Trustable and generalize biometric recognition

Ashutosh Kakadiya - 1401075, Hardil Mehta - 1401018
Harsh Mehta - 1401086, Kishan Raval - 1401117
School of Engineering and Applied Science, Ahmedabad University

---

1. ABSTRACT

In ongoing utilization of biometric identification systems, establishing the authenticity of biometric data itself has a major concern. The fact that biometric data is not replaceable and is not a secret, combined with the existence of several types of attacks that are possible in a biometric system, make the issue of security/integrity of biometric data extremely critical. We are working on watermarking method, in which we hide a user's biometric data in a variety of images. This method has ability to increase the security of both the hidden biometric data (i.e. fingerprint minutiae) and host images (i.e. fingerprints). The application provides high security to both hidden data (i.e. fingerprint minutiae) that have to be transmitted and the host image (i.e. fingerprint). The original unmarked fingerprint image is not required to extract the minutiae data.The main idea is after decomposing the bio metric into two shares, one share is given to the user and the other share is stored in the database along with a signature generated by a hash function. Furthermore, the integrity of the stored metric is also guaranteed by using the hash signatures.

2. INTRODUCTION

Despite the fact that biometric systems offer reliable techniques for personal identication, but because of the lack of a proper protection, it could be miss-used. When this data are transmitted through an insecure channel, there is a risk of being stolen or modified. Even several types of encryption to protect biometric finger data can be used as a potential mechanism but it is computationally very expensive and not secure on a large scale database, because somewhere at end user data template has to be decrypted before authentication. Hence for trustable and secure authentication, watermarking technology is essentially introduced to increase the security of fingerprint minutiae transmission and can also be used to protect the original fingerprint image.

2.1 Why Biometrics?

In an increasingly digital word, protecting confidential information is becoming more difficult. Traditional passwords and keys no longer provide enough security to ensure that data is kept out of the hands of hackers and unauthorized individuals.Biometric identification provides several advantages over traditional methods that require ID cards/tokens or Password/PIN numbers.

(1) Eliminates buddy punching - the person must be physically present at the point of identification.

(2) Provides the ability to eliminate tokens/PINs - identification based on biometric techniques alleviates the need for users to remember a password or carry a token.

(3) Improves security - protects sensitive and personal data by replacing PINs, eliminates credentials that can be stolen, and prevents unauthorized access to systems or facilities.

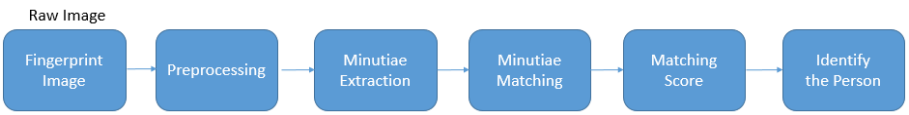


Fig. 1. Flowchart for minutiae extraction

2.2 Biometric Authentication Techniques

A biometric authentication is a pattern-recognition technique that makes a personal identication by determining the authenticity of a specic physiological characteristic of a person. An authentication is divided into two major modules:

—Enrollment Module

—Verification or Identification Module

2.3 How Biometric Technology Works

The enrollment module allows a person to enroll into the biometric system. During the enrollment, the biometric characteristic of the person is first scanned by the biometric reader, which produces the raw image of that characteristic. This raw image is further processed by the feature extractor to generate a template.This template is getting stored in the database for user verification or identification which depends on the application.

2.4 Fingerprint as a Biometric

Among all the biometric traits, fingerprints have one of the highest level of reliability. Fingerprints are the oldest and most prevalent mode for identication. The main factors for this are small and inexpensive fingerprint capture devices, fast computing hardware and recognition rate. To recognize a fingerprint, we extract a feature called minutiae. Minutiae in ngerprints are topographical relief of its ridge structure and the presence of certain ridge anomalies. Minutiae points are these local ridge characteristics that occur either at a ridge ending or a ridge bifurcation.A ridge ending is defined as the point where the ridge ends abruptly and the ridge bifurcation is the point where the ridge splits into two or more branches.

3. TECHNOLOGY USED

3.1 Feature extraction and matching

Fingerprint recognition system divides the system into two modules and they are minutiae extractor and minutiae matcher. Minutia extractor is divided into three stages and they are pre processing, minutia extraction and post processing. Cross Number(CN) method is widely used for minutia extraction. In this method, we are finding ridges, ridge ending, ridge bifurcation as fingerprint features. In minutia matching module, algorithm determines whether the two minutia sets are from the same finger or not and find the similarity score between two minutia vector of the fingerprints base on the distances between the minutia. If the similarity score is larger than the threshold it will matches the fingerprint.

3.2 Secure Hash Algorithm

The secure hash algorithms are family of cryptographic hash functions. Hash functions are very useful and widely used in information security application. Hash functions convert arbitrary length input to fixed length output. Values returned by the hash function are called message digest. Computationally

hash functions are much faster than other encryption functions. It is hard to find two different inputs of any length that results in the same hash means it is a collision free hash function. SHA0 and SHA1 is not resistant to collision attacks and hence they are not used anymore. SHA2 is totally collision free. In our algorithm we have used SHA2 to find an hash of two shares of a fingerprint, because it is practically impossible to recreate original fingerprint from the hash value.

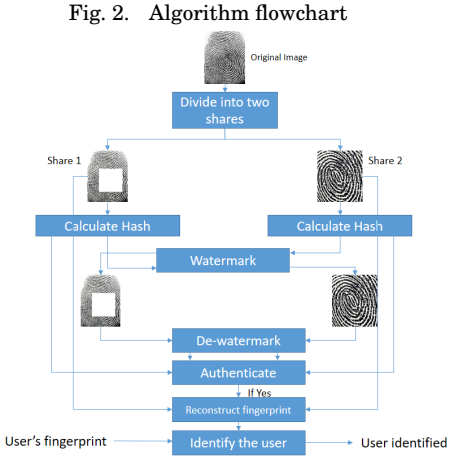
3.3 Watermarking / Steganography

Steganography is a data hiding technique that can be used along with cryptography as an extra-secure method to protect data. Steganography is a method of hiding a secret message within a larger message in such a way that one can't know the presence of the message. In our algorithm, we are hiding hash of one share into its co-responding other share. Means the hash of second share is hidden into the first share and the hash of fist share is hidden into the second share. Fig. 6 and Fig. 7 shows the watermarked image having hash of its co-responding other share.

4. ALGORITHM

Algorithm is mainly focused on the security of the biometric feature. This security has been achieved by dividing the biometric template into two parts. One part is stored in the application and other part will remain with the user. To identify the user we need to reconstruct the fingerprint and for that we need both parts of the fingerprint. Therefore finger cannot be misused. This algorithm is divided into two parts, first one is security and the second one is authentication and identification. Algorithm first authenticates the user and after successful authentication it identifies the user. Figure 1 describes the model of our algorithm.

Fig. 2. Algorithm flowchart



4.1 Security

To achieve trustability we divided user's fingerprint into two different shares as shown in the Fig. 3, Fig. 4 and Fig. 5. Each share contains hash of its corresponding other share as a hidden information. We have used secure hash algorithm to find hash of a fingerprint share and we have used watermarking/steganography to hide information. First share(Fig. 4) has the hash of second share(Fig. 5) and is stored in our database while second share(Fig. 5) having hash of first share(Fig. 4) remains with the user. Even if any of the share gets stolen no one can misuse that share without the other one. Authentication and recognition part is discussed in the algorithm section.

4.2 Authentication and Identification

Algorithm retrieves the hash from the watermarked image and compare extracted hash with its co-responding share's hash. If hash of both the shares matches, only then the system will consider the user as authenticated user. After the authentication, system regenerates the the fingerprint from the two share and compares it with the user's raw fingerprint image.

5. RESULTS

The results shows Equal Error Rate(EER), False Acceptance Rate(FAR) and False Rejection Rate(FRR) of finger print matching. The Finger print is matched in 3 ways and output FAR, FRR and EER are plotted.The three methods are:

Fig. 3. Original Fingerprint

Fig. 4. First share of fingerprint

Fig. 5. Second share of fingerprint

Fig. 6. Watermarked Image

Fig. 7. Watermarked Image

Comparison of fingerprint of person with fingerprint	1	2	3	4	5	6	7	8	9	10
Bit Error Rate	0	0.51	0.4	0.44	0.5	0.47	0.48	0.43	0.49	0.46

Table 1. Table representing BER of hash values between fingerprint 1 and fingerprint 1 to 10

(1) Full fingerprint Query Image with the Original Image

(2) First Share Image, from database, with the Original Image

(3) Second Share Image, from user's share, with the Original Image

(4) Reconstructed Image from both the shares with the Original Image

Fig. 9 shows the Output for method 1, where we observe we get EER at around 0.88 which would be the threshold for our system. Fig. 10 and Fig. 11 shows the Output for individual shares when compared with the whole image which justifies the point that a single share can't be used for a successful authentication,hence from the result we can say that our purpose of trust-ability is achieved. Fig. 12 shows the output for method 2 which proves that reconstructed image is the same as the original one. The output are as shown below.

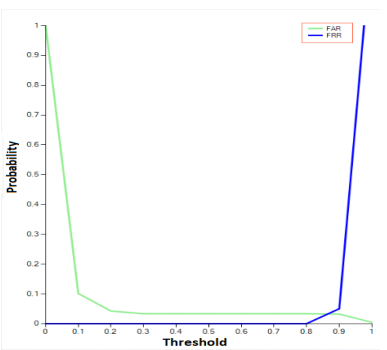


Fig. 9. FAR and FRR for original image

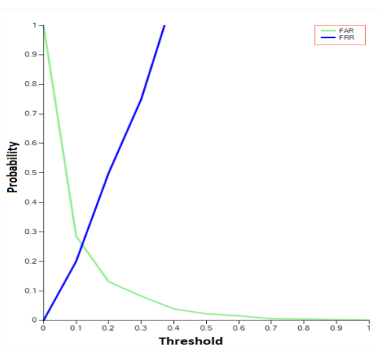


Fig. 10. FAR and FRR for Share1

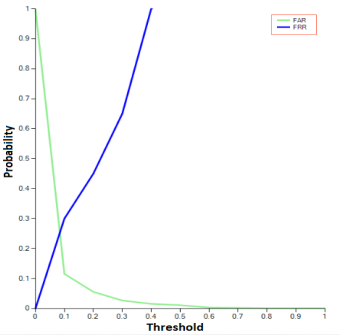


Fig. 11. FAR and FRR for share2

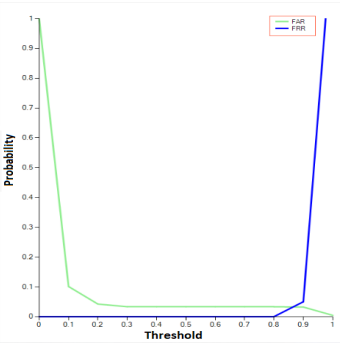


Fig. 10. FAR and FRR for reconstructed image

6. CONCLUSION

As discussed above, using multiple shares for a fingerprint, cryptography and watermarking technology we have successfully developed an algorithm which provides security and trustability for biometric feature.

7. FUTURE WORK

To improve the security and trustability we would like to explore different techniques to divide a fingerprint into two share and how would it impact our algorithm, make it faster and more generalized.

REFERENCES

[1]V. Joshi, M. Joshi and M. Raval, "Multilevel Semi-fragile Watermarking Technique for Improving Biometric Fingerprint System Security", Springer, 2017.

[2]V. Joshi, M. Raval, D. Gupta, P. Rege and S. Parulkar, "A multiple reversible watermarking technique for fingerprint authentication", Springer, 2017.

[3]M. ABDULLAH, S. DLAY and J. CHAMBERS, "A Framework for Iris Biometrics Protection: A Marriage Between Watermarking and Visual Cryptography", IEEE, 2016.

[4]P. Biometrics, "UNDERSTANDING BIOMETRIC PERFORMANCE EVALUATION", 2017.

[5]Abdullah, M. A., Dlay, S. S., Woo, W. L., & Chambers, J. A. (2016). A Framework for Iris Biometrics Protection: A Marriage Between Watermarking and Visual Cryptography. IEEE Access, 4, 10180-10193. doi:10.1109/access.2016.2623905