

## Research Article

### Performance of Data Images Encryption Based Karhunen-Loeve Transforms

<sup>1</sup>Hind Rustum Mohammed Shaban, <sup>2</sup>Inaam R. Alsaiq and <sup>1</sup>Alaa Abdul Hussein Mezher

<sup>1</sup>Computer Science Department,

<sup>2</sup>Mathematics Department, Faculty of Computer Science and Maths, Kufa University, Najaf, 54001, Iraq

**Abstract:** The purpose of this study encryption method will apply on all parts image by the Karhunen-Loeve Transform (KLT). It will be discussed time complexity and storage complexity in method (database consists of 40 images). The Karhunen-Loeve Transform (KLT) is always used in image processing and it has a wide application area. It was called "the best transform" because the decorrelation, energy concentration and Mean Square Error (MSE) is very small. The first step is found The Characteristics of the (KLT) by convert image matrix to elements vector, the second step found the covariance matrix, then compute its Great ability of decorrelation. Finally, we will reconstruct the de-noising matrix to the Image by KLT. The experimental results and security analysis confirm the effectiveness of the indicates the robustness and advantages of the algorithm.

**Keywords:** Encryption algorithms, encryption data images, encryption decryption algorithm, karhunen-loeve transforms, mathematics module

## INTRODUCTION

The necessity of information protection within a community has submitted large changes. We use data processing equipment before the widespread use, the safety of precise documents count on filing cupboard with a collection lock for saving paper-filling files or documents. In whatever way, in spite of the advanced of the computer in dealings action in the community the scenario has changed. Together, the action community worldwide working together as one structure because of advances in networking and communication technology (Salleh *et al.*, 2003).

Data protection is very important so dataencoding is one of the great used technicality. Data Encryption data is converted into from its original to another form therefore cannot be regained from the data decrypting the data. Original data is Indicate as Shares data and the transformed form is called cipher data. Encryption technique change in form data into encrypted form whom can be decrypted by the receiver only who gets data about the decoding of the ciphered data. For data protection, the encoding can be applied to text, image and video. In the suggest work Encoding is harness to promote image security. For data protection, dataencoding is one of the widely used techniques (Divya *et al.*, 2012).

Varied data have been submitted and great used encryption algorithms, like AES, RSA, or IDEA generality of whom are used in the text or binary data.

The reason of high correlation among pixels, it is difficult to use them straightaway in multimedia data and inactive for color image encryption. For multimedia data are often times of the high multitude, of large volumes and demand real-time influence (Kaur and Singh, 2013).

The Karhunen-Loeve Transform (KLT) is the proceeding mathematical procedure obtainable in the year (2008) to obtain both noise filtering and data compression in processing signals of any kind (Salleh *et al.*, 2003).

## MATERIALS AND METHODS

It is used to encrypt the values images using a mathematical model, has been applied in the Department of Computer Science as research results send to you

**Karhunen-loeve transforms:** Karhunen-Loeve Transform (KLT) that was based on statistical-based properties. The memorable usefulness of KLT is a good decorrelation. Under measuring, MSE (Mean Square Error) is the best transform, because it is always used in image processing (Jin and Gaoding, 2012).

The basic of the (KLT) is the orthogonal transform and abolish correlation. Assume random vectors  $x_1$ ,  $x_2$  and  $x_3$ , respectively, these are the vector for a point in

**Corresponding Author:** Hind Rustum Mohammed Shaban, Computer Science Department, Faculty of Computer Science and Maths, Kufa University, Najaf, 54001, Iraq

This work is licensed under a Creative Commons Attribution 4.0 International License (URL: <http://creativecommons.org/licenses/by/4.0/>).

each of all images. There are three values can be explicit in the construct of a three dimension column  $x$  where (Gonzalez and Woods, 1992):

$$x = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix}$$

If we have  $n$  recorded images, the vectors will be  $n$ -dimensional:

$$x = \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} \quad (1)$$

The proposition of element of column converts to arow vector. We can write the vectors as:

$$x = (x_1, x_2, \dots, x_n)^T$$

We can process the vectors as random quantities, then we can be written the mean vector as:

$$m_x = E\{x\} = \frac{1}{k} \sum_{n=1}^k x_n \quad (2)$$

Such that  $E\{\cdot\}$  Means "expected value", the  $x$  means that  $m_x$  harmonize a set of random vectors. The covariance matrix of the random vector can be defined as (Jin and Gaoding, 2012):

$$C_x = E\{(x - m_x)(x - m_x)^T\} \\ = \frac{1}{k} \sum_{n=1}^k x_n x_n^T - m_x m_x^T \quad (3)$$

$$= \begin{bmatrix} c_{11} & c_{12} & \dots & c_{1n} \\ c_{21} & c_{22} & \dots & c_{2n} \\ \vdots & \vdots & \dots & \vdots \\ c_{n1} & c_{n2} & \dots & c_{nn} \end{bmatrix}$$

The element  $c_{ij}$  is the covariance between the vector  $x_i$  of  $i$ -Th part of a vector and the vector  $x_j$  of  $j$ -th part of the vector. The covariance is zero if elements  $x_i$  and  $x_j$  are not correlation, therefor,  $c_{ij} = c_{ji} = 0$ . Because of  $x$  is  $n$ -order, the covariance matrix  $C_x$  is  $n \times n$  order. The matrix is real and symmetric matrix (Jin and Gaoding, 2012).

To explain the mechanics of Eq. (2) and (3), suppose the four vectors:

$$x_1 = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}, x_2 = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}, x_3 = \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix}, x_4 = \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix}$$

Applying Eq. (2) to compute the mean vector:

$$\text{Then } m_x = \frac{1}{4} \begin{bmatrix} 3 \\ 1 \\ 1 \end{bmatrix} \text{ and so } m_x m_x^T = \frac{1}{16} \begin{bmatrix} 9 & 3 & 3 \\ 3 & 1 & 1 \\ 3 & 1 & 1 \end{bmatrix}$$

To calculate  $C_x$  must be found  $E\{xx^T\}$ :

$$x_1 x_1^T = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}, x_2 x_2^T = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

$$x_3 x_3^T = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix}, x_4 x_4^T = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 0 & 0 \\ 1 & 0 & 1 \end{bmatrix}$$

$$\text{Then } E\{xx^T\} = \frac{1}{4} \begin{bmatrix} 3 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix}$$

It follows that  $C_x = E[m_x m_x^T] - E[xx^T]$

$$C_x = \frac{1}{4} \begin{bmatrix} 3 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix} - \frac{1}{16} \begin{bmatrix} 9 & 3 & 3 \\ 3 & 1 & 1 \\ 3 & 1 & 1 \end{bmatrix} = \frac{1}{16} \begin{bmatrix} 3 & 1 & 1 \\ 1 & 3 & -1 \\ 1 & -1 & 3 \end{bmatrix}$$

All the elements along the main diagonal are equal, which indicates that the three components of the vectors in the population have been the same variance,  $x_1$  and  $x_2$ , add to  $x_1$  and  $x_3$ , are a positive correlation; elements  $x_2$  and  $x_3$  are negative correlation (Jin and Gaoding, 2012).

Let  $e_i$  and  $\lambda_i, i = 1, 2, \dots, n$ , be the eigen vectors and corresponding eigen values of the matrix  $C_x$  and satisfies  $C_x e_i = \lambda_i e_i$ .

$A$  is convert  $x$ 's into vectors denoted by  $y$ 's, as follows:

$$y = A(x - m_x) \quad (4)$$

It is called the Karhunen-Loeve transform hence this choice of transformation matrix define the Hotelling transform. In my example to find matrix  $A$ , we will find the eigenvalues and eigenvectors for covariance matrix  $C$ .

$$\lambda_1 = 0.0625, \text{ the eigenvector } \begin{bmatrix} -0.5774 \\ 0.5774 \\ 0.5774 \end{bmatrix}$$

$$\lambda_2 = 0.25, \text{ the eigenvector } \begin{bmatrix} -0.1543 \\ -0.7715 \\ 0.6172 \end{bmatrix}$$

$$\lambda_3 = 0.25, \text{ the eigenvector } \begin{bmatrix} 0.8018 \\ 0.2673 \\ 0.5345 \end{bmatrix}$$

Then the matrix  $A$  will be:

$$A = \begin{bmatrix} 0.8018 & 0.2673 & 0.5345 \\ -0.1543 & -0.7715 & 0.6172 \\ -0.5774 & 0.5774 & 0.5774 \end{bmatrix}$$

Now, we will find the Karhunen-Loeve transform by Eq. (4):

$$x_1 - m_x = \begin{bmatrix} -\frac{3}{4} \\ -\frac{1}{4} \\ \frac{1}{4} \\ -\frac{1}{4} \end{bmatrix}, \quad x_2 - m_x = \begin{bmatrix} \frac{1}{4} \\ -\frac{1}{4} \\ -\frac{1}{4} \\ -\frac{1}{4} \end{bmatrix}$$

$$x_3 - m_x = \begin{bmatrix} \frac{1}{4} \\ \frac{3}{4} \\ \frac{1}{4} \\ -\frac{1}{4} \end{bmatrix}, \quad x_4 - m_x = \begin{bmatrix} \frac{1}{4} \\ -\frac{1}{4} \\ -\frac{1}{4} \\ \frac{3}{4} \end{bmatrix}$$

We find the vectors y from Eq. (4) as follows:

$$y_1 = A(x_1 - m_x) = \begin{bmatrix} -0.8018 \\ 0.1543 \\ 0.1443 \end{bmatrix}$$

$$y_2 = A(x_2 - m_x) = \begin{bmatrix} 0 \\ 0 \\ -0.4330 \end{bmatrix}$$

$$y_3 = A(x_3 - m_x) = \begin{bmatrix} 0.2673 \\ -0.7715 \\ 0.1443 \end{bmatrix}$$

$$y_4 = A(x_4 - m_x) = \begin{bmatrix} 0.5345 \\ 0.6172 \\ 0.1443 \end{bmatrix}$$

KLT has three characteristics: (Jin and Gaoding, 2012)

- We can show that the mean of the y vectors give rise to this transformation is zero; that is:

$$m_y = E\{y\} = 0$$

Proof:  $m_y = E\{y\} = E\{A(x - m_x)\}$   
 $= AE\{x\} - Am_x = Am_x - Am_x = 0$

- The covariance matrix of the y's is given by the expression

$$C_y = AC_xA^T$$

Proof:

$$C_y = E\{(y - m_y)(y - m_y)^T\}$$

$$= E\{yy^T\} \text{ Where } (m_y = 0)$$

$$= E\{(Ax - Am_x)(Ax - Am_x)^T\}$$

$$= E\{A(x - m_x)(x - m_x)^T A^T\}$$

$$= AE\{(x - m_x)(x - m_x)^T\}A^T$$

$$= AC_xA^T$$

- The covariance matrix  $C_y$  is a diagonal matrix:

$$C_y = \begin{bmatrix} \lambda_1 & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & \lambda_n \end{bmatrix}$$

Proof:

Since A is generated by  $C_x = E\{(x - m_x)(x - m_x)^T\}$  Eigenvector, so  $C_y = AC_xA^T$  Is a diagonal matrix.

Eigen vectors  $e_i$  corresponding the eigen values is the variance of the i-th element in them. The element out of main diagonal is zero, it means every element of vector y is not interconnected. We can say the random vector y is processing of unconnected peculiar variable (Jin and Gaoding, 2012).

**Inverse karhunen-loeve transform:** The process of reconstructing of x from y is the important property of the Karhunen-Loeve Transform. Since the rows of A are orthonormal vectors, we can show that  $A^{-1} = A^T$ . To obtain the original vectors x from its corresponding y by using the expression (Gonzalez and Woods, 1992):

$$x = A^T y + m_x$$

Anywise, we use form matrix  $A_k$  where the k eigenvectors corresponding to the k largest eigenvalues that instead of using all the eigenvectors of  $C_x$ , find a transformation matrix of order  $k \times n$ . The vectors y would be k dimensional, the process of reconstructing of the original vector  $\hat{x}$  is:

$$\hat{x} = A_k^T y + m_x$$

It can prove the mean square error between x and  $\hat{x}$  and can give by the equation (Gonzalez and Woods, 1992):

$$e_{ms} = \|x - \hat{x}\|^2 = \sum_{j=1}^n \lambda_j - \sum_{j=1}^k \lambda_j = \sum_{j=k+1}^n \lambda_j$$

The last equation indicates the error is zero if  $k = n$ . The  $\lambda_j$ 's the error is minimum because the choosing the k eigenvectors corresponding to largest eigenvalues. Therefore the Karhunen-Loeve Transform is optimum performance because the mean square error between the vectors x is minimum and its approximations  $\hat{x}$  (Gonzalez and Woods, 1992).



Fig. 1: Sample data base for images

### PROPOSED METHOD

In this section, the proposed technique for data images encryption based karhunen-Leoeve Transforms involves two stages (The encoding and decoding) data images Model encryption.

We have used image databases. Figure 1 shows sample database for images which are used in this study (contain 50 images) applied.

The encoding, decoding algorithms and the schemes are given in the following sections.

#### Algorithm for encoding:

**Step 1:** Formalization of vectors from the given matrix(x).

**Step 2:** Calculate meanpoint and make as a vector  $m_x$ .

**Step 3:** Calculate (cm) covariance matrix called is ( $C_x$ ).

**Step 4:** Find the eigenvalues.

**Step 5:** Find the eigenvectors.

**Step 6:** Determine the transformation matrix A.

**Step 7:** Compute the KL transform matrix from

$$y = A(x - m_x).$$

#### Algorithm for decoding:

**Step 1:** Determine the transpose of matrix A.

**Step 2:** The vector reconstruct by  $x = A^T y + m_x$ .

**Step 3:** Reconstruction of vectors to give the matrix (x).

### EXPERIMENTAL RESULTS AND PERFORMANCE MEASURES

This section will discuss in some parameters below to evaluate and compare the image and efficiency of data encryption, as follows:

**Time and space:** Speed (time) it is useful that the encoding and decoding algorithms are fast sufficient to meet real-time requirements.

**Entropy:** Entropy is a mensuration of suspicionIn collaboration with a random variable. In connection with an image, the encryption lowering the reciprocal information between pixel values and thus boost the entropy value. Entropy coding which is based on symbol probabilities, when the symbol probabilities are equal will obtain the information source is a maximum:

$$Entropy = \sum P(i) \log_2 \frac{1}{P(i)} \quad (5)$$

where, P (i) is the eventuality of the appearance of a pixel with gray scale value i (Rakesh *et al.*, 2012).

**Mean Square Error (MSE) and Peak Signal-to-Noise Ratio (PSNR):** The PSNR is the proportion of the mean square difference of the pixels for the two images to the maximum mean square difference that canexist between any two images. We can express as a decibel value. The image quality is better when the greater PSNR value (>30 dB).Since encoded image, a smaller value of PSNR is prospective (Pareek, 2012):

$$MSE = \frac{\sum_{m=1}^M \sum_{n=1}^N [P(m,n) - P^*(m,n)]^2}{M \times N} \quad (6)$$

$$PSNR = 20 * \log_{10}(255 / \text{sqrt}(MSE)) \quad (7)$$

**Root Mean Square Error (RMSE):** Root Mean Square Error of the image when the meansum in each pixel of the encoded image is the maximum value of the pixel. Some changes Occurred in the value of the pixel because of encoding method (Dhaka *et al.*, 2013):

$$RMSE = \text{sqrt}(MSE) \quad (8)$$

Table 1 display time Performance Measure for images and the inverse images encryption.

Table 2 display Performance Measures (Entropy, MSE,PSNR, RMSE) for images and inverse images encryption.

Note that Time elapsed data image transform (second) Greater than Time elapsed inverse data image transform (second) according to Table 3.

### CONCLUSION

In the practical emulation results, we can obviously see that the encoding and decoding algorithms are fast enough to find real-time requirements, also we can note that time elapsed data image transform (second) Greater Than Time elapsed inverse data image transform (second).

From the parameters it was found that encoding with Evaluation Performance and type images it used offers best results. In this study, after study Mean

Table 1: Performance measure for time (speed)








Input image (x)	Time elapsed transform (second)	Time elapsed inverse transform (second)
	0.231581	0.326225
	0.230197	0.325062
	0.228921	0.322397
	0.230033	0.322983
	0.229538	0.322553
	0.231042	0.327775
	0.232780	0.326282

Table 2: Entropy, MSE, PSNR and RMSE performance measures for images and the inverse images encryption








Input image (x)	Entropy	MSE	PSNR	RMSE
	3.2816	7.3169e-032	359.5215	1.3696e-015
	7.4715	2.0410e-031	355.0663	2.8426e-016
	6.9753	7.9708e-032	359.1498	4.8545e-016
	7.8905	1.4310e-031	356.6084	2.3614e-015
	3.4902	1.2370e-031	357.2410	1.5622e-016
	7.0097	1.6911e-031	355.8831	1.9751e-016
	6.6962	4.9279e-032	361.2382	4.5154e-016

Table 3: Display original images and the inverse images encryption with time speed















Input image (x)	Cipher image (y)	Time elapsed transform (second)	Time elapsed inverse transform (second)
		0.349608	0.333416
		0.352882	0.324601
		0.327552	0.313987

Table 3: Continue

Input image (x)	Cipher image (y)	Time elapsed transform (second)	Time elapsed inverse transform (second)
		0.293114	0.326474
		0.322221	0.284974
		0.363091	0.349068
		0.357547	0.322833

Square Error (MSE) and Root Mean Square Error (RMSE) of the image we can see that the (MSE) is very small (is approximate zero) and (RMSE) is small enough (is approximate  $e-015$ ). So that, we can say the KLT is the best transform to encryption. Since it is the lowest correlation and the highest entropy, therefore the proposed algorithm resulted is the best performance.

#### REFERENCES

- Dhaka, V., R.C. Poonia and Y.V. Singh, 2013. A novel algorithm for image steganography based on effective channel selection technique. *Int. J. Adv. Res. Comput. Sci. Softw. Eng.*, 3(8): 428-433.
- Divya, V.V., S.K. Sudha and V.R. Resmy, 2012. Simple and secure image encryption. *Int. J. Comput. Sci. Issue.*, 9(6(3): 286-289.
- Gonzalez, R.C. and R.E. Woods, 1992. *Digital Image Processing*. 2nd Edn., Prentice Hall, Upper Saddle River, NJ.
- Jin, S. and N. Gaoding, 2012. Signal processing using the wavelet transform and the Karhunen-Loeve transform. M.Sc. Thesis, Department Computer Science, School of Health and Society, Kristianstad University, Sweden.
- Kaur, R. and E.K. Singh, 2013. Image encryption techniques: A selected review. *IOSR J. Comput. Eng.*, 9(6): 80-83.
- Pareek, N.K., 2012. Design and analysis of a novel Digital image encryption scheme. *Int. J. Netw. Secur. Appl.*, 4(2): 95-108.
- Rakesh, S., A.A. Kaller, B.C. Shadakshari and B. Annappa, 2012. Multilevel Image Encryption. Retrieved from: <https://arxiv.org/ftp/arxiv/papers/1202/1202.4871.pdf>.
- Salleh, M., S. Ibrahim and I.F. Isnin, 2003. Image encryption algorithm based on chaotic mapping. *J. Teknol.*, 39(D): 1-12.