8

Improving Security for Facial Image Using Fragile Digital Watermarking

Zutao Zhang
Southwest Jiaotong University
China

1. Introduction

Recently, face recognition technique is an active field (Zhao et al., 2000; Viola et al., 2001; Gu et al., 2002) in computer vision and anti-terror, safety defense, etc. Current face recognition pays more attention to these fields: 1) detection failure of some or all of features due to a variety of lighting conditions and head motions; 2) multiple and non-rigid object tracking; and 3) features occlusion when the head is in oblique angles and so on. But the security of facial image database has rarely been studied in face recognition system. Once hackers attack facial images database by unlawful approach, such as tamper, substitution and addition etc, there are great fatal influences to the availability of commercial face recognition systems. It is very important to improve the security of facial image database.

Current security of facial image database depends on the conventional database protection strategy (Zhang et al., 2005; Su et al., 2005). To resist various attacks on facial image database, such as tamper, substitution and addition form unlawful approach, a fragile digital watermarking method is proposed to improve security of facial image database in this paper, which can distinguish any minute tampers on facial image, and detect the modification location. First, the low-frequency compressed facial image, which low-frequency wavelet coefficients of 7 Most Significant Bits (MSBs) of original facial image are non-uniform scalar quantization, is converted into a binary sequence as the watermark to be embedded. The improved security watermark scrambled by chaotic systems is embedded into the LSB of the facial image data. When facial image is identified, the fragile digital watermarking method is able to detect the tampered location and discriminate the validity of facial image database, which comes from the difference facial image between the low-frequency compressed image and reconstructed image by watermark. We also analyze the error estimation factor for identifying facial images embedded fragile digital watermarking. Experimental results show that the fragile digital watermarking technique has high sensitivity to tampers on the watermarked facial images, it not only can improve the security of the watermarked facial image database, but also will not impact feature extraction, detection rate and detection speed of face recognition.

The organization of the paper is as follows: application of the fragile digital watermarking technique to facial image database is given in Section 2. Section 3 gives the theoretical analysis about the error estimation factor after embedded fragile digital watermarking. The experimental results for implementing security of facial image database using fragile digital watermarking are provided in section 4. Finally conclusions are in section 5.

2. Fragile digital watermarking based facial image database

In 1993, Caronni (Kutter et al., 1999) proposed digital watermarking technique to complement cryptographic process to protect copyright ownership (Liu et al., 1999). Digital watermarking techniques make it possibly to embed a watermark (such as identification data, serials number, text or image etc) to audio, video, image, and multimedia data. Current digital watermarking techniques have become a solution to DRM (Digital Rights Management), images of law evidence, seal identification etc (Wang et al., 2002). Herein, a fragile digital watermarking scheme is used to improve the security of facial image database. The low-frequency compressed facial image, which low-frequency wavelet coefficients of 7 Most Significant Bits (MSBs) of original facial image are non-uniform scalar quantization, is converted into a binary sequence as the watermark to be embedded. The watermark scrambled by chaotic systems is embedded into the LSB of the facial image data to enhance security of facial image database. Experimental results are provided to support the validity of the method.

2.1 The algorithm of watermarking

The algorithm of fragile digital watermarking is as follows:

Step 1: The facial image $\overline{\mathrm{I}}$ is the new image which the least significant bit (LSB) of facial image I (size: m*n) is transformed to zero. Next, we make two-dimension wavelet of image $\overline{\mathrm{I}}$,and gain the low-frequency wavelet coefficient LL;

Step 2: The low-frequency wavelet coefficient LL is Quantized in 4-bits non-uniform scalar basing on cryptograph key1. And the low-frequency compressed facial image I_{LL} is coming into being;

The formula of quantization process is

$$\mathrm{I}_{\mathrm{LL}} = \mathrm{Q}(\mathrm{LL},\mathrm{key}_1) \tag{1}$$

Step 3: Let each element of low-frequency compressed image I_{LL} be transformed into 4-bits binary system element, and array to matrix I_{Lb} according to spatial sequence.

That is

$$(\mathrm{I}_{\mathrm{LL}})_{(m/2)*(n/2)} \rightarrow (\mathrm{I}_{\mathrm{Lb}})_{(m/2)*(n/2)} \tag{2}$$

Step 4: The chaotic sequence x^{L} can be achieved by chaotic system, which length is L. And we can acquire address sequence A using steady ranking method.

Step 5: We can gain the watermarking W which address sequence A scrambles to matrix I_{Lb} .

In this paper, matrix I_{Lb} is divided into the same size block.

nk—the number of row block

mk—the number of column block

and *L=mk*nk*

According above-mentioned valid address sequence A, scrambled matrix W can be achieved from re-ranking matrix I_{Lb} .
The formula is

$$W(i_w, j_w) \underset{\text{scramble}}{\overset{\text{resume}}{\rightleftarrows}} I_{Lb}(i_{Lb}, j_{Lb}) \tag{3}$$

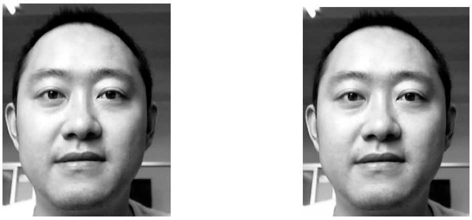
In this case ,

$$i_w = \lfloor (A(temp_{ij}) - 1) / nk \rfloor + 1$$

$$j_w = A(temp_{ij}) - (i_w - 1) * nk$$

$$temp_{ij} = (i_{Lb} - 1) * nk + j_{Lb}$$

So, the facial images embedded fragile digital watermarking come into being. In this paper, we use ORL facial database.
Fig.1 (a) shows the original facial image of database, and the facial image database embedded fragile digital watermarking is shown in Fig.1 (b). The size of image is 384*304, PSNR= 51.1237.



(a) Original image (b) Watermarked facial image

Fig. 1. Facial image embedded watermarking

2.2 Watermarking detection

The watermarking is embedded into the LSB of the facial image data to enhance security of database. The formula is

$$\overline{I} = \lfloor I / 2 \rfloor * 2 \quad I^w = \overline{I} + W \tag{4}$$

Where $\overline{I}$ is the original facial image of face recognition system, and I^w represents facial image embedded watermarking.
It is known that the least significant bit(LSB) plane is corresponding watermarking. So it needn’t use original facial image to extract watermarking.
That is

$$W^* = \text{mod}(I^*, 2) \tag{5}$$

Where I^* is the facial image which will be detected, and W^* represents the watermarking extracted from facial images.

While facial image authenticating, the general picture can be discovered from the low-frequency compressed facial image. The method is able to detect the tamper location, and discriminate the changes from comparing original facial image with low-frequency compressed facial image. The detailed approach is as follows:

Sept1: According to chaotic cryptograph key2 and watermarking W^* from new watermarked facial image, we can resume the original low-frequency compressed facial image $I_{LL}^{'}$. The general picture of facial image can be discovered from the low-frequency compressed facial image $I_{LL}^{'}$.

Sept2: The low-frequency compressed image I_{LL}^{*} can be obtained by computing the facial image I^* from the setp1 and step 2 previous algorithm of watermarking.

Sept3: The difference of image is defined as

$\Gamma = \left| I_{LL}^{'} - I_{LL}^{*} \right|$. It's very clearly that we can discriminate between image tampers from the non-zero dot distribution of Γ.

The improving security of facial image database using fragile digital watermarking is as follows:

1. First, the image of face recognition system database does not be tampered if the value of I_{LL}^{*} is equal to I_{LL};
2. If the difference of image Γ has any area of centralized non-zero dot, it is clearly that the area of facial image has been tampered.
3. The tampered location can be detected according to the area (ΔS) of centralized non-zero dot. Hence, we consider that the area of facial image has been tampered if $\Delta S \geq T$ .Where *T* is the template of threshold value.

3. Face recognition impact after embedded watermarking

At the same time, we must consider the face recognition algorithm impact when facial image database has been embedded watermarking. Whether the feature extraction, detection rate and detection speed of face recognition will be affected of not? These problems have been seldom paid attention to by former references. In this section, we give the theoretical analysis of the error estimation factor after embedded fragile digital watermarking, and identify it. Theoretic analysis and experimental results also indicate that it doesn't impact feature extraction, detection rate and detection speed of face recognition using fragile digital watermarking.

Because of being many different face recognition algorithms currently, in this paper, we will analyze a typical face recognition algorithm with SVD face recognition algorithm, and other algorithms can be deduced analogously.

3.1 SVD based face recognition algorithm

SVD (Singular Value Decomposition) is an effective algebra feature extraction method. The feature of SVD is steady, which has transpose invariability, rotation invariability, displacement invariability, enantiomorphous invariability etc. Thus, the feature of SVD can be a good algebra feature extraction to image processing (Zhou et al., 2003).So SVD algorithm can be a stable approach to detect face in variety lighting condition and oblique angles.

SVD based face recognition algorithm can transform real symmetrical matrix to diagonal matrix by orthonormal transform. And each real matrix $A_{m\times n}$ is able to be transformed into diagonal matrix using singular value decomposition (SVD). In this paper, we set $A_{m\times n}$ to a real matrix. Where rank （A） =k, that is

$$A = UDV^T \tag{6}$$

In this case, $U_{m\times m}$ and $V_{n\times n}$ are orthonormal matrixes.

Where $D_{m\times n}$ is a diagonal matrix.

In this case

$$D_{m\times n} = \begin{pmatrix} \sum_{k\times k} & O \\ O & O \end{pmatrix},$$

$$\sum_{k\times k} = diag(\sigma_1, \sigma_2, ..., \sigma_k),$$

$$U_{m\times m} = (u_1, u_2, ..., u_k, u_{k+1}, ..., u_m),$$

$$V_{n\times n} = (v_1, v_2, ..., v_k, v_{k+1}, ..., v_n),$$

Where T is the transpose and σ_i is singular value of matrix A.

$$\sigma_i = \sqrt{\lambda_i}(i = 1, 2, ..., k, ..., n)$$

Where $\lambda_1 \geq \lambda_2 \geq ..... \geq \lambda_k \geq 0$ are the non-zero eigenvalues set of AA^T and AA^T. Where $\lambda_{k+_1} = \lambda_{k+_2} = ... = \lambda_n = 0$ are eigenvalues which consist of n-1. Where $u_i, v_i (i = 1, 2, ..., k)$ are non-zero eigenvectors which belong to the non-zero eigenvalues of AA^T and $A^T A$. Where $u_i (i = k+1, ..., m)$ is the eigenvector of $A^T A$ which correspond to $\lambda_i = 0$. So $v_i (i = k+1, ..., n)$ is the eigenvector of $A\ A^T$ which correspond to $\lambda_i = 0$.

That is, formula (6) can also be written as follows:

$$A = \sum_{I=1}^{K} \sigma_i u_i v_i^T \tag{7}$$

If matrix A is a facial image, and formula (7) is the orthonormal decomposition of the facial image. If we buildup a n-dimensional column vector using singular value element σ_i in matrix Σ diagonal and the residual (n-k) zero.

That is

$$x_{n\times 1} = D_{n\times n} = e(\sigma_1, ..., \sigma_k, 0......0)^T \tag{8}$$

Where $D_{m\times n}$ is the first n-order sub-formula of D , and $e=(1,1,.....,1)_{n\times 1}^{T}$ is column vector. In this case, $x_{n\times 1}$ is singular value eigenvector of matrix A . In any case, singular value diagonal matrix Σ is unique in the condition of $\lambda_1 \geq \lambda_2 \geq ..... \geq \lambda_k$. So we can indicate that former facial image is corresponding to a unique singular value eigenvector.

Hence, we have designed a face recognition experimental system and implemented SVD algorithm basing on OpenCV (Open Source Computer Vision Library) platform. Our workgroup can analyze and validate the face recognition algorithms impact that facial images have been embedded watermarking on this experimental platform.

Next, we give the theoretical analysis about the error estimation factor after embedded watermarking, and reasons are as follows.

3.2 The error estimation factor

In order to evaluate the error estimation factor after embedded fragile digital watermarking, spectrum norm is firstly defined as :

We set $A \in R^{n\times n}$

$$\|A\|_2 = \sqrt{\lambda_{\max}} = S_{\max} \tag{9}$$

Equation (9) is the definition of spectrum norm. In this case, $\lambda_{\max}$ is the maximal eigenvalue of matrix $A^T A$, and $S_{\max}$ is the maximal singular value of matrix A .

Lemma 1:

If $U \in R^{n\times n}$ and $V \in R^{n\times n}$ are orthonormal matrix, and we set $A \in R^{n\times n}$. So we can result in

$$\|UAV\|_2 = \|A\|_2 \tag{10}$$

Lemma 2:

If we set aA to be the disturbance of matrix A , where $A \in R^{n\times n}$ is the matrix in Lemma 1. That is $\tilde{A} = A + aA$.

So $S_i(A)$ and $S_i(\tilde{A})$ are the i sequence singular values of matrix A and $\tilde{A}$, which arrange in step-down sequence. The formula can be written as:

$$\left| S_i(\tilde{A}) - S_i(A) \right| \leq \|aA\|_2 \tag{11}$$

Where the parameter i is the positive integer from number 1 to n, and $i = 1,2,.....,n$.

From the discussion in the previous Lemmas and definition, the conclusions are given as follows:

Matrix A is the original facial image, and $LSB(A)$ is LSB plane. Sign W represents watermarking, and $-LSB(A)+W$ is the error between watermarking and the original facial image which facial image LSB is transformed to zero.

And matrix $\tilde{A}$ is a facial image which has been embedded fragile digital watermarking. So, the error estimation factor after embedded watermarking is

$$\begin{aligned} &E\left|S_i(\tilde{A})-S_i(A)\right| = \left|S_i(A-LSB(A)+W)-S_i(A)\right| \\ &\le E\left\|W-LSB(A)\right\|_2 \le E\left\|W\right\|_2 \end{aligned} \tag{12}$$

Where W_{ij} satisfies the Bernoulli distribution. Therefore, $LSB(A)$ satisfies the same distribution with W_{ij} (Rafael et al., 2004). Especially that $LSB(A)$ is the LSB plane of A . It is clear that the singular value $\left|S_i(\tilde{A})-S_i(A)\right|$ is very little, and we can make a conclusion that it doesn't impact feature extraction, detection rate and detection speed of face recognition(Bernhard et al., 2002). The final experiments are provided to support above-mentioned theoretical analysis.

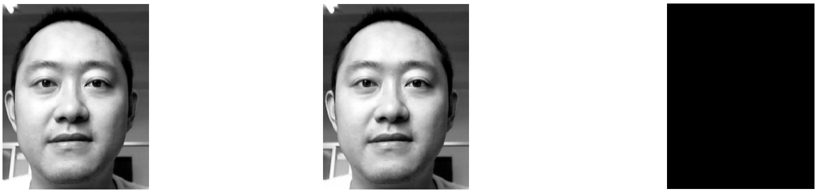
4. Experimental results

In this section, we present experimental results using above proposed method, including security experiments of facial image database and face recognition performance experiments after embedded watermarking. The experimental results are as follows:

4.1 Images security experiment

1. Valid Facial Images Database Detection

One original facial image of face recognition system database is shown in Fig.2 (a), and the image in Fig.2 (b) is the facial image embedded fragile digital watermarking. That is PSNR=51.1237. The results of detection are shown in Fig.2 (c). There isn't non-zero area in Fig.2 (c), so we can judge that this image is valid facial image of database.

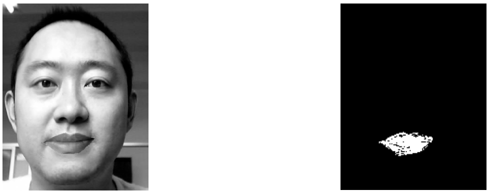


(a) Original image b) Image embedded watermarking (c) Result of authentication

Fig. 2. Valid facial image database detection

2. Tampered facial images detection

In this experiment, we use the image editor software "photoshop" to tamper the image in Fig.2 (b). We tamper the mouth of Fig.2 (b) with other person's mouth, as shown in Fig.3 (a). The result of detection is shown in Fig.3 (b), where there is non-zero centralized area. Because the shape of non-zero centralized area is a mouth, we can detect that mouth of image database has been tampered, and indicate the tampered location.



(a) Tempered image (b) Detection result

Fig. 3. Tampered facial image detection

3. Invalid Facial Images database Detection

If there is an invalid facial image of face recognition database in Fig.4 (a), the result of detection is shown in Fig.4 (b). The image of detection not only has random noise but also has not non-zero centralized area. So we can make a conclusion that the image in Fig.4 (a) is an invalid facial image of database.

(a) No watermarking image (b) Detection result

Fig. 4. Invalid facial image database detection

4.2 Face recognition algorithms impact after embedded watermarking

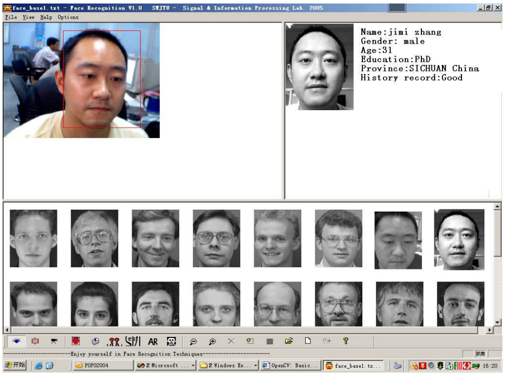
Finally, we have designed a face recognition experimental system and implemented SVD algorithm, EHMM algorithm and PCA algorithm basing on OpenCV. We can analyze and compare the face recognition algorithms impact after embedded watermarking.

In above three typical face recognition algorithms, we use ORL facial images database. There are 400 facial images in database, forty persons and each person has 10 images. We use first image to build facial feature, and 10 facial images are all used to recognition. The experimental results are as follows:

From all results, we see that the proposed method may not only indicate the tampered location, but also detect the validity of facial image of database. It improves the security of facial image database. Extensive experiments also indicate that it doesn’t impact feature extraction, detection rate and detection speed of face recognition using fragile digital watermarking.

Algorithm		Recognition accuracy	Detection rate	Time	Detection speed
SVD	No watermarking	330 images	82.5%	1.38 sec	0.00345 sec/image
	watermarked	329 images	82.255%	1.40 sec	0.0035 sec/image
EHMM	No watermarking	329 images	82.255%	52 sec	0.13 sec/image
	watermarked	328 images	82%	52.5 sec	0.1312 sec/image
PCA	No watermarking	343 images	85.75%	3 sec	0.0075 sec/image
	watermarked	340 images	85%	3.5 sec	0.00875 sec/image

Table 1. Shows face recognition algorithms impact after embedded watermarking. For comparison, we have finished SVD algorithm, EHMM algorithm and PCA algorithm experiments. From table 1, we see the impact of detection rate, detection time and detection speed is very little after embedded watermarking.



Name:jimi zhang
Gender: male
Age:31
Education:PhD
Province:SICHUAN China
History record:Good

---------------------Enjoy yourself in Face Recognition Techniques---------------------

Fig. 5. The experimental interface of face recognition algorithm impact after embedded watermarking

5. Conclusion

In this paper, we proposed a fragile digital watermarking for facial image database authentication, which not only can distinguish any minute tampers of facial image database but also detect the modification location. The watermarking has been used to resist various attacks on facial image database, such as tamper, substitution and addition form unlawful approach. We also give the theoretical analysis about the error estimation factor for identifying facial images embedded fragile digital watermarking. Experimental results show that the fragile digital watermarking technique has high sensitivity to tampers on the watermarked facial images, it not only can improve the security of the watermarked facial image database, but also will not impact feature extraction, detection rate and detection speed of face recognition.

6. Acknowledgements

The work is supported by the National Natural Science Foundation of China (Grant No.51175443) and the National Natural Science Foundation of China (Grant No.60971104).

7. References

Zhao, W.; Chellappa. R. & Phillips,P. J. (2000). Face Recognition: A Literature Survey", UMD CfAR Technical Report CAR-TR948.

Viola P.; Jones M.(2001). Rapid object detection using a boosted cascade of simple features, IEEE Proc. on computer vision and pattern recognition, 2001, IEEE Press: 511-518.

Gu, H.S.; Qiang, J. & Zhu, Z.W.(2002). Active Facial Tracking for Fatigue Detection, Proceedings of the Sixth IEEE Workshop on Applications of Computer Vision (WACV02),COMPUTER SOCIETY 2002 IEEE.

Zhang, X.H; Shan, S.G. & Gao,W.(2005). Evaluation and Analysis of Some Automatic Face Recognition Technologies, Application Research of Computer.

Su,J.X.(2002) Information analyzing mathematics and Artificial intelligence Pattern Recognition, GUO FANG KE JI University publishing company, No.5, May.2005.

He,H.J.; Zhang, J.S. & Tian.L.(2005). A Fragile Watermarking Scheme with Discrimination of Tampers on Image or Watermark, ACTA ELECTRONICA SINICA Vol.33 No.9, Sep. 2005.

Kutter. M.; Petitcolas,F. A. P.(1999). A fair benchmark for image watermarking systems, Electronic Imaging’99, Security and Watermarking of Contents, vol.3657,Sans Jose,CA,USA,25-27 Juuary, 1999.

Liu,R.Z.; Tan.T.N.(2001).SVD Based Digital Watermarking Method, ACTA ELECTRONICA SINICA, 2001, Vol.29(2)168-171.

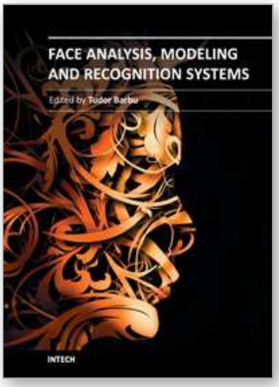
Wang,X.Q.; Yang,F.C. S.&Zhan, H.B. The System Design of MMS Material Copyright Distinguishing Based on Digital Watermarking Technique.

Zhou, D.L.; Gao, W.; Zhao D.B.(2003). Face Recognition Based on Singular Value Decomposition and Discriminant KL Projection, 2003 Journal of Software , Vol.14, NO.4.

Rafael, C.; Gonzalez, R.E .W(2004).Digital Image Processing Second Editon ,Publishing House Electronics Industry.2004.

Bernhard, F; Fröba, A.E(2004). Face Detection with the Modified Census Transform, Proceeding of the Sixth IEEE International Conference on Automatic Face and Gesture Recognition (FGR’04).

Bernhard, F; Fröba, A.E(2002). Robust Face Detection at Video Frame Rate Based on Edge Orientation Features, Proceedings of the Fifth IEEE International Conference on Automatic Face and Gesture Recognition (FGR’02).



ISBN 978-953-307-738-3
Hard cover, 212 pages
Publisher InTech
Published online 30, September, 2011
Published in print edition September, 2011

InTech Europe
University Campus STeP Ri
Slavka Krautzeka 83/A
51000 Rijeka, Croatia
Phone: +385 (51) 770 447
Fax: +385 (51) 686 166
www.intechopen.com

InTech China
Unit 405, Office Block, Hotel Equatorial Shanghai
No.65, Yan An Road (West), Shanghai, 200040, China
中国上海市延安西路65号上海国际贵都大饭店办公楼405单元
Phone: +86-21-62489820
Fax: +86-21-62489821