

Final key=Append the key vector of length vector to value of K.

VI. CONCLUSION:

Modern information technology revolution that is heavily networked requires authentication that is the binding of an identity to the principle. The traditional authentication weaknesses can be solved using biometric technologies such as fingerprints, hand geometry, facial thermographs, face recognition and DNA.

The security strength of the biometric methods should be proven. In particular the biometric methods should be tested against any cryptanalytic attack. Time and space complexity analysis should be performed on any successful attack, since as the computer power grows, theoretical attacks that are not feasible with the present computing scenario, will be successful in the near future. So research should be undertaken by institutions whose expertise is to test the vulnerability of security systems. This will give users from government, public and private sectors choice among the various biometric technologies that will expand biometric market and it will make it competitive and trusty. It will also help manufacturers to evaluate their biometric products against standard tests.

ACKNOWLEDGMENT

A work of this nature requires the blessings and patience of a number of people. We would like to acknowledge the guidance of all our colleagues in this work. We would also like to thank god for his blessings and acknowledge his presence in all our efforts.

REFERENCES

1. R. M. Bolle, N. K. Ratha, A. Senior, and S. Pankanti. Minutiae template exchange format. In *Proc. AutoID 1999, IEEE Workshop on Automatic Identification Advanced Technologies*, pages 74{77, 1999.
2. R. Cappelli, A. Erol, D. Maio, and D. Maltoni. Synthetic fingerprint image generation. In *Proc. International Conference on Pattern Recognition (ICPR), vol. 3*, pages 475{478, 2000.
3. T. C. Clancy, N. Kiyavash, and D. J. Lin. Secure smartcard-based fingerprint authentication. In *Proc. ACM SIGMM Multimedia, Biometrics Methods and Applications Workshop*, pages 45{52, 2003.
4. Colorado State University. Evaluation of face recognition algorithms. Available at www.cs.colostate.edu/evalfacerec/ index.htm
5. Congress of the United States of America. Enhanced Border Security and Visa Entry Reform Act of 2002. Available at http://unitedstatesvisas.gov/pdfs/ Enhanced Border SecurityandVisa Entry.pdf, 2002.
6. S. Dass and A. K. Jain. Fingerprint classification using orientation field °ow curves. In *Proc. Indian Conference on Computer Vision, Graphics and Image Processing*, pages 650{655, 2004.
7. S. C. Dass. Markov random field models for directional field and singularity extraction in fingerprint images. *IEEE Transactions on Image Processing*,13(10):1358{1367, October 2004.
8. Institute of Paper Science and Technology, Georgia Institute of Technology. Watermarks. Available at http://www.ipst.gatech.edu/amp/education/watermark/watermarks.htm.
9. A. K. Jain, R. Bolle, and S. Pankanti, editors. *Biometrics: Personal Identification in Networked Society*. Kluwer Academic Publishers, New York, 1999.
10. A. K. Jain, L. Hong, S. Pankanti, and R. Bolle. An identity authentication system using fingerprints. *Proceedings of the IEEE*, 85(9):1365{1388, September 1997.
11. A. K. Jain and U. Uludag. Hiding biometric data. *IEEE Transactions on PatternAnalysis and Machine Intelligence*, 25(11):1494{1498, November 2003.
12. Body Check: Biometric Access Protection Devices and their Programs Put to the Test Lisa Thalheim, Jan Krissler, and Peter-Michael Ziegler
13. T. Matsumoto, H. Matsumoto, K. Yamada, and S. Hoshino. Impact of artificial gummy fingers on fingerprint systems. In *Proc. of SPIE, Optical Security and Counterfeit Deterrence Techniques IV, vol. 4677*, pages 275{289, 2002.