Available online at www.sciencedirect.com
SCIENCE DIRECT
Pattern Recognition 39 (2006) 910–920
PATTERN RECOGNITION
THE JOURNAL OF THE PATTERN RECOGNITION SOCIETY
www.elsevier.com/locate/patcog

Authenticating corrupted photo images based on noise parameter estimation

Sang-Woong Lee, Ho-Cheol Jung, Bon-Woo Hwang, Seong-Whan Lee*

Department of Computer Science and Engineering, Korea University, Anam-dong, Seongbuk-ku, Seoul 136-713, Korea

Received 31 August 2004; received in revised form 9 September 2005; accepted 20 September 2005

Abstract

Photo image authentication is an interesting and demanding field in the computer vision and image processing community. This research is motivated by its wide range of applications, which include smart card authentication systems, biometric passport systems, etc. In this paper, we propose a method of authenticating corrupted photo images based on noise parameter estimation. The proposed method first generates corrupted images by adjusting the noise parameters in the initial training phase. This set of corrupted images and the noise parameters can be represented by a linear combination of the prototypes of the corrupted images and the noise parameters. In the testing phase, the noise parameters of the corrupted photo image can be estimated with a corrupted image and an original image. Finally, we can make a synthesized photo image from the original photo image using the estimated noise parameters and verify it with the corrupted photo image. The experimental results show that the proposed method can estimate the noise parameters accurately and improve the performance of photo image authentication.

Keywords: Photo image authentication; Noise model; Corrupted photo image; Noise parameter estimation

1. Introduction

1.1. Motivation

Interest in photo image authentication has increased over the last few years. The photo image authentication market is currently expanding, and many fields, such as smart card authentication systems and biometric passport systems, are starting to use photo image authentication techniques for security reasons. For example, the immigration office in the airport matches a real face and a photo image on the passport. Criminals sometimes replace a photo image on the passport with their own image. In this case, officer cannot know this forgery passport. In this paper, photo image authentication refers to the verification of a scanned facial image of an identification card, passport or smart card based on its comparison with an original facial image contained in a database. This can be available assuming that the office has originally registered image. However, the scanned photograph used to be corrupted by real problems, such as scratch, blur and discoloration (Fig. 1). If a image was corrupted, it is very difficult to discriminate automatically between the corrupted image of same person and that of different person (Fig. 2). In fact, handling corrupted photo images is one of the most difficult and commonly occurring problems in image processing applications. In order to prevent a photo image from corruption, memory-on-card system appears recently. However, most of recent ID cards in the world have a photo image and it needs much time that most cards are changed to smartcard. This paper is for general cards with a photo image. Additionally, most of the current approaches to face authentication require at least two training images per person, in order to obtain good performance. Unfortunately, in real-world tasks, such a requirement cannot always be satisfied. Therefore, an authentication algorithm is needed to solve these problems.

* Corresponding author. Tel.: +82 2 3290 3197; fax: +82 2 926 2168.
E-mail addresses: sangwlee@image.korea.ac.kr (S.-W. Lee), hcjung@image.korea.ac.kr (H.-C. Jung), bwhwang@image.korea.ac.kr (B.-W. Hwang), swlee@image.korea.ac.kr (S.-W. Lee).

0031-3203/$30.00
doi:10.1016/j.patcog.2005.09.017

Fig. 1. Examples of photo images scanned from identification cards.

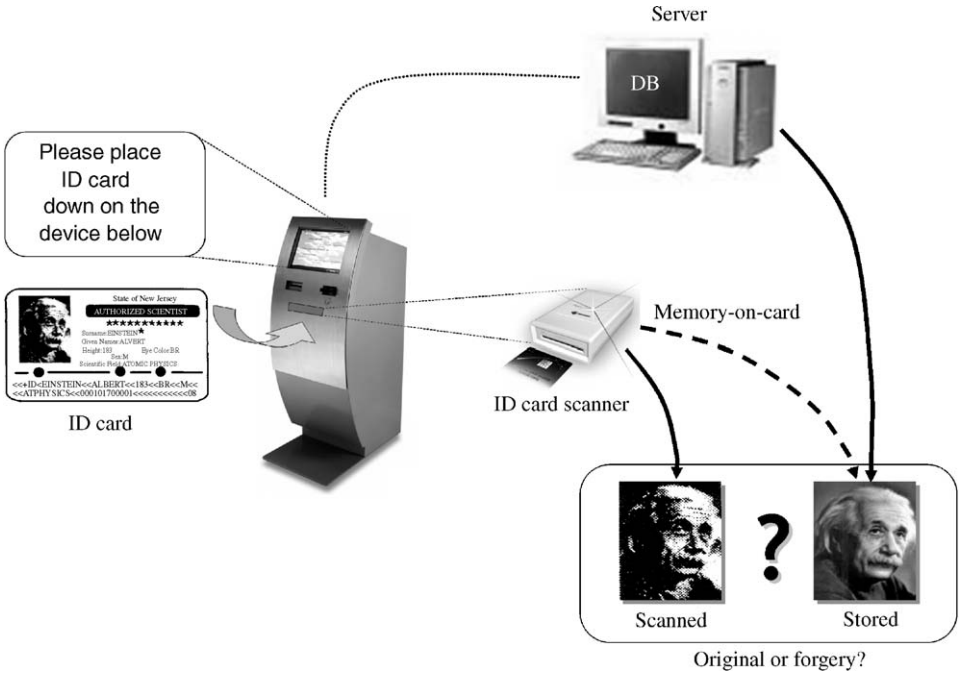


Fig. 2. Forgery discrimination system.

1.2. Paper outline

In this paper, in order to solve the above two problems, namely the corruption of photo images and the requirement of multiple training images per person, we propose an efficient photo image authentication method based on noise parameter estimation.

Our proposed method is different from previous approaches in the following two ways. Firstly, the proposed method performs efficient photo image authentication by estimating the noise parameters of the corrupted photo images using a noise model, whereas previous approaches performed authentication by extracting the robust features contained in the corrupted images [1,2]. Secondly, the proposed method is very useful for practical applications, because it allows the authentication to be accomplished with only one training image per person, in contrast to the existing approaches which require multiple training images [3–5].

The strategy that we adopt to authenticate corrupted photo images incorporates the following four steps. Firstly, noise models consisting of the corrupted image and noise parameters are generated from the training images. Secondly, linear coefficients are computed by decomposition of the noise model, and then the noise parameters are estimated by applying these coefficients to the linear composition of the noise parameters. Thirdly, a synthesized image is obtained by applying the estimated parameters to the original image contained in the database. Finally, photo image authentication is performed by matching the synthesized photo image and the corrupted photo image.

This paper is organized as follows: In Section 2, we provide a concise review of previous approaches to face authentication involving corrupted images. In Sections 3 and 4,

we describe the noise model used for noise parameter estimation and the method employed for photo image authentication, respectively. The experimental results obtained for the photo image authentication system are given in Section 5. Finally, in Section 6, we present conclusive remarks and briefly discuss some ideas for further research.

2. Related works

Research of face authentication has been carried out for a long time. In particular, several researchers have recently studied methods of dealing with corrupted images. In previous studies, modelling the properties of noise, as opposed to those of the image itself, has been used for the purpose of removing the noise from the image. However, these methods cannot remove noise that is distributed over a wide area, because they use only local properties. In addition, regions within the image which have similar noise properties are degraded in the process of removing the noise. Also, these methods cannot recover regions that are damaged by noise or occlusion. The corruption of photo images is a commonly occurring phenomenon, which is a source of serious problems in many practical applications such as face authentication. There are several approaches which can be taken to solve the noise problem and to eliminate the requirement of multiple training images per person. Herein, we introduce three popular approaches.

2.1. Robust feature extraction in corrupted image

Sanderson and Bengio [6] proposed a method of extracting robust features in various image conditions. To accomplish this, they proposed a new feature set, utilizing polynomial coefficients derived from 2D discrete cosine transform (DCT) coefficients obtained from horizontally and vertically neighboring blocks. The proposed feature set is superior (in terms of its robustness to illumination changes and discrimination ability) to the features extracted using previous methods. This method is based on robust feature extraction against Gaussian white noise and Gaussian illumination changes, however, it does not consider the question of which features are required for the purpose of authentication in images corrupted by scratch, blur and discoloration.

2.2. Reconstruction of partially corrupted image

Turk and Pentland [7] proposed a method of reconstructing noisy or missing parts of a partially corrupted face using eigenfaces based on principal component analysis (PCA). However, their method showed good results only when applied to an unknown face of a person for whom multiple images are available in the training set, or a face that was itself part of the initial training set.

Takahashi and Kurita [8] also proposed a method of removing noise using Kernel principal component analysis (KPCA). This method is able to remove outliers in data vectors and replace them with the values estimated via KPCA [9]. By repeating this process several times, it is possible to obtain feature components less affected by the outliers. This method is more effective at outlier removal than the standard method of PCA proposed in [7]. However, it is not efficient for real-time face authentication, because it takes too much time to remove the noise using the Kernel function.

2.3. Face authentication based on virtual view

Previous studies have focused on the utilization of training algorithms using multiple training images per person [3–5]. In many applications, however, only one sample image per person is available to the face authentication system [5]. Therefore, it is not possible to use statistical approaches, such as linear discriminant analysis (LDA) and support vector machines (SVM), which require at least two training images per person.

Because of these problems, many researchers have turned their attention to face recognition using virtual models. Beymer and Poggio [10] proposed the pose invariant face recognition method based on virtual views. These virtual views were generated using the concept of linear object classes. This method performs face recognition by synthesizing various virtual views from one example view. It offers good performance in relation to various kinds of poses, but difficulties are encountered in the case of virtual view generation for occluded regions.

3. Noise model

3.1. General characteristics of noise

Noise in an image can generally be grouped into two classes:

- Image independent noise.
- Image dependent noise.

Image independent noise can generally be described by an additive noise model, where the recorded image $f(i, j)$ is the sum of the true image $s(i, j)$ and the noise $n(i, j)$:

$$f(i, j) = s(i, j) + n(i, j).$$

The noise, $n(i, j)$, is often zero-mean and described by its variance, σ_n^2. The impact of the noise on the image is often described by the signal-to-noise ratio (SNR), which is given by

$$SNR = \frac{\sigma_s}{\sigma_n} = \sqrt{\frac{\sigma_f^2}{\sigma_n^2} - 1},$$

where σ_s^2 and σ_f^2 are the variances of the true image and the recorded image, respectively.

In many cases, the additive noise is evenly distributed over the frequency domain, whereas an image contains mostly low frequency information. Hence, the noise is dominant for high frequencies and its effects can be reduced using some kind of lowpass filter. This can be done using either a frequency filter or a spatial filter.

Image-dependent noise can be described by modelling noise with a multiplicative, or non-linear model.

3.2. Noise analysis in the case of corrupted images

There are infinite kinds of noise such as blur, speckles, stains, scratches, folding lines, etc. Actually, in corrupted photo images, most noise can be synthesized using the combination of adjustments of contrast, brightness, and Gaussian blur parameter. For instance, the corruption caused by many scratches looks like the blurred one. However, it needs another model or hierarchical analysis to represent locally corrupted images.

In this paper, we assume that the corruption of the images originates from changes in contrast, brightness, Gaussian noise and Gaussian blur.

Firstly, we define an image whose contrast and brightness are changed, as follows:

$$I_{CB}(x, y) = c \times I_{org}(x, y) + b, \tag{1}$$

where I_{CB} is the image corrupted by the change of contrast and brightness, I_{org} is the original image, c is the contrast parameter, and b is the brightness parameter.

Secondly, we define a corrupted image which is generated by applying Gaussian blur, as follows:

$$I_G(x, y) = I_{org}(x, y) * G_{blur}(x, y), \tag{2}$$

where G_{blur} is the Gaussian blur filter, and $*$ is the image convolution operator.

$$G_{blur}(x, y) = \frac{1}{2\pi\sigma^2} e^{-(x^2+y^2)/2\sigma^2}, \tag{3}$$

where σ in (3) is the Gaussian blur parameter. Fig. 3 shows examples of corrupted images so generated.

3.3. Definition of our noise model

In this section we will formally specify the noise model. We define the corrupted image, I^c, as follows:

$$I^c = I_{CB} * G_{blur}. \tag{4}$$

Then, more formally, the noise model is defined as the combination of corrupted images, I^c, and the noise parameters, P.

$$N_i = \begin{pmatrix} I_i^c \\ P_i \end{pmatrix} \quad (i = 1, \ldots, m), \tag{5}$$

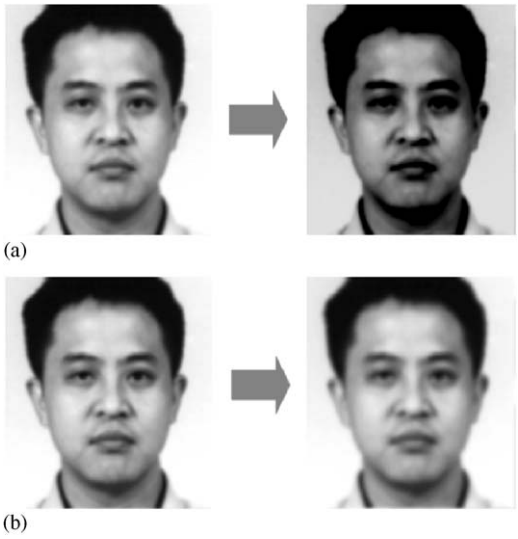


Fig. 3. Examples of corrupted images: (a) adjustment of contrast and brightness, (b) Gaussian blur.

where $I^c = (x_1, \ldots, x_k)^{\mathrm{T}}$, $P = (p_1, \ldots, p_l)^{\mathrm{T}}$. $x_1, \ldots, x_k$ are the intensities of the pixels in the corrupted image, k is the number of pixels in the corrupted image, p is the noise parameter value, l is the number of noise parameters used and m is the number of corrupted images. In this paper, we used $l = 3$, $p_1 = c$, $p_2 = b$, and $p_3 = \sigma$ since we consider the changes in contrast, brightness and Gaussian blur. Thus, the noise model, N, is represented as follows:

$$N = \bar{N} + \sum_{i=1}^{m-1} \alpha_i n_i(j), \quad (j = 1, \ldots, k, k+1, \ldots, k+l), \tag{6}$$

where $\bar{N}$ is the mean of N_i $(i = 1, \ldots, m)$. By PCA, a basis transformation is performed to an orthogonal coordinate system formed by eigenvector n_i of the covariance matrices on the data set of m corrupted images and noise parameters. The probability for coefficients $\vec{\alpha}$ $(\vec{\alpha} \in R^{m-1})$ is defined as:

$$p(\vec{\alpha}) \sim \exp\left[-\frac{1}{2}\sum_{i=1}^{m-1}\left(\frac{\alpha_i}{\xi_i}\right)^2\right], \tag{7}$$

where with ξ_i^2 being eigenvalues of the covariance matrix, C_s.

4. Photo image authentication

4.1. Overview

The proposed method involves the estimation of the noise parameters using the least squares minimization (LSM) method. Fig. 4 shows the overview of proposed procedure and Fig. 5 depicts the basic idea behind the noise parameter estimation method.

In order to authenticate corrupted photo images, the proposed method includes the following two phases, the

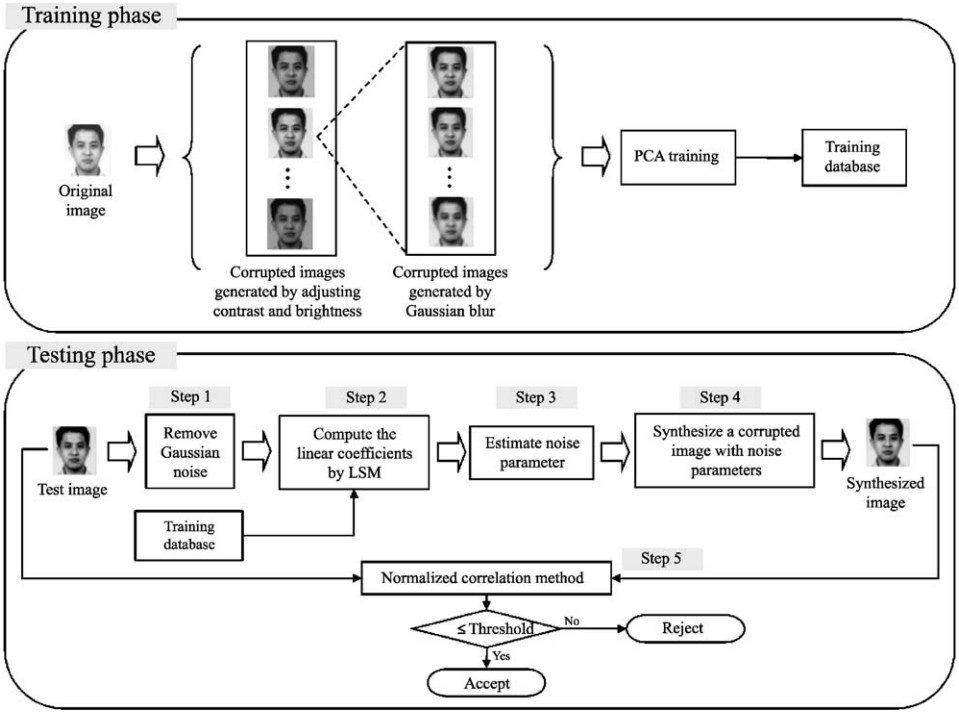


Fig. 4. Overview of authentication procedure.

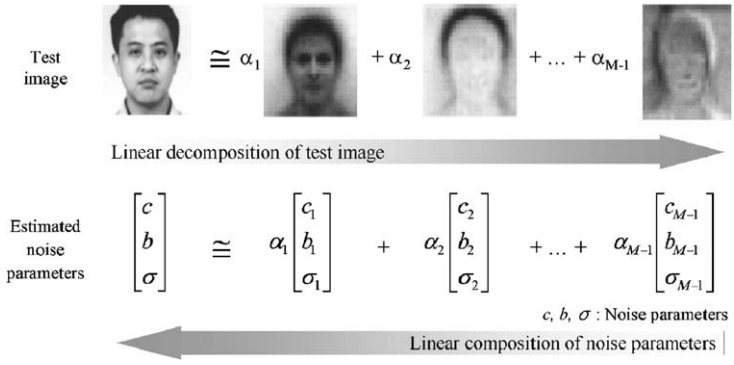


Fig. 5. Noise parameter estimation based on PCA.

training phase and testing phase. In the training phase, we first generate corrupted images by adjusting the parameters of contrast, brightness and Gaussian blur of an original photo image. Then, we obtain the basis vectors of the corrupted images and the noise parameters. In the testing phase, the photo image authentication procedure for the corrupted photo image is performed as follows:

- *Step* 1. Remove the Gaussian noise by using the Wiener filter for the test image.
- *Step* 2. Compute the linear coefficients of the sub-matrix of eigenvectors corresponding to the corrupted images obtained from the result image in Step 1, using the LSM method.
- *Step* 3. Estimate the noise parameters of the sub-matrix of eigenvectors corresponding to the noise parameters by using the obtained linear coefficients so obtained.
- *Step* 4. Synthesize the corrupted photo image by applying the estimated noise parameters to the original photo image.
- *Step* 5. Perform the photo image authentication between the test image and the photo image synthesized from original photo image obtained in Step 4.

In Step 1, we first remove the Gaussian noise contained in the test image by means of the Wiener filter. The Wiener filter is the classic linear noise reduction filter [11]. In Steps 2 and 3, the noise parameters are estimated by minimizing the error function using the least-square minimization method [12]. In Step 4, we generate a synthesized photo image for the purpose of photo image authentication. Finally, photo image authentication is performed using the normalized correlation method described in Step 5 [13].

4.2. Noise parameter estimation

Using the noise model, only an approximation of the required parameters can be obtained. The goal is to estimate the noise parameters by finding an optimal solution in such an overdetermined condition. At first, we want to find the value of α which satisfies Eq. (8).

$$\tilde{N}(j) = \sum_{i=1}^{m-1} \alpha_i n_i(j), \quad (j = 1, \ldots, k), \tag{8}$$

where j is the pixel in the corrupted image, k is the number of pixels in the corrupted image and the difference image is defined as $\tilde{N} = N - \bar{N}$. Generally, there may not exist any value of α that perfectly fits $\tilde{N}$. Therefore, we choose $\alpha^\star$ to minimize the error function described in Eq. (8).

To do this, we first define an error function, $E(\alpha)$, in Eq. (10), and set a condition to minimize the error function. The goal is to find the value of α which minimizes the error function, $E(\alpha)$, according to the following equation:

$$\alpha^\star = \arg\min_{\alpha} E(\alpha). \tag{9}$$

The error function is given as

$$E(\alpha) = \sum_{j=1}^{k} \left(\tilde{N}(j) - \sum_{i=1}^{m-1} \alpha_i n_i(j) \right)^2. \tag{10}$$

We then find the coefficient values that minimize the error function using the LSM method. According to Eqs. (9) and (10), we can solve this problem by the least-square method. Eq. (8) is equivalent to the following:

$$\begin{pmatrix} n_1(1) & \cdots & n_{m-1}(1) \\ \vdots & \ddots & \vdots \\ n_1(k) & \cdots & n_{m-1}(k) \end{pmatrix} \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_{m-1} \end{pmatrix} = \begin{pmatrix} \tilde{N}(1) \\ \vdots \\ \tilde{N}(k) \end{pmatrix}. \tag{11}$$

We can rewrite (11) as

$$\mathbf{I_N}\alpha = \tilde{\mathbf{I}}_\mathbf{N}, \tag{12}$$

where

$$\mathbf{I_N} = \begin{pmatrix} n_1(1) & \cdots & n_{m-1}(1) \\ \vdots & \ddots & \vdots \\ n_1(k) & \cdots & n_{m-1}(k) \end{pmatrix}, \quad \alpha = (\alpha_1, \ldots, \alpha_{m-1})^{\mathrm{T}},$$

$$\tilde{\mathbf{I}}_\mathbf{N} = (\tilde{N}(1), \ldots, \tilde{N}(k))^{\mathrm{T}}. \tag{13}$$

The least-squares solution to an inconsistent $\mathbf{I_N}\alpha^\star = \tilde{\mathbf{I}}_\mathbf{N}$ of k equation in $m-1$ unknowns satisfies $\mathbf{I_N^T I}\alpha^\star = \mathbf{I_N^T}\tilde{\mathbf{I}}$. If the columns of $\mathbf{I_N}$ are linearly independent, then $\mathbf{I_N^T}\tilde{\mathbf{I}}_\mathbf{N}$ has an inverse and

$$\alpha^\star = (\mathbf{I_N^T I_N})^{-1}\mathbf{I_N^T}\tilde{\mathbf{I}}_\mathbf{N}. \tag{14}$$

The projection of $\tilde{\mathbf{I}}_\mathbf{N}$ onto the column space is therefore $\hat{\mathbf{I}}_\mathbf{N} = \mathbf{I_N}\alpha^\star$. By using Eqs. (6) and (14), we obtain

$$N(j) \cong \bar{N}(j) + \sum_{i=1}^{m-1} \alpha_i^\star n_i(j), \quad (j = 1, \ldots, k), \tag{15}$$

where j is the pixel in the corrupted image and k is the number of pixels in the whole region of the photo image.

We previously made the assumption that the columns of $\mathbf{I_N}$ are linearly independent in Eq. (12). Otherwise, Eq. (14) may not be satisfied. If $\mathbf{I_N}$ has dependent columns, the solution represented by $\alpha^\star$ will not be unique, in which case we will have to choose a particular solution from among the possible ones. The optimal solution of $\hat{\mathbf{I}}_\mathbf{N} = \mathbf{I_N}\alpha^\star$ is the one that has minimum length according to Eq. (7). The optimal solution in this case can be obtained by calculating the pseudoinverse of $\mathbf{I_N}$ [14]. However, in our case, where the goal is to effectively estimate the noise parameters from a corrupted photo image, this is unlikely to happen.

To estimate the noise parameters, the linear coefficients are applied to the sub-matrix of eigenvectors corresponding to the noise parameters. Therefore, the estimated noise parameters can be defined as in Eq. (16).

$$P = \bar{N}(k+s) + \sum_{i=1}^{m-1} \alpha_i n_i(k+s), \quad (s = 1, \ldots, l). \tag{16}$$

4.3. Authentication

Given the test image and the original image, the purpose of photo image authentication is to decide if the test image is identical to the original image. In this work, we first remove the Gaussian noise from the test image. After estimating the noise parameter, P, for the test image, the synthesized image is obtained by applying P to the original image as described by Eqs. (1) and (2). Then, we used the normalized correlation method for the purpose of authenticating the test image with the synthesized image.

4.3.1. Normalized correlation method

Let f be an image of size $M \times N$ and, w be an image of size $J \times K$. Then, the correlation between $f(x, y)$ and $w(x, y)$ is

$$c(s, t) = \sum_x \sum_y f(x, y) w(x - s, y - t), \tag{17}$$

where $s = 0, 1, \ldots, M-1, t = 0, 1, \ldots, N-1$, and the summation is taken over the image region where w and f overlap. As s and t are varied, $w(x, y)$ moves around the image area, giving the function $c(s, t)$. The maximum value of $c(s, t)$ indicates the position where $w(x, y)$ best matches $f(x, y)$.

The correlation function has the disadvantage of being sensitive to changes in the amplitude of $f(x, y)$ and $w(x, y)$. An approach frequently used to overcome this difficulty is

to perform matching via the correlation coefficient, which is defined as

$$\tau(s,t)=\frac{\sum_x\sum_y[f(x,y)-\bar{f}][w(x-s,y-t)-\bar{w}]}{\sqrt{(\sum_x\sum_y[f(x,y)-\bar{f}]^2\sum_x\sum_y[w(x-s,y-t)-\bar{w}]^2)}}, \quad (18)$$

where $s=0,1,\ldots,M-1$, $t=0,1,\ldots,N-1$, $\bar{w}$ is the average value of the pixels in $w(x,y)$, $\bar{f}$ is the average value of $f(x,y)$ in the region coincident with the current location of w, and the summations are take over the coordinates common to both f and w. The value of the correlation coefficient $\tau(s,t)$ lies between -1 and 1, independent of scale changes in the amplitude of $f(x,y)$ and $w(x,y)$. We refer to (18) as normalized correlation. When f and w are face region images, $\tau(0,0)$ represents the similarity between the two photo images.

5. Experimental results and analysis

5.1. Experimental data and environments

To test the proposed method, we used the Korean Face Database (KFDB) introduced in [15] (Fig. 6) and photo images scanned from the identification cards of 150 persons with corresponding non-corrupted original images.

In order to use the scanned image, we should extract facial images from ID card. Fortunately, most of ID cards have a standard form and a set pattern, and a facial image in an ID card is put in a fixed location. With a little of information, facial images can be easily extracted. These facial images are normalized in terms of scale as the same size as non-corrupted images.

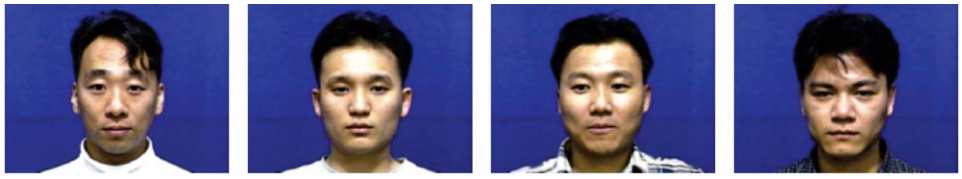
We used 100 persons for whom only one frontal image is included in the KFDB and, from these images, we generated 100 corrupted images containing simulated noise using the method introduced in Section 3.2.

Table 2 shows the noise parameters used to generate the corrupted images containing the simulated noise. In Table 1, parameter c represents the change in contrast, parameter b represents the change in brightness and σ is the parameter pertaining to Gaussian blur. We used all possible combinations of these parameters to estimate the unknown noise parameters.

We also tested the proposed algorithm against photo images scanned from identification cards (Fig. 7). The resolution of the images was 200 × 290 pixels and the color images were converted to 8-bit gray level images. Also, these 150 photo images were scanned with a 300 dpi scanner and resized to 200 × 290.

5.2. Experimental analysis

In the experiments, we performed the following three evaluations. First, we generated corrupted images containing simulated noise from the images contained in the KFDB



(a)

(b)

Fig. 6. Examples of frontal face images in KFDB: (a) original images, (b) corrupted images with simulated noise.

Table 1
Noise parameters used to generate corrupted images

	1	2	3	4	5	6	7	8	9	10
c	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9	1.0
b	−0.20	−0.15	−0.10	−0.05	0	0.05	0.10	0.15	0.20	0.25
σ	0.2	0.4	0.6	0.8	1.0	1.2	1.4	1.6	1.8	2.0

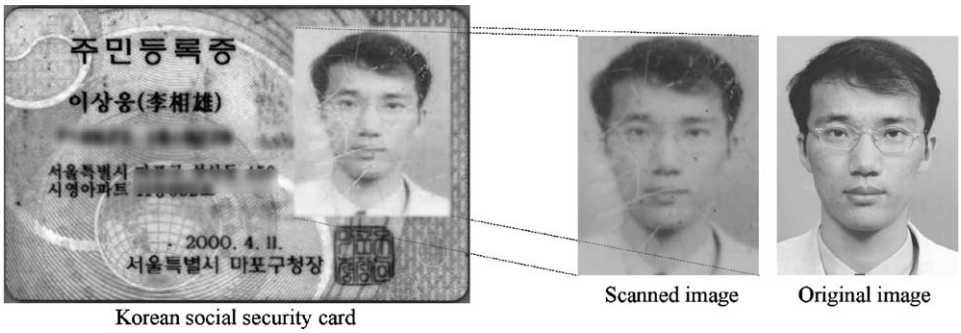


Fig. 7. Example of original image and corrupted photo images in identification cards.

Table 2
Noise parameter estimation for corrupted images with simulated noise

	1	2	3	4	5	6	7	8	9	10
c	0.23	0.38	0.45	0.64	0.49	0.12	0.35	0.45	0.82	0.93
c'	0.26	0.41	0.49	0.62	0.46	0.08	0.39	0.41	0.86	0.91
b	−0.040	0.045	−0.080	−0.08	−0.12	−0.07	0.240	0.220	−0.07	0.055
b'	−0.035	0.035	−0.095	−0.08	−0.11	−0.06	0.245	0.195	−0.09	0.065
σ	0.26	1.35	0.38	0.49	1.25	0.64	1.82	0.86	0.91	1.93
σ'	0.24	1.32	0.36	0.51	1.26	0.68	1.86	0.89	0.93	1.92

and estimated the noise parameters using these images. Second, we compared the image before the synthesis with the one after the synthesis of the corrupted image by the estimated noise parameters of the corrupted images including simulated noise for testing. In order to evaluate the performance, we used a normalized correlation method. Finally, we authenticated the photo images scanned from identification cards.

5.2.1. Experimental results for noise parameter estimation

In this experiment, we evaluated the accuracy of the proposed method by estimating the noise parameters of artificially corrupted images containing simulated noise. We estimated the noise parameters using corrupted images containing simulated noise, not including the training data. In the experiment on the corrupted images with simulated noise, the performance of the proposed method was evaluated 10 times, by observing the difference between the real noise parameters and the estimated noise parameters.

In Table 2, c, b, σ are the real parameters and the averages of c', b', σ' are the estimated parameters. Table 2 and Fig. 8 show the real parameters and the averages of the estimated parameters obtained using the proposed method with regard to the contrast, brightness and Gaussian blur, respectively. The experimental results show that the proposed method estimated the noise parameters accurately, since there is little or no error between the real and estimated noise parameters. Therefore the proposed method is accurate enough to use for the estimation of noise parameters for photo image authentication.

In this case, however, the estimation error of the noise parameters for the corrupted photo images depends on the number and the value of the noise parameters. Therefore, it is very important to use suitable parameters to generate the corrupted images.

5.2.2. Experimental results on comparison of the similarity

Fig. 9 shows the effectiveness of the proposed method in the corrupted images containing simulated noise, which were made from KFDB. We used a normalized correlation method to measure the similarity between the corrupted photo image and the synthesized photo image, as well as between the corrupted photo image and the original photo image. In Fig. 9, it can be seen that the similarity between the images after the estimation of the noise parameters is higher than that before the estimation of the noise parameters. As a result of this experiment, the proposed method was shown to provide an accurate method of estimating the noise parameters, as well as of improving the performance of photo image authentication. The performance of this method is expected to be particularly good in the case of corrupted photo images.

Fig. 10 shows the similarity between the images before and after noise parameter estimation, in the case of 33 images randomly selected among 150 photo images scanned from identification cards. In this experiment, we show that, in each case, the similarity between the synthesized photo image and the test image is generally higher than that between the original photo image and the test image. In the case of the real corrupted images, however, it is difficult to estimate the

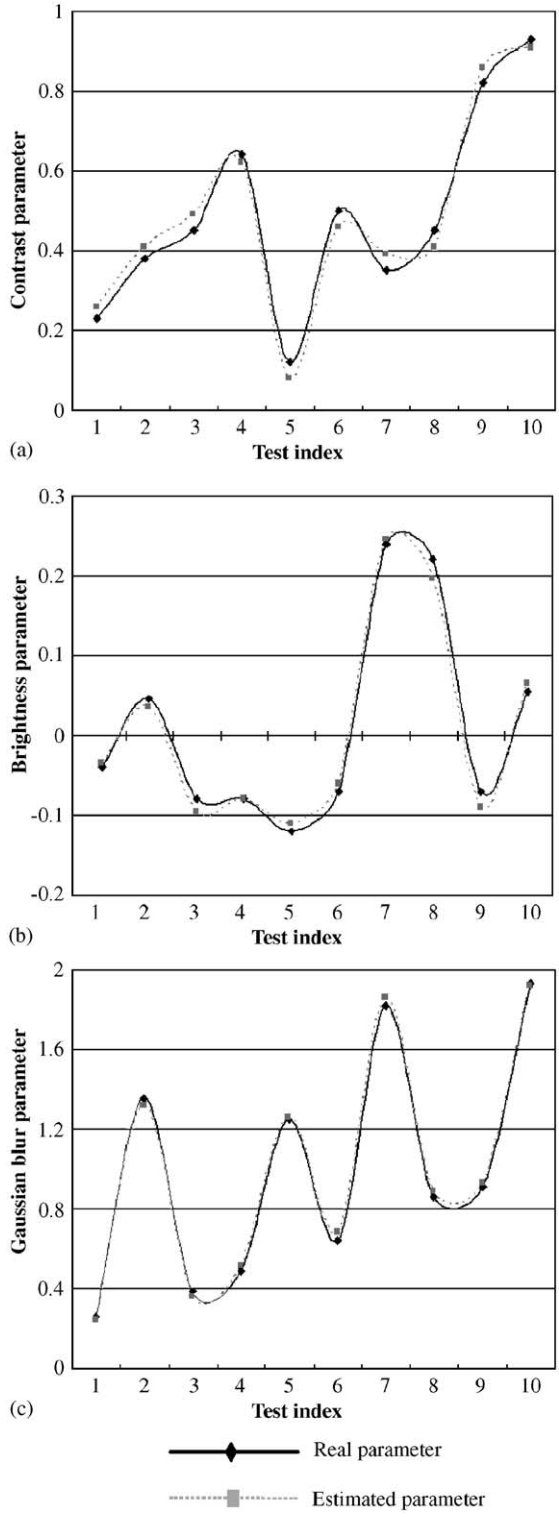


Fig. 8. Comparison of the real parameters and the estimated ones: (a) contrast parameter, (b) brightness parameter, (c) Gaussian blur parameter.

parameters accurately, due to the existence of various types of noise in the real data. Thus, the synthesized image by the parameter estimation is not identical to the test image scanned from identification card. Nevertheless, the proposed method increases the similarity by more than 5%.

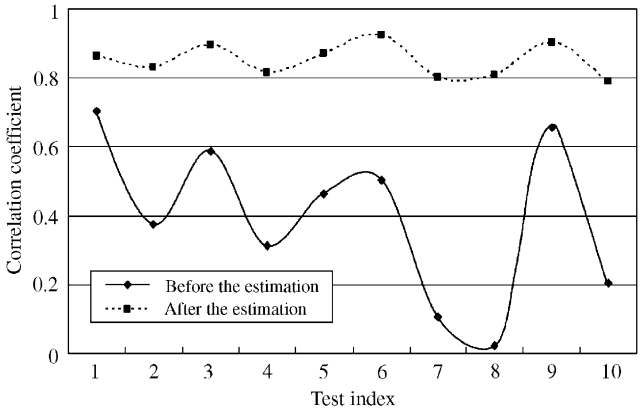


Fig. 9. Similarity between the images before and after the application of the noise parameters.

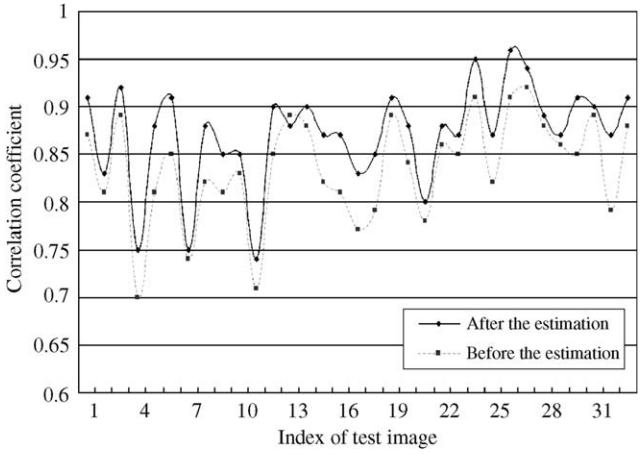


Fig. 10. Comparison of similarity between before and after the noise parameter estimation for randomly selected 33 test images.

Fig. 11 shows examples of the original images, test images and synthesized images, respectively. In Section 3, we defined noise models assuming that the corruption of the images is not locally appeared in images. As shown in Fig. 11, we could not reconstruct a variety of local corruptions such as sharp scratch, stains, fold lines, etc. However, it can be confirmed visually that the synthesized images are more similar to the test images than the original images are. Additionally, the correlation coefficients after the estimation are higher than those before the estimation.

5.2.3. Experimental results obtained for photo image authentication

Since the performance of authentication systems is measured in terms of the false reject ratio (FRR) achieved at a fixed false accept ratio (FAR) or vice versa, we can choose the operating point having $FAR = FRR$ by controlling the threshold. For safety critical applications, a low value of FAR is desirable. The best method is the one which provides

Fig. 11. Examples of original images, test images and synthesized images.

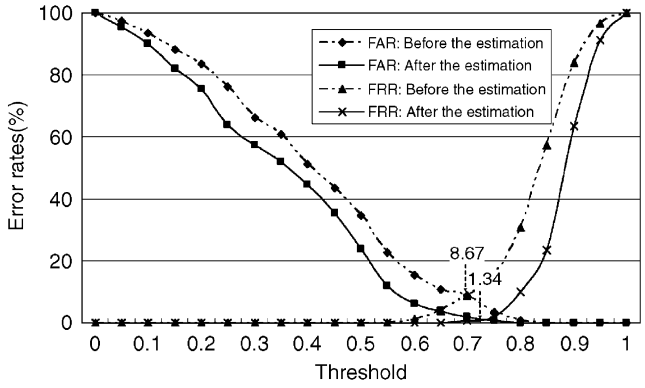


Fig. 12. ROC curve for threshold value used 150 images scanned from identification card.

the lowest FRR for a given FAR. For other applications, one might want the lowest FAR for a given FRR.

Fig. 12 shows the results of an experiment designed to authenticate real photo images. In order to find the equal error rate (EER), we repeatedly perform experiments with increase of the threshold value. In this figure, it can be seen that the EER is improved from 8.67% down to 1.34%. As a result of this experiment, we showed that the proposed method is more robust for authenticating corrupted photo images than before. Therefore, the proposed method can be applied to various fields of image processing such as photo image verification systems for credit cards and automatic teller machine transactions, smart card identification systems, biometric passport systems, etc.

6. Conclusions and further research

Herein, we proposed a new method of authenticating corrupted photo images based on noise parameter estimation. In order to authenticate corrupted photo images, the proposed method consists of the following two phases. Firstly, during the training phase, we generate corrupted images from an original image using various noise parameters and then we obtain the basis vectors of the corrupted images and noise parameters by PCA. Secondly, during the testing phase, the linear coefficients of the sub-matrix of eigenvectors corresponding to the corrupted images are computed by LSM. Then, the noise parameters are estimated by using the linear coefficients so obtained. Finally, the synthesized face image is generated by applying the estimated parameters to the original face image, and photo image authentication is performed by matching the synthesized photo image and the corrupted photo image.

In contrast to the previous techniques, the proposed method deals with the corrupted photo images based on noise parameter estimation and uses only one image per person for training. In this paper, we proved that the estimated parameter values are very close to the real ones. With the images obtained from the KFDB and photo images scanned from identification cards, the proposed method provided for the accurate estimation of the parameters and improved the performance of photo image authentication.

The experimental results show that the noise parameter estimation of the proposed method is quite accurate and that this method is very useful for authentication, because of its solving the noise problem of corrupted photo images. Also, the proposed method offers good performance in the case of corrupted photo images scanned from identification cards.

Further research is needed to develop a method of estimating partial noise parameters in a local region and generating various corrupted images for the purpose of accurate authentication. We expect that the proposed method will be applied to practical applications requiring photo image authentication, such as biometric passport systems and smart card identification systems.

Acknowledgements

This research was supported by the Intelligent Robotics Development Program, one of the 21st Century Frontier

R&D Programs funded by the Ministry of Commerce, Industry and Energy of Korea.

References

[1] C. Sanderson, K.K. Paliwal, Fast features for face authentication under illumination direction changes, Pattern Recognition Lett. 24 (14) (2003).
[2] F. Smeraldi, J. Bigun, W. Gerstner, Support vector features and the role of dimensionality in face authentication, Lecture Notes in Computer Science, Pattern Recogn. Support Vector Mach. (2388) (2002) 249–259.
[3] A.M. Martinez, A.C. Kak, PCA versus LDA, IEEE Trans. Pattern Anal. Mach. Intell. 23 (2) (2001) 229–233.
[4] P.N. Belhumeur, J.P. Hespanha, D.J. Kriegman, Eigenfaces vs. fisherfaces: recognition using class specific linear projection, IEEE Trans. Pattern Anal. Mach. Intell. 19 (7) (1997) 711–720.
[5] A.M. Martinez, Recognizing imprecisely localized, partially occluded, and expression variant faces from a single sample per class, IEEE Trans. Pattern Anal. Mach. Intell. 24 (6) (2002) 748–763.
[6] C. Sanderson, S. Bengio, Robust features for frontal face authentication in difficult image condition, in: Proceedings of International Conference on Audio- and Video-based Biometric Person Authentication, Guildford, UK, 2003, pp. 495–504.
[7] M. Turk, A. Pentland, Eigenfaces for recognition, J. Cognitive Neurosci. 12 (1) (1991) 71–86.
[8] T. Takahashi, T. Kurita, Robust de-noising by Kernel PCA, in: Proceedings of International Conference on Artificial Neural Networks, Madrid, Spain, 2002, pp. 739–744.
[9] B. Schölkopf, A. Smola, K.-R. Müller, Non-linear component analysis as a Kernel eigenvalue problem, Neural Comput. 10 (5) (1998) 1299–1319.
[10] D. Beymer, T. Poggio, Face recognition from one example view, in: Proceedings of International Conference on Computer Vision, Massachusetts, USA, 1995, pp. 500–507.
[11] K.R. Castleman, Digital Image Processing, Prentice-Hall, Englewood Cliffs, NJ, 1996, pp. 218–219.
[12] B.-W. Hwang, S.-W. Lee, Reconstruction of partially damaged face images based on a morphable face model, IEEE Trans. Pattern Anal. Mach. Intell. 25 (3) (2003) 365–372.
[13] M. Sadeghi, J. Kittler, K. Messer, A comparative study of automatic face verification algorithms on the BANCA database, in: Proceedings of International Conference on Audio- and Video-based Biometric Person Authentication, Guildford, UK, 2003, pp. 35–43.
[14] G. Strang, Linear Algebra and Its Applications, Harcourt Brace Jovanovich College Publishers, New York, 1988, pp. 442–451.
[15] B.-W. Hwang, H. Byun, M.-C. Roh, S.-W. Lee, Performance evaluation of face recognition algorithms on the Asian face database KFDB, in: Proceedings of International Conference on Audio- and Video-based Biometric Person Authentication, Guildford, UK, 2003, pp. 557–565.

About the Author—SANG-WOONG LEE received his B.S. degree in Electronics and Computer Engineering from Korea University, Seoul, Korea, in 1996, and his M.S. degrees in Computer Science and Engineering from Korea University, Seoul, Korea, in 2001. Currently, he is a Ph.D. candidate at the Department of Computer Science and Engineering, Korea University, Korea. His present research interests include face recognition, gesture recognition and robot vision.

About the Author—HO-CHOUL JUNG received his B.S. degree in Control and Instrumentation Engineering from Seoul National University of Technology. Currently, he is a M.S. degree candidate at the Department of Visual Information Processing, Korea University, Korea. His present research interests include face authentication, principal component analysis, support vector machines and their applications in face recognition, computer vision and the pattern recognition related fields.

About the Author—BON-WOO HWANG received his B.S. and M.S. degrees in Electronic Engineering from SungKyunKwan University, Seoul, Korea, in 1995 and 1997, respectively; and Ph.D. degree in Science and Engineering from Korea University, Seoul, Korea in 2002. In May 2001, he joined Virtualmedia, Seoul, Korea and he was the director of research center. Currently he is a postdoctoral fellow at the Robotics Institute of Carnegie Mellon University, Pittsburgh, USA. His research interests include face recognition, image processing, and computer vision.

About the Author—SEONG-WHAN LEE received his B.S. degree in Computer Science and Statistics from Seoul National University, Seoul, Korea, in 1984, and his M.S. and Ph.D. degrees in computer science from KAIST in 1986 and 1989, respectively. From February 1989 to February 1995, he was an assistant professor in the Department of Computer Science at Chungbuk National University, Cheongju, Korea. In March 1995, he joined the faculty of the Department of Computer Science and Engineering at Korea University, Seoul, Korea, as an associate professor, and he is now a full professor. He was the winner of the Annual Best Paper Award of the Korea Information Science Society in 1986. He obtained the First Outstanding Young Researcher Award at the Second International Conference on Document Analysis and Recognition in 1993, and the First Distinguished Research Professor Award from Chungbuk National University in 1994. He also obtained the Outstanding Research Award from the Korea Information Science Society in 1996. He has been the associate editor of the Pattern Recognition Journal, the International Journal of Pattern Recognition and Artificial Intelligence, the International Journal on Document Analysis and Recognition, and the International Journal of Computer Processing of Oriental Languages. He is a fellow of IAPR, a senior member of the IEEE Computer Society and a life member of the Korea Information Science Society and the Oriental Languages Computer Society. His research interests include pattern recognition, computer vision and intelligent robots. He has published more than 200 publications in these areas in international journals and conference proceedings, and has authored five books.