HIDING FINGERPRINT INFORMATION IN FACE IMAGES

Ahmadian P.,Rahmati M. - AmirKabir University, Tehran, Iran
Pouya.Ahmadian@Henesis.eu, Rahmati@aut.ac.ir

ICVSS 2011
Sicily ~ 11-16 July
International Computer Vision Summer School

Abstract

With the wide spread of biometric identification systems, establishing the authenticity of biometric data has emerged as an important issue. This work presents a watermarking technique which can hide fingerprint information in face image without any noticeable damage to image. Thus, the reliability of identification results increases and if for any reason one biometric feature fails the other one can be used. The method is also robust to blurring, rotation, JEPG compression and cropping attacks.

Introduction

ICAO standard has chosen fingerprints, face and iris as the biometrics used for travel documents [1]. A method of information hiding for purpose of identification is designed which employs fusion of Fingerprint and facial image. To make the practice more applicable, biometrics data follow the ICAO standards. Because of large data for watermarking and facial picture being small and gray image; the usual watermarking techniques don't yield acceptable results.

Conclusion

The watermarking method is amplitude modulation-based, can change 40% of host image pixels without any effect on image and is proven flexible under possible damages to face image.

References

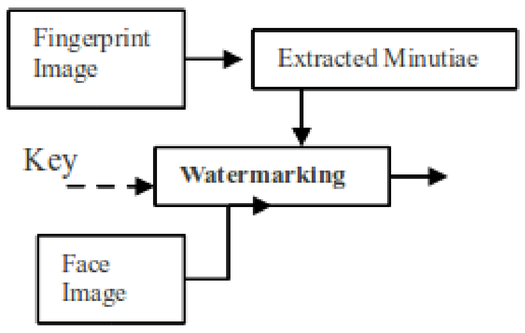
[1] ICAO official site: `www.ICAO.int`

[2] Kutter M., Jordan F., Bossen F., "Digital signature of color images using amplitude modulation ", in *In Proc. SPIE, Storage and Retrieval for Image and Video Databases V*, vol. 3022, pages 518-526, 1997

[3] Chung M., Chang K., Hsiao S., "Robust Spatial-Domain Watermarking Methods Based on a Weighting Table with Fine Tune Technique', in *Proc. International Computers Symposium, (ICS 2000)*, 2000

Method and Formula

The general block diagram of data hiding architecture is described below:

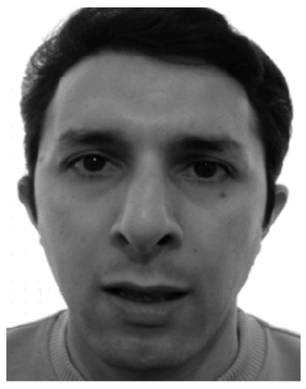


The (i,j)th pixel of face image is changed by extension of the blue channel watermarking method of [2]:

$$P_{WM}(i,j) = P(i.j) + (2s-1)P_{AV}q \times (1+\frac{P_{SD}(i,j)}{A})(1+\frac{P_{GM}(i,j)}{B})\beta(i,j)$$

Result

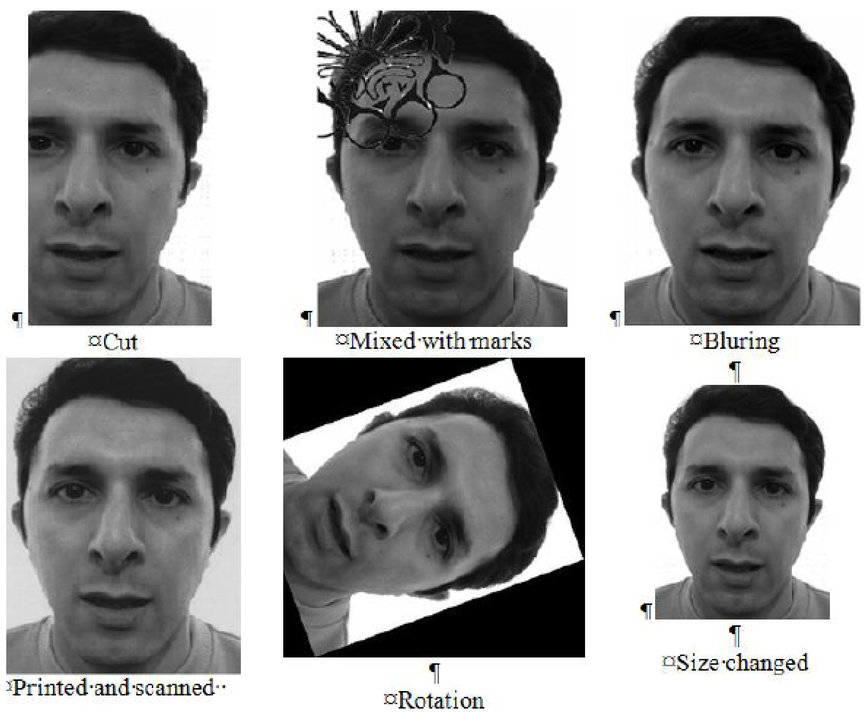
The watermarked image of a real subject face containing 20 minutiae extracted from his fingerprint image:



PSNR= 46.24, considering that the images with PSNR > 40 are said to be indistinguishable from their original [3], the visual quality of image is good.

Robustness under attacks

The watermarked face image was subjected to 5 different attacks. Due to the use of three components (row, column and orientation) for each minutia, and by using nine bits for each component, a total of $20 \times 3 \times 9 = 540$ bits was store in face image with size 300×365 (See Result section).
The image was then subjected to attracts such as rotation, blurring, JPEG compression, cropping and mixed with a mark. In each case number of minutiae extracted correctly in various degrees of attack was measured. Moreover, image was printed on a normal paper and then scanned with different scanners and different dpi. This experiment was to investigate whether is possible to extract minutiae when face image is printed on a ID card and the digital copy is not at hand.



Some of the results are shown in the above images. Under all these attacks watermark image showed acceptable robustness. Obviously by increasing the degree of attacks the number of correctly extracted minutiae decreased. However, method robustness can be improved by simply embedding the minutiae in host image more then once. Extracting minutiae from printed image was possible with accuracy up to 99.4 %. The printers and scanners used was normal devices used for ordinary images. This shows great potential of method in this area.