Communications on Applied Electronics (CAE) – ISSN : 2394-4714
Foundation of Computer Science FCS, New York, USA
Volume 3– No.3, October 2015 – www.caeaccess.org

Image Encryption by PCA

Mohammad Mofarreh-Bonab
University of Bonab
Electrical and Electronic Engineering department,
University of Bonab, Bonab, East Azarbaijan, Iran

Mostafa Mofarreh-Bonab
Shahid Beheshti University
Electrical and Electronic Department, Shahid Beheshti University, Velenjak, Tehran, Iran

ABSTRACT
Besides ever increasing digital world, the importance of information security aspects becomes increasingly clear day by day. Several solutions are introduced to provide the required security for various applications and encryption is one of these solutions [2]. In image encryption, conventional algorithms encounter some kinds of complexity due to high amount of data that should be processed. In this paper, a new method is introduced for image encryption using PCA method. This algorithm is more advantageous especially in applications that integrity of database is more important, such as a prison and the prisoner's photo database. In such cases, the security system should provide two major requirements:1) avoid changing an image in the database and 2) hiding real images from unauthorized access. The simulation results show that the mentioned method is capable to manage these two requirements properly.

General Terms
Encryption, Security, Principal Component Analysis

Keywords
Encryption, security, database, image, storage, PCA, Eigen face

1. INTRODUCTION
Rapid growth of computer networks and other digital portable devices such as smart phones and cameras, has introduced great security and storage challenges to this industry [4]. Many methods have introduced to deal with these challenges. Each method have its benefits and some defects that make them suitable or inappropriate for special applications. By taking compression and encryption simultaneously into account, these systems can be more practical. As an example, in [5] S. S. Maniccam et al. have presented an image encryption system using SCAN pattern [2]. In this paper, we use the fact that PCA method transfers data into another domain in the way that each element of transformed domain is related to the all image database.So any change in images results in change in entire transformed domain data. This issue can satisfy the first requirement of supposed system. Incorporating some cryptography techniques such as permutation or more complicated cryptography algorithms such as chaotic based methods [6] can satisfy the second requirement.

2. PCA METHOD
PCA is a statistical tool which has many applications especially in database processing [1]. Suppose there are M square N*N monochrome images. This obligation doesn't make any restriction for colored and non-square images, since colored non-square images can be supposed as 3 square monochrome images. By reshaping the square matrix of phosphorescence of images, these images can be expressed as 1*N2 vectors Fi in equation (1-1). In proposed approach, images are transferred to another field. All images are put in X matrix that its elements are the phosphorescence of images.

$$X = \begin{bmatrix} F_1 \\ \vdots \\ F_M \end{bmatrix}_{M\times N^2}, F_i = (x_{i1}, x_{i2}, \dots, x_{iN^2}) \qquad \text{Eq 1-1}$$

That Fi indicates the i[th] image that converted to a vector. Now, PCA method can be applied to X matrix. PCA for images called KL transform or HOTELLING transform, too.

Before applying KL transform, we make some definitions.

The mean matrix,$\bar{M}_x$: that contains mean values of each image and expressed as:

$$\bar{\mathrm{M}}_{\mathrm{x}} = \frac{1}{\mathrm{M}}\begin{bmatrix} \sum_{\mathrm{k=1}}^{\mathrm{N^2}} \mathrm{x_{1,k}} \\ \sum_{\mathrm{k=1}}^{\mathrm{N^2}} \mathrm{x_{2,k}} \\ . \\ . \\ \sum_{\mathrm{k=1}}^{\mathrm{N^2}} \mathrm{x_{M,k}} \end{bmatrix}_{\mathrm{M\times 1}} = \begin{bmatrix} \mathrm{m_1} \\ \mathrm{m_2} \\ . \\ . \\ \mathrm{m_M} \end{bmatrix} \qquad \text{Eq 1-2}$$

$\widetilde{M}_x$is the matrix that contains the values of $\bar{M}_x$ M times and expressed as:

$$\widetilde{M}_x = [\bar{M}_x, \quad \bar{M}_x, \quad \bar{M}_x, \dots, \bar{M}_x]_{M\times N^2}$$

Covariance matrix C_x for M vectors:

$$C_x = [c_{i,j}]_{M\times M}$$

$$c_{i,j} = \frac{1}{N^2-1} \times \sum_{k=1}^{N^2} \left[(x_{i,k} - \bar{M}_x(i,1)) \times (x_{j,k} - \bar{M}_x(j,1))\right]$$

For applying KL transform, M eigenvectors v_i , $i = 1,2,\dots,M$ and M eigenvalues λ_i , $i = 1,2,\dots,M$ can be found, which satisfy equation (1-3):

$$\forall i \in \{1,2,\dots,M\} C_x.v_i = \lambda_i.v_i$$

$$v_i = \begin{bmatrix} v_1(i) \\ v_2(i) \\ \vdots \\ v_M(i) \end{bmatrix} \qquad \text{Eq (1-3)}$$

Eigenvectors can build a matrix called V or modal as below:

$$V = [v_1, v_2, \dots, v_M]^T{}_{M\times M}$$

So:

$$\Rightarrow V = \begin{bmatrix} v_1(1) & \cdots & v_M(1) \\ \vdots & \ddots & \vdots \\ v_1(M) & \cdots & v_M(M) \end{bmatrix}_{M\times M} \qquad \text{Eq (1-4)}$$

Communications on Applied Electronics (CAE) – ISSN : 2394-4714
Foundation of Computer Science FCS, New York, USA
Volume 3– No.3, October 2015 – www.caeaccess.org

Applying KL transform makes Y matrix:

$$Y = V.\left(X - \tilde{M}_x\right) \qquad \text{Eq (1-5)}$$

3. PCA METHOD FOR IMAGE ENCRYPTION

The mentioned approach in this paper is based on saving V and Y matrix instead of real images. If equation (1-4) expressed in matrixes, we have:

$$Y_{M\times N^2} = \begin{bmatrix} v_1(1) & \cdots & v_M(1) \\ \vdots & \ddots & \vdots \\ v_1(M) & \cdots & v_M(M) \end{bmatrix}_{M\times M} \times$$

$$\left(\begin{bmatrix} X_{11} & \cdots & X_{1N^2} \\ \vdots & \ddots & \vdots \\ X_{M1} & \cdots & X_{MN^2} \end{bmatrix}_{M\times N^2} - \begin{bmatrix} m_1 & \cdots & m_1 \\ \vdots & \ddots & \vdots \\ m_M & \cdots & m_M \end{bmatrix}_{M\times N^2} \right)$$

Y matrix transferred the images to another field and we can call any rows of Y as an image that reshaped to a vector. These images called Eigen faces that produced based on all the images of database jointly. This concept means that changing an image in the database results to changes in Y and V matrixes and since recovery of real images needs Y and V matrixes, so the whole database has been changed. It's clear that by applying KL transform conceivability of changing some images in the database without any results on other images is impossible. For strengthen the security of M, Y and V matrixes, we can apply a cryptography algorithms -such public key algorithm- to mentioned matrixes and decrease the accessibility of database as well as possible.

Images that results from Y matrix have some properties that make them individual [1];

- Each image is based on all the other images in the database and if one of them has been changed, the C_x matrix will be changed and as a result, all the Y elements will be changed.
- Because the images of Y matrix derive from all the real images -and not from one of them- so these images don't have any similarity to real images of database, so recognition of individual image is impossible.
- Saving Y, V and $\tilde{M}_x$ matrix, if any of their elements has been changed, all the retrieved images will be changed and unauthorized access to database will be clear.

4. SIMULATION RESULTS

In this paper, 40 face images of ORL database have been selected. All of these images are monochromic images and are face images from different nationalities. These images are shown in figure 1:

Figure 1: 40 face images from ORL database for simulation

Applying KL transform to these images results in Eigen faces shown in figure 2.

Figure 2: Eigen faces derived from ORL

And if a simple encryption algorithm like exchanging the rows of Y, M and V matrixes [3], these Eigen faces have been changed too and recognition of the images is harder than previous. Figure 3 shows the result of this exchange:

Figure 3: the effect of exchanging rows of Y, M and V matrix

From histogram point of view, the histogram of encrypted images has a Gaussian distribution and is shown in figure 4.

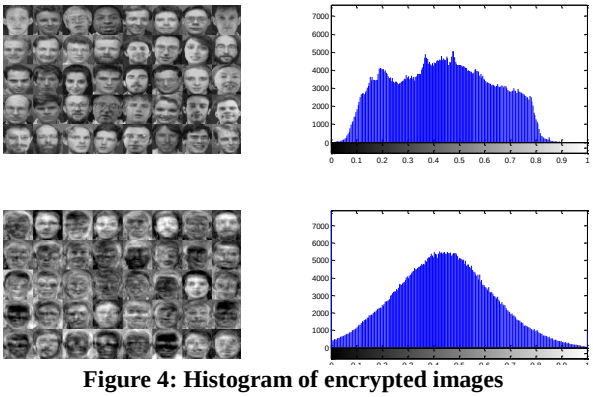

Figure 4: Histogram of encrypted images

5. CONCLUSION

In this paper, a new method for image encryption has been introduced which not only encrypts the images from unauthorized access, but also prevent changing the images into fake ones. This method is used in such way that applying a tiny change in one of the images in the database will lead to huge changes in all the database images. As a result, least changes in any members of the database is easily detectable by the security system.

6. REFERENCES

[1] Mostafa Mofarreh-Bonab, Mohamad Mofarreh-Bonab, "Face Database Compression by Hotelling Transform using a New Method" 2nd World Conference on Information Technology (WCIT-2011), Bahcesehir University & Near East University, Antalya, Turkey, November 23-26, 2011

[2] AditeeGautam, MeenakshiPanvar, P. R. Gupta, "A New Image Encryption Approach Using Block Based Transformation Algorithm"International Journal of Advanced Engineering Sciences and Technologies (IJAEST),Vol No. 8, Issue No. 1, 090 - 096.

[3] SeshaPallaviIndrakanti, P. S. Avadhani, "Permutation based Image Encryption Technique" International Journal of Computer Applications IJCA, vol. 28, No. 8, 2011.

[4] Linhua Zhang, Xiaofeng Liao,Xuebing Wang, "An Image Encryption Approach Based on Chaotic Maps"Chaos, Solitons and Fractals 24 (2005) pp: 759–765

[5] S. S. Maniccam, N. G. Bourbakis, "A Lossless Image Compression and Encryption using SCAN", Pattern Recognition 34 (2001), 1229-1245

[6] Chen, Guanrong, Yaobin Mao, and Charles K. Chui. "A symmetric image encryption scheme based on 3D chaotic cat maps." Chaos, Solitons & Fractals 21.3 (2004) pp. 749-761.