CSIT (December 2013) 1(4):343–348
DOI 10.1007/s40012-013-0033-1

BRIEF REPORT

Identification and authentication using visual cryptography based fingerprint watermarking over natural image

Jaishri Chourasia

Received: 26 April 2013 / Accepted: 12 November 2013 / Published online: 3 December 2013
© CSI Publications 2013

Abstract Protection of biometric data is gaining interest and hence digital watermarking techniques are one of the best ways to protect biometric data from accidental or intentional attacks. We have proposed fingerprint watermarking scheme over natural image based on visual cryptography for identification and authentication. The scheme does not embed the fingerprint directly onto the natural image instead using the concept of visual cryptography fingerprint is divided into parts called as shares. The verification share is generated at the time of fingerprint embedding process and while performing identification and authentication master share is generated. Fingerprint is extracted using these two shares. Correlation value between original fingerprint and extracted fingerprint is the deciding factor for identification and authentication. The experimental results show that the scheme is robust against various watermarking attacks.

Keywords Fingerprint · Natural image · Digital watermarking · Visual cryptography · Identification · Authentication

1 Introduction

Biometrics is the science of establishing the identity of an individual based on physical characteristics such as face, fingerprint, face, gait etc. Fingerprints are the most widely form of biometric identification. Fingerprint identification is commonly employed in the forensic science to support criminal investigations, and in biometric systems such as civilian and commercial identification devices. Biometric authentication has recently received great interest from computer science researchers. With its unique characteristics, biometric authentication is believed to be a reliable authentication method in the near future [1]. However, on the way it becomes true, [2] shows that impostors can do at least 8 types of attacks onto the biometrics authentication system. From that finding, researchers have been proposing several ways to enhance authentication system's security. Among those, using digital watermarking to secure template stores and data communication between client and server is widely used, especially in network environment. Moreover, this method can be used for multi-biometrics authentication system in which one or more biometrics can be embedded into other biometrics for improving accuracy and reducing bandwidth.

According to [1] biometric watermarking was introduced as the synergistic integration of biometrics and digital watermarking technology. In the battle of copyright piracy, several technological approaches and solutions have been suggested and implemented [3]. The watermark is nowadays used in conjunction with several biometrics including fingerprint [4], signature [5], face [6], hand [4], iris [7], voice [8], retina [9]. Fingerprints are unique biometrics that is mainly used for the establishment of instant personal identity. However, they are susceptible to accidental and intentional attacks, when transmitted over network. Thus, a protective scheme is needed which will preserve fidelity and prevent alterations. This is more important with respect to biometric identifiers because of their uniqueness. A solution to this situation is watermarking.

Due to the combination of the computer and communication technology, more and more digital information are transmitted and exchanged over the internet. It has created an environment that digital information is easy to distribute, duplicate and modify.

J. Chourasia (✉)
Cummins College of Engineering for Women, Pune, India
e-mail: jaishri.chourasia23@gmail.com

The image watermarking method must satisfy the following requirements [10]:

1. Transparency: The embedded watermark pattern does not visually spoil the original image and should be perceptually invisible.
2. Robustness: The watermark pattern is hard to detect and remove in illegal way. It should be immune to various possible attacks.

The rest of the paper is organized as follows: Sect. 2 describes the (2, 2) visual cryptography scheme which is used for the generation of shares of the fingerprint. Section "3" describes the proposed watermarking scheme. Section "4" shows experimental results. Finally, Sect. 5 includes analysis of scheme and Sect. 6 concludes the paper.

2 Brief description of (2, 2) visual cryptography scheme

To encrypt the secret information using (2, 2) visual cryptography scheme, the secret information is divided into two shares such that each pixel in the original image is replaced with the non-overlapping block of two subpixels. Anyone who holds only one share will not able to reconstruct the secret information as single share does not contain complete secret information [11], [12].

Figure 1 illustrates encoding scheme for (2, 2) visual cryptography which is to be applied on the every pixel of the secret information. If pixel P is white of the secret information then it is replaced with two identical blocks of subpixels. If the pixel P is black of the secret information then it is replaced with two complementary blocks of subpixels. To decrypt the secret information, each share is xeroxed onto the transparency. Superimposition of both transparencies will reveal the secret information [13].

3 The proposed fingerprint watermarking scheme

Figure 2 shows proposed fingerprint watermarking scheme over the natural image. The original fingerprint and natural image is to be registered by the candidate to the notarial

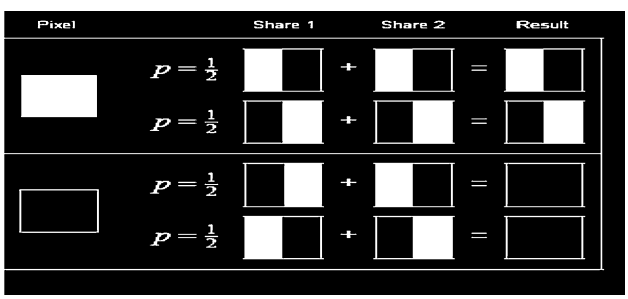


Fig. 1 (2, 2) Visual cryptography scheme

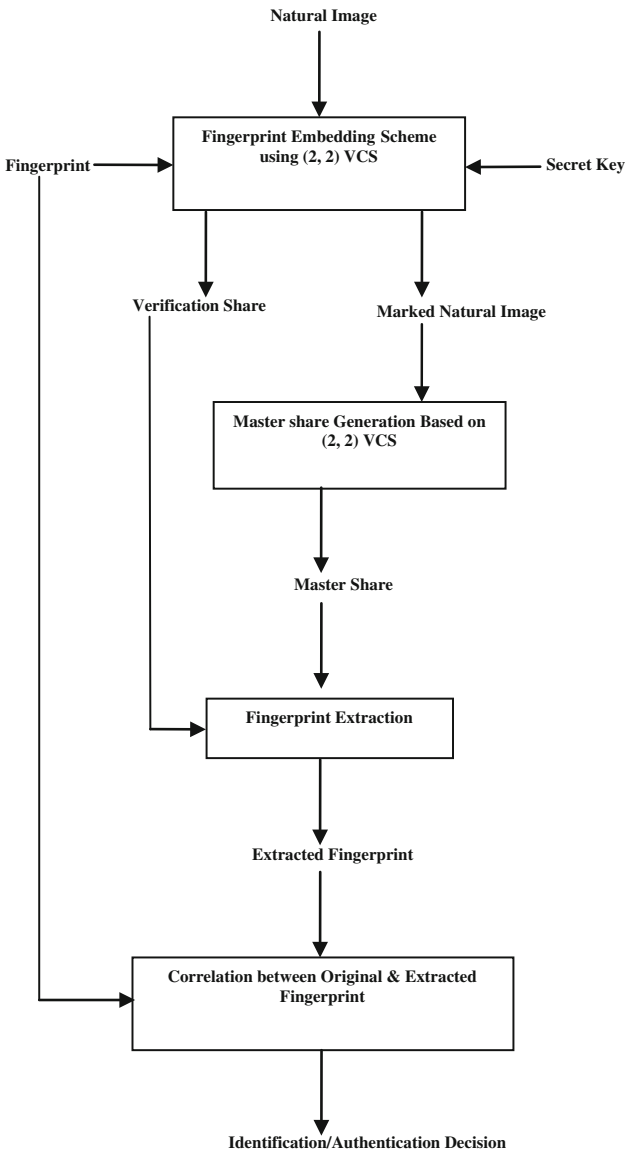


Fig. 2 Proposed fingerprint watermarking scheme

organization. The organization uses these information along with the secret key to generate the part of the fingerprint pattern, called as verification share using (2, 2) visual cryptography scheme. While performing identification and authentication organization uses marked image, verification share and secret key to generate second share of the fingerprint pattern, called as master share. These two shares are used to extract the fingerprint pattern. The correlation between the extracted fingerprint pattern and original fingerprint pattern is the deciding factor for the identification and authentication.

3.1 Fingerprint embedding scheme

To embed the fingerprint H of size $P \times Q$ over the natural image I of the size $X \times Y$ a number 'K' is selected as a

Table 1 The rules for generation of verification share

Color of the ith pixel in watermark pattern W_i	ith element in binary matrix Z_i	Pair of bits (V_{i1}, V_{i2}) to be assigned in verification share (V)
Black	1	(0.1)
Black	0	(1.0)
White	1	(1.0)
White	0	(0.1)

Table 2 The rules for generation of master share

ith element in binary matrix Z_i	Pair of bits (S_{i1}, S_{i2}) to be assigned in master share (S)
1	(1.0)
0	(0.1)

secret key. The secret key should be different for different natural image and it must be kept secretly. The embedding scheme includes following steps:

Input: Secret Key (K), natural image (I) of size X × Y.

Output: Marked natural image (M) of size X × Y.

Step1. Select a number K as the secret key for the natural image (I) and fingerprint (H).

Step2. Convert H to bi-level image (W) using *im2bw* function of MATLAB.

Step3. Use 'K' as the seed to generate $P \times Q$ random numbers over the interval [1, h]; where h = X × Y. Let R_i is ith random number. The same seed (secret key) will be used for extraction purpose to generate master share hence the original fingerprint pattern can be revealed if and only if same seed (secret key) is used, else extraction procedure returns an output that resembles random noise.

Step4. Assign the ith pair (V_{i1}, V_{i2}) of the verification share (V) based on the information given in the Table 1 using the pixel value of W and matrix Z.

Step5. Assemble all the pair values to construct the verification share (V). The size of verification share will be $P \times 2Q$ because one pixel of fingerprint H is divided into two subpixels to generate verification share.

3.2 Fingerprint extraction and identification/ authentication scheme

To extract the fingerprint from the marked natural image (M) following steps is to be followed:

Input: Marked natural image (M) of size X × Y, fingerprint pattern (W) of size $P \times Q$, verification share (V) of size $P \times 2Q$.

Output: Master share (S) of size $P \times 2Q$, extracted fingerprint (W′).

Step1. Use secret key' K' as a seed to generate $P \times Q$ random numbers over the interval [1, h]; where h = X × Y. Let R_i is ith random number.

Step2. Creation of binary matrix Z of size P × Q such that the elements of the matrix Z are the least significant bit of the R_i; ith random number.

Step3. Assign the ith pair (S_{i1}, S_{i2}) of the master share (M) based on the information given in the Table 2.

Step4. Assemble all the pair values to construct the master share (S). The size of master share will be $P \times 2Q$ because one pixel of fingerprint H is divided into two subpixels to generate master share.

Step5. To extract the fingerprint pattern compare verification share (V) and master share (S). If the ith pair (V_{i1}, V_{i2}) of V is equal to the ith pair (S_{i1}, S_{i2}) of S then assign the ith element value of the extracted fingerprint pattern 1 else assign 0.

Step6. Calculate the correlation between the W and W′. If the correlation is in the interval [0.9 1] then the candidate is authenticated.

4 Experimental results

This section presents some experimental results concerning the proposed scheme. The proposed scheme is tested on the natural image of the size 225 × 225 which is shown in the Fig. 3. The fingerprint pattern to be embedded is of size 54 × 69 shown in the Fig. 4. Figure 5 shows marked image and Figs. 6 and 7 shows the verification and master share. Figure 8 shows the extracted fingerprint pattern. All experiments are implemented using MATLAB Image Processing toolbox.

To test the robustness of the proposed scheme several watermarking attacks have been applied such as noise, sharpening, blurring, average filter distortion, jpeg compression etc. Even if marked image is attacked by various watermarking attacks; fingerprint pattern can be extracted successfully as shown in the Figs. 9, 10, 11, 12, and 13.

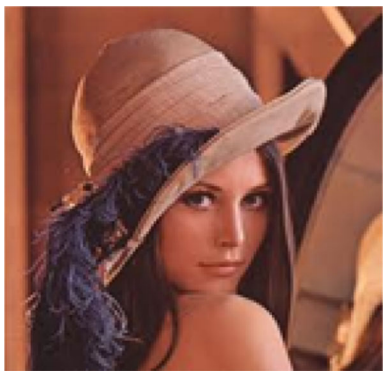
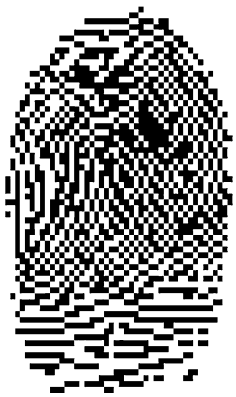


Fig. 3 Natural image

Fig. 4 Original fingerprint



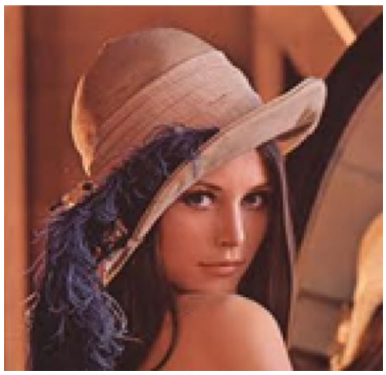


Fig. 5 Marked natural image

Fig. 6 Verification share

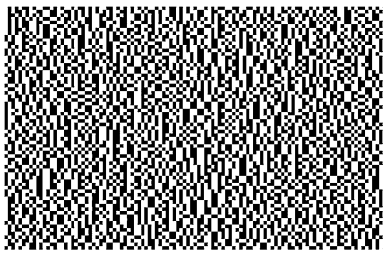
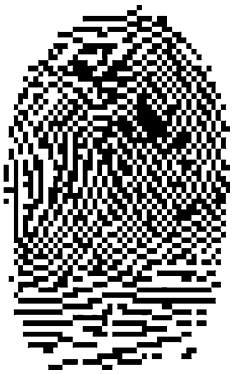


Fig. 7 Master share

Fig. 8 Extracted fingerprint



(b)

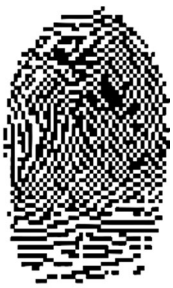


Fig. 9 **a** Salt & pepper noise attack on Fig. 5 **b** Extracted fingerprint

(b)

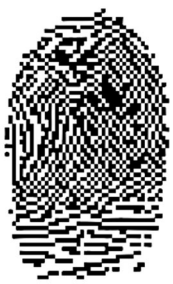


Fig. 10 **a** Sharpen attack on Fig. 5 **b** Extracted fingerprint

Fig. 11 **a** Blurring attack on Fig. 5 **b** Extracted fingerprint

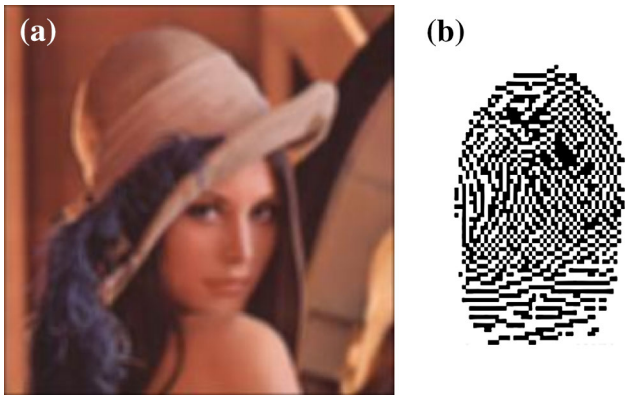


Fig. 12 **a** Averaging filter attack on Fig. 5 **b** Extracted fingerprint

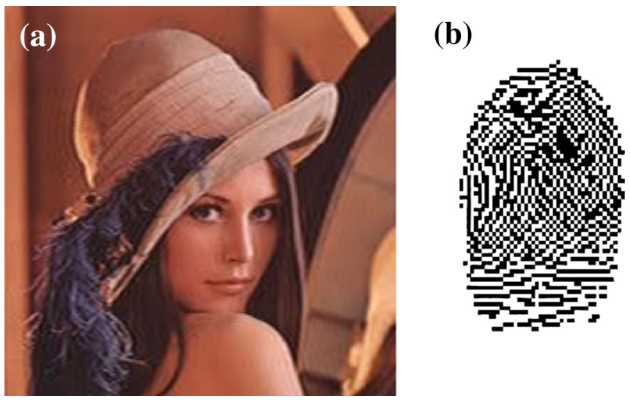


Fig. 13 **a** JPEG compression on Fig. 5 **b** Extracted fingerprint

5 Correlation between original fingerprint and extracted fingerprint pattern

After performing various attacks on the marked natural image we prove the robustness of the proposed scheme. The correlation between the original fingerprint and extracted fingerprint can be taken as the deciding factor for identification and authentication. However there are several others such as minutiae based and pattern based techniques could be applied for identification and authentication.

Table 3 Correlation between the original and extracted fingerprint pattern after several attacks

Attack method	Correlation factor between original and extracted fingerprint (in %)
No attack	99.75
Salt & Pepper noise	98.54
Sharpening	99.66
Blurring	98.67
Averaging filter	98.58
Jpeg compression	99.56

As shown in the Table 3 correlation factor between original and extracted watermark pattern is 0.99 (99 %) approximately for all cases, it means scheme is robust.

6 Conclusion

We have proposed an approach for biometric security using fingerprint watermarking over natural image for identification and authentication. Among the various biometrics, fingerprints are more famous in the authentication area, as they are unique to each person and are mainly used for the establishment of instant personal identity. However, they are susceptible to accidental and intentional attacks, when transmitted over network. The scheme preserves fidelity and prevents alterations and provides following advantages:

1. It does not require any complex transformations for embedding fingerprint such as FFT, DCT etc. because scheme uses visual cryptography scheme.
2. It maintains the quality of the natural image after embedding the fingerprint.
3. Even if the natural image is distorted or modified fingerprint as watermark over natural image can be used for authentication and identification of the person.
4. This approach can be used in smart card, driving license also criminal information could be stored in this way.
5. The key point of the proposed scheme is the secret key. For each image a different secret key will be used and hence each time different verification share will be generated. This will increase the reliability to the system. If one applies incorrect secret key, then the watermark extraction procedure returns an output that resembles random noise.

References

1. Low CY, Teoh AB, Tee C (2009) Fusion of LSB and DWT biometric watermarking using offline handwritten signature for copyright protection. In: Proceedings of the third international

conference on advances in biometrics, vol 5558. Lecture notes In computer science, pp 786–795
2. Ratha NK, Connell JH, Bolle RM (2000) Secure data hiding in wavelet compressed fingerprint images. In: Proceeding of the ACM multimedia workshops, Los Angeles, pp 127–130
3. Schaathun HG (2006) On watermarking/fingerprinting for copyright protection. In: Proceedings of the first international conference on innovative computing, information and control, vol 3. IEEE Computer Society, pp 50–53
4. Jain S (2000) Digital watermarking techniques: a case study in fingerprints and faces. In: Proceedings ICVGIP 2000, pp 139–144
5. Maiorana E, Campisi P, Neri A (2007) Biometric signature authentication using radon transform-based watermarking techniques. In: IEEE biometrics symposium, pp 1–6
6. Tzouveli P, Ntalianis K, Kollias S (2005) Human face watermarking based on zernike moments. In: Proceedings of the fifth IEEE international symposium on signal processing and information technology, pp 399–404
7. Ryoung K, Jeong DS, Kang BJ, Lee EC (2007) A study on iris feature watermarking on face data. In: Proceedings of the 8th international conference on adaptive and natural computing algorithms, part II, vol 4432. Lecture notes in computer science, pp 414–423
8. Lee Y, Kang HJ, Ki YH (2005) Copyright authentication enhancement of digital watermarking based on intelligent human visual system scheme, knowledge-based intelligent information and engineering systems. Intell Watermarking Algorithms Appl 3682:567–572
9. Coatrieux G, Lamard M, Daccache W, Puentes W, Roux C (2006) A low distorsion and reversible watermark: application to angiographic images of the retina. In: 27th annual international conference of the engineering in medicine and biology society, 2005 IEEE-EMBS, pp 2224–2227
10. Hou Y-C, Chen P-M (2000) An asymmetric watermarking scheme based on visual cryptography. Proc ICSP 2:992–995
11. Shamir A (1996) How to share a secret. Commun ACM 22:612–613
12. Naor M, Shamir A (1995) Visual cryptography: advances in cryptology—Eurocrypt'94. In: Proceeding, LNCS, vol 950. Springer-Verlag, pp 1–12
13. Naor M, Shamir A (1996) Visual cryptography II: improving the contrast via the cover base. Workshop on security protocols, Cambridge