Concealing the Level-3 features of Fingerprint in a Facial Image

Dr.R.Seshadri ,B.Tech,M.E,Ph.D
Director, S.V.U.Computer Center
S.V.University, Tirupati

Yaswanth Kumar.Avulapati,M.C.A,M.Tech,(Ph.D)
Research Scholar, Dept of Computer Science
S.V.University, Tirupati

Abstract

Biometrics is the science of establishing the identity of an individual based on their physical, chemical and behavioral characteristics of the person. Biometrics is increasingly being used for authentication and protection purposes and this has generated considerable interest from many parts of the information technology people.

In this paper we proposed facial image Watermarking methods that can embedded fingerprint level-3 features information into host facial images. This scheme has the advantage that in addition to facial matching, the recovered fingerprint level-3 features during the decoding can be used to establish the authentication. Here the proposed system concealing of vital information human being for identification and at the same time the system protect themselves from attackers.

Keywords-

Biometrics,Watermarking, ,Encryption

Introduction

A biometrics trait can't be easily transferred, forgotten or lost. The rightful owner of biometric template can be easily identified and it is difficulty to duplicate the biometric trait. Biometrics offers many advantages over the traditional Pin Number, Passwords etc.

Conventional token-based or knowledge based identification techniques are unable to separate an authorized person and an fake person who fraudulently acquires the access privilege of an authorized person.

Biometrics is based on using physiological, behavioral and chemical characteristics in personal identification and can easily separate an authorized person and a fake person..

In order to encourage the wide spread consumption of biometric techniques an increased level of security of biometric data is required. Encryption and watermarking are among the possible techniques to achieve this security.

Encryption does not provide security once the data is decrypted. On the other hand, watermarking involves embedding information into the host data itself so it can provide security even after decryption. Furthermore, encryption can be applied to the watermarked data. However, embedding watermark may change the inherent characteristics of the host image. Therefore, the verification performance based on (decoded) watermarked images should not be inferior compared to performance based on non-watermarked images.

Here we proposed a watermarking method that embeds fingerprint Level -3 features information of a user in his/her Facial images.

Watermarking Techniques

All watermarking techniques are examples of **steganography** the process of concealing secret messages in a document or picture so that only the sender and intended recipient know that the message even exists and, more importantly, know how to retrieve it.

The classic example is the spy who sends a long letter to a "friend," describing his travels. The document appears innocuous to anyone intercepting it. But the recipient knows that every 10th letter in the document spells out a secret message.

Similarly, watermarking subtly modifies each image so that no one can tell it has been altered. Just like the example of the letter, a very simple way to watermark images would be to either increase the brightness of every 150th pixel by a small amount or leave it alone, depending on whether we wanted to encode a "1" or a "0." The recipient of our watermarked image could simply subtract
the original image from the watermarked image and would be left with a series of grey dots on a black background. The grey dots would be our hidden binary message. This is an extremely simplified example; actual methods currently in use are much more complex.

Watermark Is:

a) Data added to and often hidden within a media file
b) Usually a small amount of data, often just a unique identification number
c) Very hard to remove by distorting the Image
d)Difficult to find if you don't know the Secret key
e) Typically the same data repeated in every Video frame

Watermarking systems and techniques are not generic or standardized a watermark generated by one technology

cannot be read by a system using a different technology. And even when two systems use the exact
same technology, one customer would not be able to read another's watermarks without the secret "key" that reveals where to find the watermark and how to decode it.

Regardless of how complicated the math, the basic process of adding a watermark is fairly simple. The watermark is typically executed as a "filter" applied to an uncompressed video frame, resulting in an uncompressed frame that contains the embedded information. The watermarking filter must be programmed with the data to be embedded, as well as with the "key" that enables that data to be hidden.

Fingerprint level -3 Feature as watermark

Embedding Fingerprint level-3 features information into a facial image can enhance the security of a fingerprint based personal authentication system.

For Example: In any application the facial image is presented on the top of the card and fingerprint image of a person will be stored hidden state in a smart card that he/she carries . At an access control site, the facial image of the user will be sensed and it will be compared to the fingerprint stored(hidden)on his/her smart card. Along with this facial matching, our proposed system will extract the fingerprint information hidden in the facial image. The recovered fingerprint will be used as a second source of authenticity either automatically or by a human in a supervised biometric application. The block diagram of the proposed system is given in the fig 1.

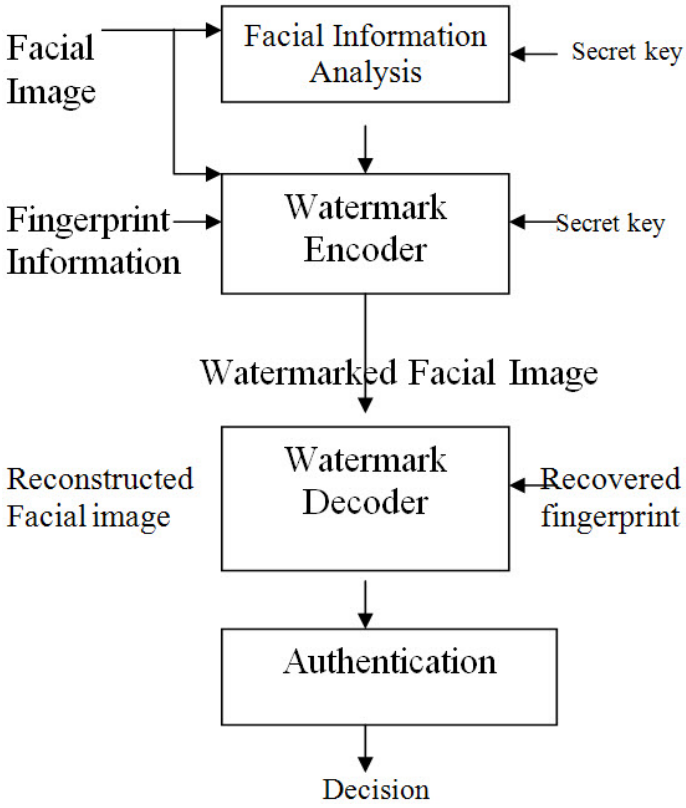

Fig.1.Fingerprint Level-3 Features are Concealing in Facial Image

Fig. 2.Facial image of a person

Fig.3.Fingerprint image

Fig.4. Fingerprint concealing with the facial Image

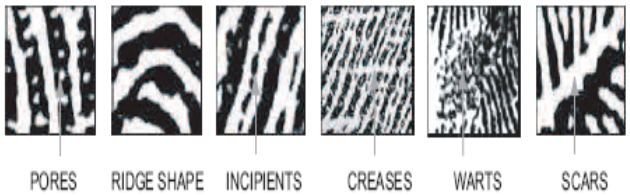

Fig.5 Concealed Fingerprint Level-3 Features in facial image

Conclusion:

Finally we conclude that the proposed method is strong and can bear certain types of attacks. The ability of biometric based identification methods can distinguish between an authorized person and a fake person who fraudulently acquire the access privilege of an authorized person is one of the main reasons for their popularity compared to conventional methods. However security is an important issue. Watermarking and stenography are only solutions to prevent from fake persons.

References:

[1].A. K. Jain,Patrick Flynn,Arun A.Ross . "Handbook of Biometrics".
[2] U. Uludag, B. Gunsel, and M. Ballan, "A spatial methodfor watermarking of fingerprint images", *Proc. First Intl. Workshop on Pattern Recognition in Information Systems*, Setúbal, Portugal, July 2001, pp. 26-33.
[3] A.K. Jain, L. Hong, S. Pankanti, and R. Bolle, "An identity-authentication system using fingerprints", *Proc. IEEE*, vol. 85, no. 9,
[4] **"**Hiding a Face in a Fingerprint Image" Anil K. Jain, Umut Uludag and Rein-Lien Hsu
[5] U. Uludag, B. Gunsel and A.M. Tekalp, "Robustwatermarking of busy images," *Proc. SPIE EI*, San Jose,Jan. 2001, vol. 4314, pp. 18-25.
[6] A.K. Jain, R. Bolle, and S. Pankanti, (Eds.), *Biometrics: Personal Identification in NetworkedSociety*, Kluwer Academic Publishers
[7]A.K. Jain, L. Hong, S. Pankanti, R. Bolle, An identityauthentication system using fingerprints, Proc. IEEE 85 (9) 1365–1388.
[8] M. Turk, A. Pentland, Eigenfaces for recognition, J. CognitiveNeurosci. 3 (1) 71–86.
[9] A.K. Jain, A. Ross, S. Pankanti, A prototype hand geometry-basedv erification system, in: Proceedings of Second International Conference on AVBPA, Washington, DC, USA, pp. 166–171.

Authors Profile

Dr.R.Seshadri was born in Andhra Pradesh, India, in 1959. He received his **B.Tech** degree from Nagarjuna University in
1981. He received his **M.E** degree in Control System Engineering from PSG College of Technology, Coimbatore in 1984. He was awarded with **PhD** from Sri Venkateswara University, Tirupati in 1998. He is currently Director, Computer Center, S.V.University, Tirupati, India. He has Published number of papers in national and international conferences, seminars and journals. At present 12 members are doing research work under his guidance in different areas

Mr.YaswanthKumar .Avulapati received his **MCA** degree with **First class** from Sri Venkateswara University, Tirupati. He received his **M.Tech** Computer Science and Engineering degree with **Distinction** from Acharya Nagarjuna University, Guntur.He is a research scholar in S.V.University Tirupati, Andhra Pradesh.He has presented number of papers in national and international conferences, seminars.He attend Number of work shops in different fields.