Biometric Template Security For Face Spoofing

Sheeba Ann Thomas[1], Bibin Varghese[2], Smitha C Thomas[3]
Department of Computer Science and Engineering
[1,2,3] Mountzion college of engineering , Kadamanitta, Pathanamthitta,India

Abstract- *Biometric systems are commonly used in our day-to-day life. Now a days, criminals are developing technique to accurately simulate the physical, physiological and behavioral characteristics of valid user known as spoofing attack. Face being a promising trait due to convenience and acceptability. So, it can be easily fooled with printed photographs and by attacking the templates stored in the database. Visual cryptography is a secret sharing scheme where a secret image is encrypted into the number of shares which independently disclose no information about the original image. There are various biometric templates like fingerprints, face, voice, signature and iris. In particular we focus on biometric template security which is an important issue. we are assigning a unique number to every template which is encrypted using Visual Cryptography. Visual cryptography provides an extra layer of authentication. The combination of biometrics and visual cryptography is a promising information security technique which offers an efficient way to protect the biometric template. In this work, we are providing two-fold security to the face template Biometric authentication is used for identification and access control. Biometric recognition offers a reliable solution to the problem of user authentication in identity management system. With the widespread deployment of biometric system, there is an increasing concern about the security and privacy in the biometric technology.*

Keywords- Identity management, biometric system security, template protection, biometric template

I. INTRODUCTION

Biometric sample is a data that is obtained by a biometric system’s capture device. This biometric sample is collected during enrollment and it is the first time when an individual uses the biometric system. This data could be n image or multiple of images of the shape of the individuals face, finger, iris etc. This data then becomes a master-profile from which the unique features of the individual’s finger, face etc., are extracted, analyzed and then converted to a mathematical file. These mathematical files come to be known as the biometric template. So, a biometric template is a digital representation of the unique features that have been extracted from a biometric sample and is stored in a biometric database. An attacker can potentially read or even replace the templates stored in the system database with a desired template (e.g., attacker’s own template) in order to gain illegitimate access. Note that access of the user’s biometric data by an adversary is a compromise of user’s privacy. Furthermore, the accessed template can be used to generate spoof biometrics and compromise biometric systems in which the same user is enrolled.

Maintaining security of the biometric template is most important as any attack on the biometric templates can lead to a failure of the biometric system. Biometric device vendors use one-way encoding of biometric data in their devices. This means the template cannot be used to reconstruct the original biometric pattern.

II. CONSEQUENCES OF TEMPLATE COMPROMISE

There are a number of different ways an adversary can use the information available in the templates stored in a database.

Database linkage

The adversary can as certain if two templates from different databases belong to the same person. This allows the adversary to track the activities of a user. Furthermore, different databases may contain different pieces of information about an individual, a linkage across different databases will thus allow an adversary to consolidate such information enabling him to stage a more severe identity related attack.

System Intrusion

There are three main ways in which an adversary can use the stolen biometric templates to gain illegitimate access to a biometric system: template replay, spoof construction and targeted false accepts. An adversary can possibly inject the templates stolen from a biometric system directly into the system in which the same user is enrolled. The biometric image can also be recovered from the templates, e.g. by using a hill climbing attacks, and can be used to prepare spoof biometrics. A spoof can then be used by an adversary to gain illegitimate access to the biometric systems. Finally, if an adversary can access the biometric data in a system database, he can determine if a user’s biometric trait is similar to his own.

III. BIOMETRIC TEMPLATE ATTACK

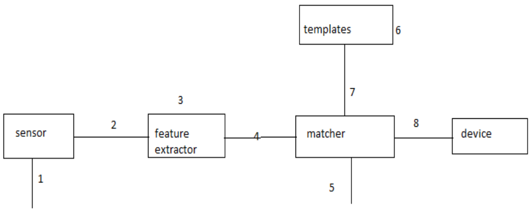

Fig 1. Attacks

Now-a-days, recognizing person using alphanumeric passwords is not sufficient for the identity determination because they can be easily guessed or stolen. Therefore, using biometric system is generally pattern recognition system that determines person based on his physiological characteristic. Use of the biometric templates provides advantages like convenience, reliability, universality etc. Several places where attacks are possible in biometric system are shown in Figure 1.

IV. VISUAL CRYPTOGRAPHY

The basic visual cryptography scheme was proposed by Naor and Shamir‟s .In this scheme for sharing a single Pixel p, in a binary image Z into two shares A and B is illustrated in Table I. If p is white, one of the first two rows of Table 1 is chosen randomly to encode A and B. If p is black, one of the last two rows in Table I is chosen randomly to encode A and B. Thus, neither A nor B exposes any clue about the binary color of p. When these two shares are superimposed together, two black sub-pixels appear if p is black, while one black sub-pixel and one white sub-pixel appear if p is white as indicated in the rightmost column. Based upon the contrast between two kinds of reconstructed pixels can tell whether p is black or white. Performance of visual cryptography scheme mainly depends on pixel expansion and contrast. Pixel expansion refers to the number of subpixels in the generated shares that represents a pixel of the original input image. It represents the loss in resolution from the original picture to the shared one. Contrast is the relative difference in weight between combined shares that come from a white pixel and a black pixel in the original image. Plenty of research has been made to improve the performance of basic visual cryptography scheme. Many authors have proposed the visual cryptography schemes in which pixel expansion is 1. These schemes can be used as quality of retrieved images is good.

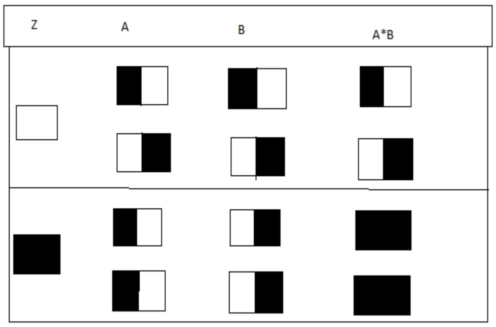

Table 1. Visual Cryptography

V. TEMPLATE PROTECTION TECHNIQUE

Since, securing the face template is the main aim of our project we are using Visual Cryptography technique for protecting the face template. In this system there are two main modules: Enrollment module and Authentication module. Enrollment module is further divided into two sub modules namely: SNF module and VC module. If we consider an example of an employee working in an organization, he will have to go through both the processes given below to have access to his organization.

Enrollment: There are two sub modules: SNF module and VC module.

SNF Module: The system administrator will collect the face image of the employees for letting them access to the organization. These images will be given to the SNF module which includes three steps that are: Segmentation, Normalization and Feature extraction. From this, the extracted facial template is stored in the database with name as any random number. Further, the bmp/png image of this number will be made and sent to the VC module. The three steps of the SNF module are explained below.

Segmentation: This is performed to extract the facial template from the face image. The Hough Transform, a standard computer vision algorithm is used here to deduce the radius and centre coordinates of the nodal points.

VC Module: The extracted iris template is stored in the database and using Random number generator algorithm, a random number is generated and is stored in the database as the extracted template image‟s name. This number is given as input to the VC module which then generates two shares, out of which one share is stored in the database and the other is stored on the user ID card. This ends the enrollment module. Authentication For this phase, user will come and give his eye image. His face image will go through the SNF process. Then this extracted image will be compared with the extracted image stored in the database while enrollment phase. If both the templates match then we consider that the user is a registered employee and he can proceed for the further Login process. But, if the templates do not match, then the user is asked to go through the enrollment phase.

Once he proceeds to the Login process, he will provide the ID card on which the share is stored. At the same time system will find his corresponding second share from the database. These both shares will be superimposed and will be decrypted to find the number. The decrypted number will be compared with the image name which was also stored as the number. If both the numbers match then the user is given access to the organization. But, if they don"t match then access is denied. Here, there may be a possibility of the user being a registered employee of the organization but the card which he is using does not belong to him. So even if the extracted templates match in the first process of authentication, because of the two fold security, the stolen ID card can be returned to the employee who owns it.

The working of proposed system is shown in Fig. 2 below.

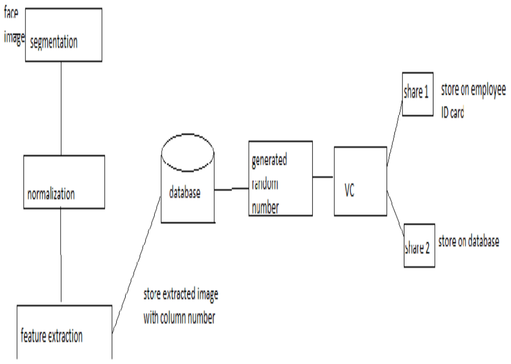

Fig 2. Employee Authentication

VI. CONCLUSION

There are various techniques adopted by the researchers to secure the raw biometric templates. In this paper a method is proposed to provide two-fold security to the iris template using Visual Cryptography. We can protect the biometric data and template by using cryptography, steganography and watermarking. In this paper a system is proposed by visual cryptography technique to protect the face template to make it secure from attack in system database as well as dual layer of authentication to the users.

ACKNOWLEDGEMENT

We would like to thank, first and foremost, Almighty God, without his support this work would not have been possible. We would also like to thank all the faculty members of Mount Zion college of engineering, for their immense support.

REFERENCES

[1] Moni Naor and Adi Shamir, “Visual cryptography” .In Proceedings of the advances in cryptology– Eurocrypt, 1-12,1995.

[2] Lin Kezheng, Fan Bo, Zhao Hong, “visual cryptographic scheme with high image quality”. In Proceedings of the International Conference on Computational Intelligence and Security, 366-370,IEEE ,2008.

[3] Wen-Pinn Fang “Non-expansion visual secret sharing in reversible style”. IJCSNS International Journal of Computer Science and Network Security, 9(2), February 2009.

[4] Xiao-qing Tan, “Two kinds of ideal contrast visual cryptography schemes”. In Proceedings of the International Conference on Signal Processing Systems, 450-453, 2009.

[5] Ao Shan, Ren Weiyin, Tang Shoulian “Analysis and Reflection on the Security of Biometrics System” 2008 IEEE.

[6] F. Hao, R. Anderson, and J. Daugman, "Combining crypto with biometrics effectively," IEEE Transactions on Computers, vol. 55, pp. 1081-1088, 2006.

[7] A.K. Jain, A. Ross and U. Uludag, “Biometric template security: Challenges and solutions”, Proceedings of 13th European Signal Processing Conference (EUSIPCO), 2005.