

# Fractional Bio-Image Encryption using Karhunen-Loeve Transform

T.Sivakumar

Assistant Professor (Senior Grade)  
Department of Information Technology  
PSG College of Technology, Coimbatore-641 004,  
India.

R.Venkatesan, Ph.D

Professor  
Department of Computer Science and Engineering  
PSG College of Technology, Coimbatore -641004,  
India.

## ABSTRACT

Bio-images such as fingerprint, face and iris are sensitive and hence small change in such images could affect the result substantially. The processing overhead could be reduced by encrypting a preferred region instead of encrypting the entire image. In this paper a novel fractional bio-image encryption method is presented using Karhunen-Loeve (KL) transform, which is a reversible linear transform. The original image ( $x$ ) is given as input to cropping function to identify and extract the region to be encrypted. Next, the extracted region, in the form of square, is given as input to the KL transform which in turn produces the cipher image ( $y$ ) and the inverse transform key ( $T$ ). The encrypted region is combined with the original image to get the partial cipher image. Since the inverse transform key ( $T$ ) plays a major role for decryption, it could be given to the receiver by encrypting with symmetric key cryptosystem. On receiving the partial encrypted image ( $y$ ) the receiver identify and extract the encrypted region and apply the inverse of KL transform using the inverse key ( $T$ ). The result is merged with the received image to get the original image ( $x$ ). The histograms of the encrypted portion of the images are nearly uniform and different from the histogram of original images. This method of fractional bio-image cryptosystem will reduce the overhead of encryption and decryption processes.

**Keywords:** Bio-image encryption, Partial image encryption, KL transform, Histogram, Correlation.

## 1. INTRODUCTION

Biometric images such as fingerprint, face and iris are sensitive; it's enough to encrypt a preferred region of the image. Traditional cryptosystems such as DES, AES, and IDEA have been well suited to protect textual data. Use of traditional cryptosystem to encrypt images directly is not good for two reasons: (a) the image size is much larger than of text, it need more time to directly encrypt the images, and (b) the decrypted text must be equal to the original text, but this is not required for images (i.e., small distortion is acceptable due to human perception) [2]. KL transform is the best among all linear transforms with respect to energy compaction. The primary properties of KL Transform are (a) reversible linear transform, (b) exploits the statistical properties, (c) discard redundancy, (d) minimizes the total mean square error, and (e) Gaussian distribution. This paper proposed a new partial image encryption scheme using KL transform.

## 2. RELATED WORK

Hongjun Liu et al [1] have proposed a novel confusion and diffusion method for image encryption. This scheme confuse the pixels by transforming the nucleotide into its base pair for random times, the other is to generate the new keys according

to the plain image and the common keys, which can make the initial conditions of the chaotic maps change automatically in every encryption process. For any size of the original grayscale image, after being permuted the rows and columns respectively by the arrays generated by piecewise linear chaotic map (PWLCM), each pixel of the original image is encoded into four nucleotides by the deoxyribonucleic acid (DNA) coding. Experiment results and security analysis show that the scheme can not only achieve good encryption result, but also the key space is large enough to resist against common attacks.

Ismet Ozturk et al, [2] analyzed seven existing image encryption algorithms and added compression for two algorithms such as Mirror-like Image Encryption (MIE) and Visual Cryptography (VC). In the new enhanced scheme, encrypted images are compressed by either loss or lossless compression algorithms before transmission to the destination. The modified MIE algorithm reduces the disk storage space and network bandwidth. In the paper [3] a new encryption method is developed and a comparison is done by transforming images using DCT, DWT and DCT with DWT. The new scheme uses DNA base pairs for key generation and the encrypted image is highly uncorrelated with the original image.

Kanso, et al [4] suggested an image encryption algorithm based on a three dimensional (3D) chaotic map that can defeat several existing attacks. Use three rules to determine the shuffling, mixing and scrambling process of the pixel values of the plain-image. The image pixels are shuffled according to a search rule based on the 3D chaotic map. Then 3D chaotic maps are used to scramble shuffled pixels through mixing and masking rules, respectively. Simulation results show that the suggested algorithm satisfies the required performance tests such as high level security, large key space and acceptable encryption speed.

Liu Hongjun, et al [5] designed a stream-cipher algorithm based on one-time keys and robust chaotic maps. Utilized the piecewise linear chaotic map as the generator of a pseudo-random key stream sequence. This algorithm combines good confusion and diffusion properties by repeating encryption  $\alpha$  times. The authors concluded that the cryptosystem has higher security due to an extremely large key space. In paper [6], the authors introduced a block-based transformation algorithm based on the combination of image transformation and the Blowfish encryption algorithm. The algorithm resulted in the best performance; the lowest correlation and the highest entropy.

Nooshin Bigdeli et al, [7] presented an image encryption algorithm based on chaotic neural network (CNN). The employed CNN is comprised of two 3-neuron layers called

chaotic neuron layer (CNL) and permutation neuron layer (PNL). The values of RGB (Red, Green and Blue) color components of image constitute inputs of the CNN and three encoded streams are the network outputs. The main features of the algorithm are, (a) large key space including a 160-bits authentication code which could be extended up to 224 bits, and (b) this scheme leads to the highest security level in terms of the key space, key sensitivity, correlation coefficients, entropy and computational complexity of the cipher-images.

S.V. Sathyanarayana et al, [8] used the cyclic elliptic curves of the form  $y^2 + xy = x^3 + ax^2 + b$ ;  $a, b \in GF(2^m)$  with order  $m$  to design of a symmetric key image encryption scheme with key sequence derived from random sequence of cyclic elliptic curve points. The encrypted image does not have residual information and the corresponding histograms are almost flat offering good security for images. Also this cryptosystem is secure against the statistical, brute force and cryptanalytic attacks.

Seyed Mohammad, et al [9] presented a chaos-based image encryption algorithm to encrypt color images by using a Coupled Two-dimensional Piecewise Nonlinear Chaotic Map (CTPNM) and a masking process. In order to generate the initial conditions and parameters of the CTPNM, 256-bit long external secret key is used. The algorithm combines the key stream generation process, the diffusion-substitution process and the masking process into a single coherent encryption platform to strengthen the security and sensitivity of cryptosystem. Distinct characteristics of the algorithm are high security, high sensitivity, and high speed. Results show that the number of pixel change rate (NPCR), the unified average changing intensity (UACI), and entropy can satisfy security and performance requirements. Tzung-Her Chen et al, [10] designed a novel RG-based (Random Grids) VSS (Visual Secret Sharing) scheme with the capability of encrypting multiple secret images at once into only two circular cipher-grids. To decrypt all secrets, decoders stack the two circular cipher-grids to disclose the first secret and then gradually rotate one circular cipher-grid at a fixed degree to reveal the second. Compared with conventional VC-based (Visual Cryptography) VSS, this scheme has no pixel expansion, a higher capacity for secret sharing, and no need for a complex VC codebook to be redesigned.

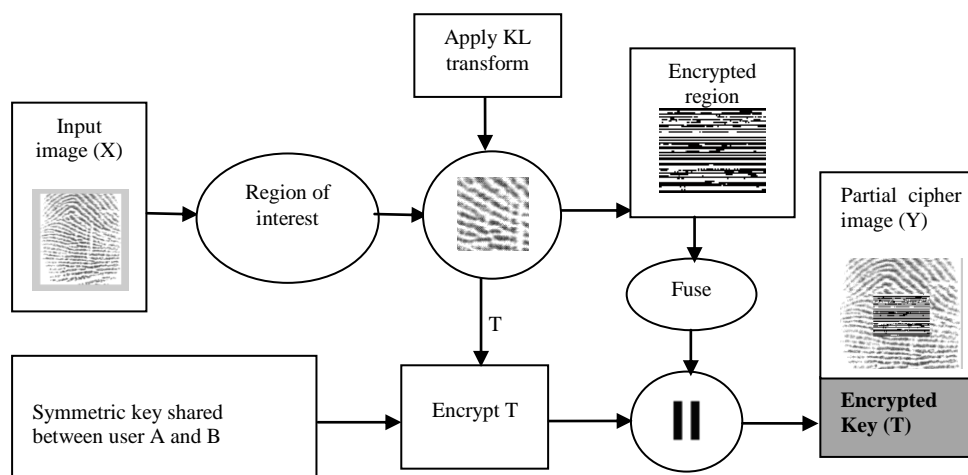
Sapna Sasidharan, et al [11] suggested a partial image encryption scheme using Discrete Wavelet Transform (DWT) and RC4 Stream Cipher. The approximation matrix (lowest frequency band) is encrypted using the stream cipher as it holds most of the image's information. The encryption time is reduced by encrypting only the part of the image and maintains a high level of security by shuffling the rest of the image using the shuffling algorithm. The algorithm is considered as a fast image encryption algorithm, due to the selective encryption of certain portion of the image (lowest frequency band).

Subba Rao, et al [12] presented an effective approach for partial image encryption with pseudo random sequences (PRS). They have encrypted the correlated data instead of encrypting the entire image in order to speed up the entire operation. The most significant bit (MSB) planes have high adjacent correlation between the pixels whereas the least significant bit (LSB) plane contains comparatively more uncorrelated data. These can serve as a good alternative for partially encrypting the MSB planes with low complexity to provide security against casual listeners. Results show that the new approach is able to reduce the residual intelligence as would have been obtained by encrypting the entire image.

### 3. THE PROPOSED SYSTEM

The original image ( $x$ ) is given as input to the "Region of Interest" function to identify and extract the region, in the form of square, to be encrypted. Next, the extracted region is given as input to the KL transform which in turn produces the cipher image ( $y$ ) and the inverse transform key ( $T$ ). The encrypted region is input to "Fuse" function which replaces the region of interest by the encrypted region. Also the inverse transform key ( $T$ ) is further encrypted by the key shared between the source and destination.

At the destination, first the receiver identifies and extracts the encrypted region and applies the inverse of KL transform with the inverse key ( $T$ ) to get the decrypted region of the image. The decrypted region is merged with the received image to produce the original image ( $x$ ) using the function "Fuse". The overall working model of the fractional bio-image encryption scheme is shown in Figure 1 and 2.



**Fig 1: Encryption at Source (A)**

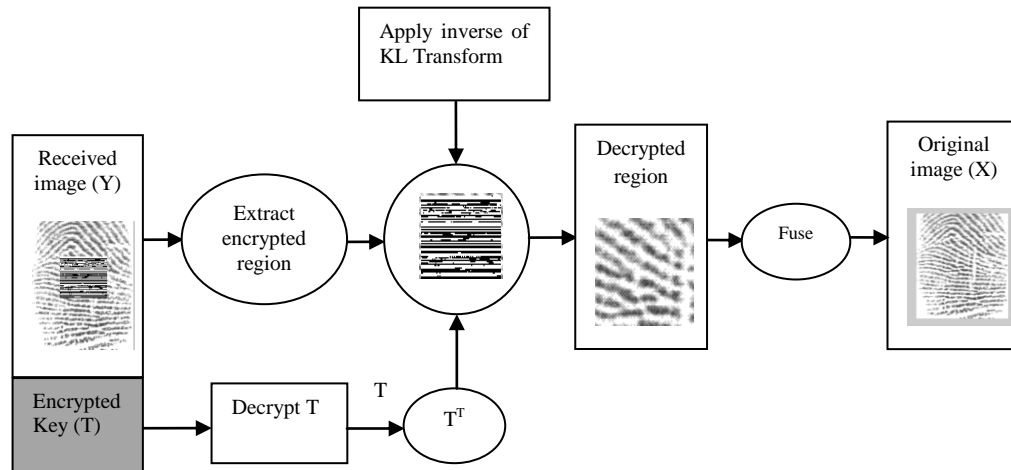


Fig 2: Decryption at Destination (B)

### 3.1 THE ALGORITHM

The source (A) and destination (B) have to generate a pair of key (private and public) and exchange the public key or generate and share a symmetric session key. The following steps to be followed when user A (source) and user B (destination) wants to communicate with each other.

- Step 1: Input the plain image (x) and extract the region of interest to encrypt.
- Step 2: Apply KL Transform over the output of step 2 which yields cipher image (y) and the inverse transform key (T).
- Step 3: Encrypt the inverse transform key (T) using symmetric key (K). ie,  $E[K, T]$ .
- Step 4: Fuse the encrypted region with the plain image.
- Step 5: Concatenate the result of step 3 and step 4 and send the result to destination.
- Step 6: Decrypt the inverse transform key (T) using the symmetric key shared by user A and B. ie.  $D[K, E(K, T)]$
- Step 7: Take the transpose of inverse transform key ( $T^T$ ).
- Step 8: Identify and extract the encrypted region of the partial cipher image.
- Step 9: Apply the inverse KL transform. i.e., multiply the result of step 6 and step 7.
- Step 10: Fuse the decrypted region with the received partial cipher image to obtain the original image (x).

## 4. IMPLEMENTATION

This section provides the algorithm for KL Transform, which is used to convert the input image (x) into cipher image (y), and the implementation of the proposed scheme on bio-images such as fingerprints, iris and face images.

### 4.1 ALGORITHM FOR KL TRANSFORM

- Step 1: Formation of vectors from the given matrix (x).
- Step 2: Determination of covariance matrix.
- Step 3: Determination of Eigen values of the covariance matrix.
- Step 4: Determination of Eigen vectors of the covariance matrix.
- Step 5: Normalization of the Eigen vectors.
- Step 6: Compute the KL transform matrix from the Eigen vector of the covariance matrix (v).
- Step 7: KL transform of the input matrix.  
ie, cipher image,  $y = v(x)$
- Step 8: Reconstruction of input values from the transformed coefficients. ( $x = v' * y$ )

### 4.2 EXPERIMENTAL RESULTS

The implementation of the proposed scheme on fingerprint, iris and face images to produce the partial cipher image is done for square as region of interest. While processing the fingerprint image, first the core point of the fingerprint image is identified using detection of curvature technique and a square region of size 100x100 pixels is extracted around the core point. For iris and face images a constant region of size 100x100 pixels is extracted starting from the (x, y) coordinate given by the user. The implementation of the proposed scheme on fingerprint, iris and face images are shown in Table 1. Results show that there is no exact relationship between the original and encrypted images.

Table 1. Results of Proposed Scheme

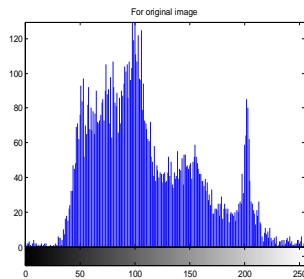
Input Image (x)	Extracted Region	Encrypted Region	Partial Cipher Image (y)

## 5. ANALYSIS OF PROPOSED MODEL

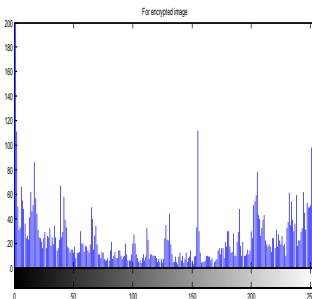
The proposed system provides a partial bio-image cryptosystem for images such as fingerprint, iris and face using single and onetime key. The inverse transform key (T) is used only once for the image from which the key is generated. To transmit  $n \times n$  cipher image it is necessary to transmit another  $n \times n$  inverse key (T) for decryption. This method of designing cryptosystem is more suitable for small images. For big images it occupies more bandwidth in the communication link, but when compared to steganography, the proposed scheme needs less bandwidth.

An additional processing overhead is incurred to encrypt and decrypt the inverse key (T) for secure distribution. The amount of processing overhead incurred by this process depends upon the chosen cryptosystem to distribute the inverse key. Always an attacker's aim is to identify the key used between the two communicating parties rather than the plaintext message. Once the key is compromised all past and future communication between the communicating parties can be decrypted. Since, in the proposed method the key is depends on the input image and it is used only one time it is less prone to cryptanalysis or brute-force attack. Since the decryption process involves transpose of a matrix and multiplying two matrices the amount of time taken is very less.

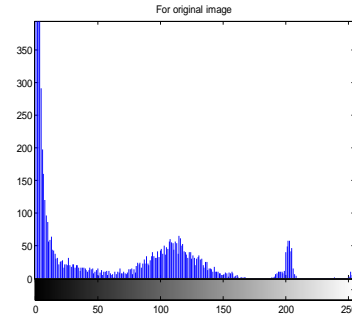
The strength of an encrypted image is proved by analyzing the histogram and correlation value of the original and encrypted images. For a high scrambled image the histogram is should flat as much as possible. Figure 3, 4, and 5 represents the histograms of the original and the encrypted images given in Table 1. The histograms of the encrypted images are fairly uniform and are significantly different from that of the original images.



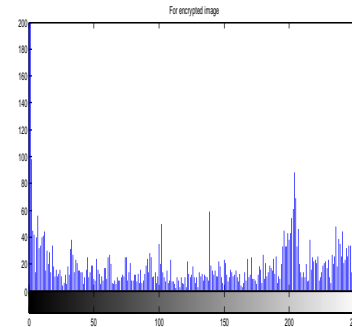
**Fig 3: (a) Histogram of fingerprint image before encryption**



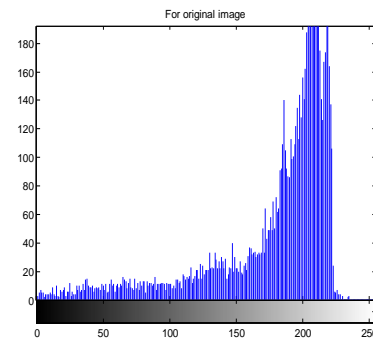
**Fig 3: (b) Histogram of fingerprint image after encryption**



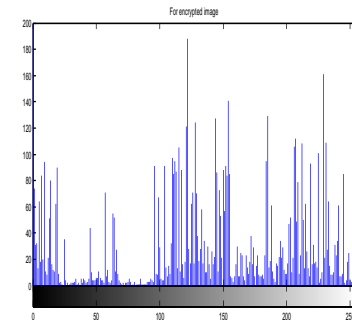
**Fig 4: (a) Histogram of iris image before encryption**



**Fig 4: (b) Histogram of iris image after encryption**



**Fig 5: (a) Histogram of facial image before encryption**



**Fig 5: (b) Histogram of facial image after encryption**

Correlation is a statistical technique that can show whether and how strongly pairs of variables are related. The correlation coefficient of each pair is calculated by using the following formula:

$$r_{x,y} = \frac{\text{cov}(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \quad (1)$$

where,

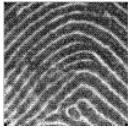

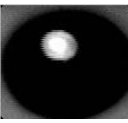



$$\text{cov}(x, y) = \frac{1}{N} \sum_{i=1}^N (x_i - E(x))(y_i - E(y)) \quad (2)$$

$$E(x) = \frac{1}{N} \sum_{i=1}^N x_i \quad (3)$$

$$D(x) = \frac{1}{N} \sum_{i=1}^N (x_i - E(x))^2 \quad (4)$$

Where n is the number of data pairs, x is the plain image and y is the cipher image. The range of the correlation coefficient is -1 to +1. A positive relationship exists when both variables are increase or decrease at the same time. A negative relationship exist when one variable increases and the other variable decreases or vice versa. A weak relationship exists if the value of r is close to zero. Table 2 shows the correlation coefficient value between the original and encrypted images.

**Table 2. Correlation coefficient values**

Original Image	Encrypted Image	Correlation Value
		0.0225
		0.0668
		-0.0247

The correlation value shows that the statistical relationship between the original and encrypted image is close to zero and hence there is no exact relationship between the original and encrypted images.

## 6. CONCLUSION

Since Bio-Images such as fingerprint, iris and facial are more sensitive, in this paper, a novel partial bio-image encryption method is presented using Karhunen-Loeve (KL) transform, which is a reversible linear transform. The output of KL transform is treated as cipher image, and it uses only one key for decryption and does not use any key for encryption. The inverse transform key (T) is derived from the input image and it is used only once per image. For secure transmission of T, it is encrypted by symmetric cryptosystem. The histogram of the encrypted image is almost uniform and different from that of the original image. The correlation value shows that there is a weak relationship between the original and encrypted region of the input images.

## 7. REFERENCES

- [1] Hongjun Liu, Xingyuan Wang, and Abdurahman kadir, "Image encryption using DNA complementary rule and chaotic maps", Elsevier, 2012.
- [2] Ismet Ozturk and Ibrahim Sogukpinar, "Analysis and Comparison of Image Encryption Algorithms", World Academy of Science, Engineering and Technology, 2005.
- [3] Sumathy K, and R.Tamilselvi, "Comparison of Encryption Levels for Image Security Using Various Transforms", International Conference on Information and Network Technology, IACSIT Press, Singapore, 2011.
- [4] Kanso, M. Ghebleh, "A Novel Image Encryption Algorithm based on 3D Chaotic Map", Elsevier, December 2011.
- [5] Liu Hongjun and Wang Xingyuan, "Color Image Encryption based on One-time Keys and Robust Chaotic Maps", Computers and Mathematics with Applications – Elsevier, 2010.
- [6] Mohammad Ali Bani Younes and Aman Jantan, "Image Encryption using Block-Based Transformation Algorithm", International Journal of Computer Science, 2008.
- [7] Nooshin Bigdeli, Yousef Farid, Karim Afshar, "A Novel Image Encryption/Decryption Scheme based on Chaotic Neural Networks", Elsevier, 2012.
- [8] Sathyanarayana S.V, M. Aswatha Kumar and K.N. Hari Bhat, "Symmetric Key Image Encryption Scheme with Key Sequences Derived from Random Sequence of Cyclic Elliptic Curve Points", International Journal of Network Security, 2011.
- [9] Seyed Mohammad Seyedzadeh, and Sattar Mirzakuchaki, "Fast Color Image Encryption Algorithm Based on Coupled 2D Piecewise Chaotic Map", Elsevier, 2011.
- [10] Tzung-Her Chen, Kuang-Che Li, "Multi-image Encryption by Circular Random Grids", Elsevier, 2011.
- [11] Sapna Sasidharan and Deepu Sreeba Philip, "A Fast Partial Image Encryption Scheme with Wavelet Transform and RC4", International Journal of Advances in Engineering & Technology, 2011.
- [12] Subba Rao Y.V, Abhijit Mitra and S. R. Mahadeva Prasanna, "A Partial Image Encryption Method with Pseudo Random Sequences", Springer, 2006.