

# A Novel Framework for Image Encryption using Karhunen-Loeve Transform

T. Sivakumar

Assistant Professor (Senior Grade)  
Department of Information Technology  
PSG College of Technology, Tamilnadu-641004, India.

R. Venkatesan, Ph.D

Professor & Head  
Department of Computer Science and Engineering  
PSG College of Technology, Tamilnadu-641004, India.

## ABSTRACT

The Karhunen-Loeve (KL) transform is widely used technique for image compression or clustering analysis. Since KL transform is a reversible linear transform, a novel cryptosystem is developed to provide confidentiality service for images. The original image ( $x$ ), in the form of square matrix, is given as input to the KL transform which in turn produces the encrypted image ( $y$ ) and the decryption key ( $k$ ). Since the key matrix ( $k$ ) plays a major role for decryption, it is encrypted by the receiver's public key by using RSA algorithm. The encrypted image ( $y$ ) and key matrix ( $k$ ) are transmitted over the public network. On receiving the encrypted image ( $y$ ) and key matrix ( $k$ ), the receiver takes the transpose of the decrypted key matrix ( $k$ ) and multiplies the result with the encrypted image ( $y$ ) to get the original image ( $x$ ). The time complexity of the proposed scheme is calculated separately for both encryption,  $O(n^2)$ , and decryption,  $O(n^3)$ . The histograms of the encrypted images are almost uniform and different from that of the original images. This method of image cryptosystem is more suitable for small images.

**Keywords:** Image Encryption, KL Transform, Image Histogram, and Correlation Coefficient

## 1. INTRODUCTION

In this fast growing technical world, where the Internet provides essential communication between tens of millions of people and is being increasingly used as a tool for transmission of digital images, security becomes a tremendously important issue. Most traditional cryptosystems have been designed to protect textual data. Traditional encryption algorithms such as data encryption standard (DES) and RSA, has the weakness of low-level efficiency when the image is large. Use of traditional cryptosystem to encrypt images directly is not good for two reasons [5]: (a) since the image size is much larger than that of text, it needs 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).

The basic function of the KL transform depends on the statistics of input data and the coefficients in the Karhunen-Loève theorem are random variables. It is the best among all linear transforms with respect to energy compaction which means most of the 'energy' of the transform coefficients is concentrated within the first few components. The foremost properties of KL Transform are (a) reversible linear transform, (b) exploits the statistical properties, (c) discards redundancy, (d) minimizes the total mean square error, and (e) Gaussian distribution. The following are some major requirements to design any cryptosystem:

1. An encryption scheme is unconditionally secure if the ciphertext generated by the scheme does not contain enough information to determine uniquely the corresponding plaintext.
2. Reversible transformation: A block cipher operates on a plaintext block of  $n$  bits to produce a ciphertext block of  $n$  bits. There are  $2^n$  possible different plaintext blocks and, for the encryption to be reversible (ie. for decryption to be possible), each must produce a unique ciphertext block.
3. Diffusion: The statistical structure of the plaintext is dissipated into long-range statistics of the ciphertext. This is achieved by having each plaintext digit affect the value of many ciphertext digits.
4. Size of input plaintext message must be equal to the size of output ciphertext message produced by the scheme.

Since KL transform satisfies some of the above said properties of cryptosystem, this paper focus on to design and develop a cryptosystem to provide confidentiality service for images.

## 2. RELATED WORK

In Hill cipher algorithm, the inverse of the key matrix used for encrypting the plaintext does not always exist. If the key matrix is not invertible, then encrypted text cannot be decrypted. Bibhudendra et al [1], proposed a novel Advanced Hill (AdvHill) encryption technique, which uses an involutory matrix, to encrypt an image. In the Involutory matrix generation method the key matrix used for the encryption is itself invertible. Thus the computational complexity is reduced by avoiding the process of finding inverse of the matrix at the time of decryption.

In [3], the authors have made use of five discrete orthogonal transforms in speech encryption systems. The transforms considered are the Discrete Fourier Transform, Discrete Cosine Transform, Walsh Hadamard Transform, Karhunen-Loeve Transform and the Discrete Prolate Spheroidal Transform. First the speech samples converted to a transform domain and the encryption is done in the transform domain. The encrypted transform samples are converted back to the time domain and transmitted. The authors concluded that, the DCT, DFT and DPST can be used in narrow band systems such as speech transmission over public switched telephone network and the KLT and WHT are more suitable where wider bandwidth is available. The transformation is done twice during encryption and twice during decryption.

G.A.Sathishkumar et al [4] provided a secure image encryption technique using multiple chaotic based circular mapping. Here, first, a pair of sub keys is given by using chaotic logistic maps. Second, the image is encrypted using

logistic map sub key and its transformation leads to diffusion process. This chaos based image cipher will be suitable for applications like wireless communications. Han Shuihua, et al, [5] designed a asymmetric image encryption scheme based on certain matrix transformation. To implement this algorithm, first, a pair of keys is created based on matrix transformation; second, the image is encrypted by using private key in its transformation domain; finally the receiver uses the public key to decrypt the encrypted messages. Because of the proposed scheme is based on matrix transformation, it is easily implemented and highly efficient to quickly encrypt and decrypt image messages.

HaojiangGao et al [6] presented a Nonlinear Chaotic Algorithm (NCA) which uses power function and tangent function instead of linear function. The proposed encryption algorithm is a one-time-one-password system. Compared with some general encryption algorithms such as DES, the encryption algorithm is more secure. The authors concluded that the chaotic encryption algorithm is sensitive to the key; a small change of the key will generate a completely different decryption result and can not get the correct plain-image.

HongjunLiu et al [7], 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 permuting the rows and columns using 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.

Huaqian Yang et al [8] crypt analyzed some chaos-based image encryption algorithms with substitution-diffusion structure and identified the common flaws or deficiencies of these algorithms. The summarization of the flaws is (a) the key for encryption/decryption is independent of the plain-image and this favors known plaintext and chosen plaintext attacks, (b) in the diffusion process, the change in the current pixel value only affects a few cipher image pixels in one round and so at least two overall rounds of substitution-diffusion are required and (c) it is difficult for the receiver to determine whether the decrypted image is exactly the one sent. So the authors proposed a fast image encryption and authentication scheme. A keyed hash function is introduced to generate a 128-bit hash value from both the plain-image and the secret hash keys. The hash value plays the role of the key for encryption and decryption while the secret hash keys are used to authenticate the decrypted image.

IsmetOzturk et al [9] 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 [10] 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.

Encrypted image is highly uncorrelated with the original image.

A. Kanso et al [11] suggested a novel image encryption algorithm based on a three dimensional (3D) chaotic map that can defeat several existing attacks. The method uses 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 and Wang Xingyuan [12] have designed a stream-cipher algorithm based on one-time keys and robust chaotic maps. The algorithm employed piecewise linear chaotic map as the generator of a pseudo-random key stream sequence. The proposed algorithm combines good confusion and diffusion properties by repeating encryption  $\alpha$  times. The authors concluded that the proposed cryptosystem has higher security due to an extremely large key space. In [13], the authors introduced a block-based transformation algorithm based on the combination of image transformation and the Blowfish encryption algorithm. The proposed algorithm resulted in the best performance; the lowest correlation and the highest entropy.

NooshinBigdeli et al [14] presented a novel image encryption/decryption algorithm based on chaotic neural network (CNN). The employed CNN 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 proposed algorithm are, (a) large key space including a 160-bits authentication code which could be extended up to 224 bits, and (b) proposed 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.S. Maniccam et al [15] presented a new image and video encryption method based on the SCAN methodology, which is a formal language-based two-dimensional spatial accessing methodology. The basic idea of the proposed image encryption method is to rearrange the pixels of the image and change the pixel values. The pixel rearrangement is done by scan keys. The pixel values are changed by a simple substitution mechanism which adds confusion and diffusion properties to the encryption method. The main characteristics of the proposed encryption methods are (a) lossless encryption of image, (b) number of encryption keys is larger than that of most existing image or video encryption methods, (c) encryption keys have variable lengths, (d) capability to encrypt large blocks of any one-dimensional digital data, and (e) encryption uses only integer arithmetic and it can be easily implemented in hardware. The complexity of the SCAN methodology is of the order of  $O(n^2 + \log_2 n)$ , for images of  $n \times n$  pixels.

S.V. Sathyanarayana et al [16] 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 Seyedzadehet al [17] proposed a chaos-based image encryption algorithm to encrypt color images by using a Coupled Two-dimensional Piecewise Nonlinear Chaotic Map, called CTPNCM, and a masking process. In order to generate the initial conditions and parameters of the CTPNCM, 256-bit long external secret key is used. Proposed system combine 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 (NPCR: 40.99672, UACI: 40.334904, Entropy: 47.99921).

Tzung-Her Chen [18] proposed 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, the proposed scheme has no pixel expansion, a higher capacity for secret sharing, and no need for a complex VC codebook to be redesigned.

### 3. PROPOSED SYSTEM

In the proposed scheme, first the input image  $x$  in the form of matrix is converted into a square matrix by padding row or column. Padding process is done by repeating the last row or column of the input matrix to the necessary number of times. Second the input image ( $x$ ) is given as input to KL Transform which returns the encrypted image ( $y$ ) along with the decryption key ( $k$ ). This decryption key ( $k$ ) is further encrypted using the public key of the receiver and sent along with the encrypted image. At the destination, the receiver first decrypts the key matrix ( $k$ ) using its private key. Next, transpose of the key matrix ( $k$ ) is taken and the result is multiplied with the received encrypted image ( $y$ ) to produce the original image ( $x$ ). The overall working model of the proposed scheme is shown in Figure 1 and 2.

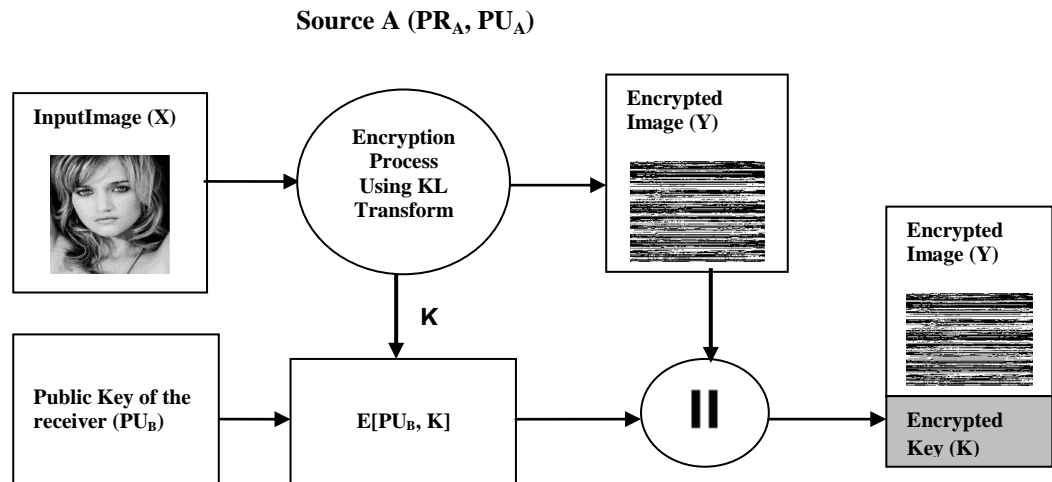


Fig 1 Encryption at Source

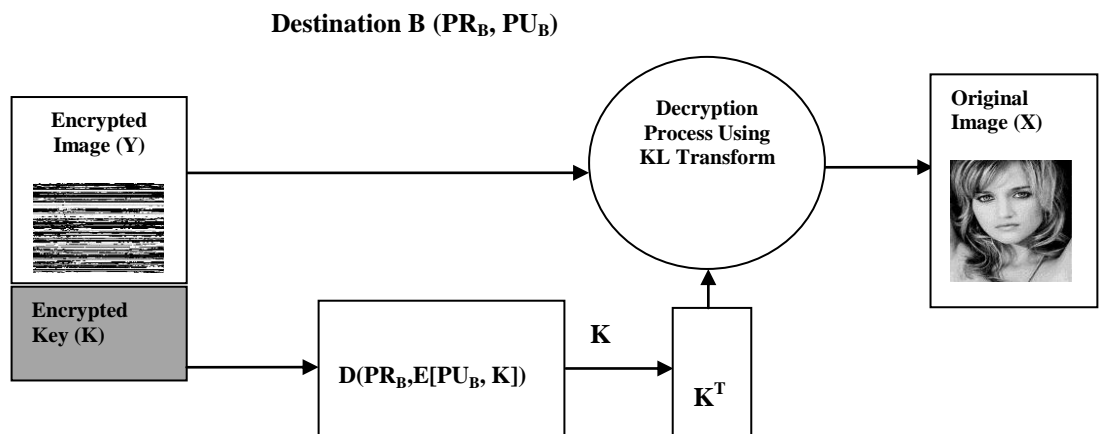


Fig 2 Decryption at Destination

### 3.1 ALGORITHM FOR PROPOSED SCHEME

The sender (A) and receiver (B) have to generate a pair key (private and public key) and exchange the public 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 plaintext matrix (x) and convert x as a square matrix.

Step 2: Apply KL Transform over the input message x which yields ciphertext (y) and key matrix (k).

Step 3: Encrypt the key (k) using receiver's public key ( $PU_B$ ), ie.  $E[PU_B, k]$  and concatenate the result with y and send to the user B.

Step 4: Decrypt the key (k) using the private key of user B. ie.  $D[PR_B, E[PU_B, T]]$

Step 5: Transpose of k is taken (ie.  $k^T$ ).

Step 6: The original message (x) is obtained by multiplying the ciphertext (y) and key matrix (k).

### 4. IMPLEMENTATION AND RESULTS

This section provides the algorithm for KL Transform [10], which is used to convert the input image (x) into cipher image (y), and the implementation of the proposed scheme on various 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.














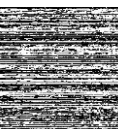



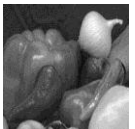












ie, cipher image,  $y = v(x)$

Step 8: Reconstruction of input values from the transformed coefficients. ( $x = v^T * y$ )

#### 4.2 EXPERIMENTAL RESULTS

The implementation of the proposed scheme on various images to produce the cipher image (y) is shown for ten sample images in Table 1. Results show that there is no exact relationship between the input and encrypted images. Also the decrypted image exactly matches with the original image.

Table 1 Results of Proposed Scheme

S.No	Input Image (X)	Encrypted Image (Y)	Decrypted Image (X)
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			

## 5. ANALYSIS OF PROPOSED MODEL

The proposed system provides an efficient cryptosystem without using key for encryption and uses key only for decryption. Since the key is derived from the input image, the key is used only once for the image from which the key is generated. To transmit  $n \times n$  cipher image it is necessary to send another  $n \times n$  key matrix for decryption. This method 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 uses fewer bandwidths.

An additional processing overhead is incurred to encrypt and decrypt the key matrix ( $k$ ) for secure distribution. The amount of processing overhead incurred by this process depends upon the chosen public-key cryptosystem to distribute the key ( $k$ ). 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 the key depends on the input image and it is used only one time it is less prone to cryptanalysis or brute-force attack. The time complexity is calculated for encryption phase and decryption phase separately. The running time of encryption phase comprises of formation of vector, which is  $O(n)$ , and finding the covariance matrix, which is  $O(n^2)$ , Eigen values and Eigen vectors, which is  $O(n^2)$ . The decryption phase involves the multiplication of the cipher image with the transpose of the key matrix to produce the original image, its needs running time of  $O(n^3)$ . The decryption process involves transpose of a matrix and multiplying two matrices, the amount of time taken for decryption is very less.

Shannon [2] suggested two methods such as histogram and correlation based on confusion and diffusion in order to counteract powerful attacks based on statistical analysis. By analyzing the histograms of the encrypted images the strength of an encrypted image is proved. Figure 3 and 4 represents the histograms of the original and the encrypted images given in Table 1 with s.no. 1 and 2 respectively. The histograms of the encrypted images are fairly uniform and are significantly different from that of the original images.

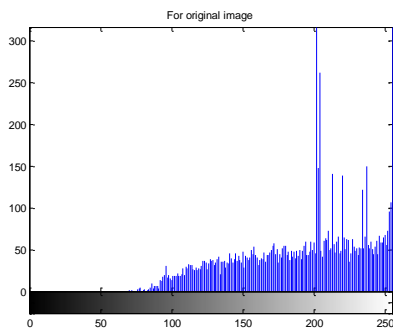


Figure 3 (a) Histogram of image before encryption

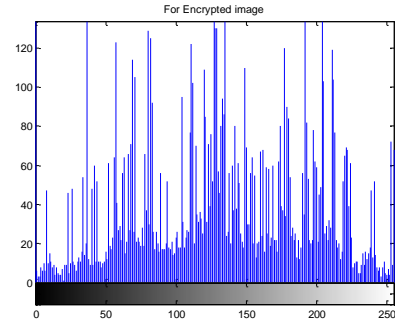


Figure 3 (b) Histogram of image after encryption

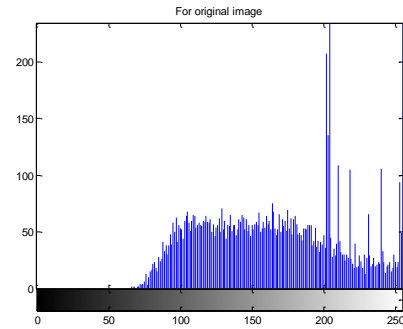


Figure 4 (a) Histogram of image before encryption

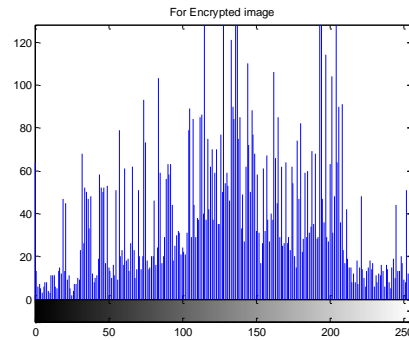


Figure 4 (b) Histogram of image after encryption

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:

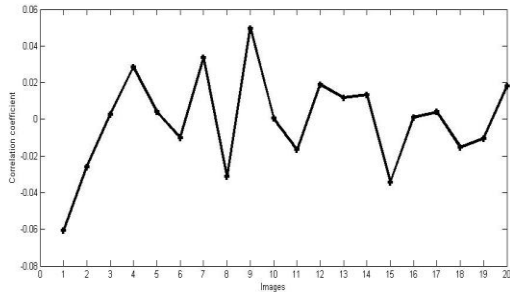
$$\gamma_{x,y} = \frac{\text{cov}(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \quad (1)$$

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

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

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

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. Figure 5 shows the correlation coefficient value between the original and encrypted images.



**Figure 5 Correlation coefficient values**

From the correlation chart it is inferred 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

The proposed scheme provides an efficient cryptosystem using KL Transform to provide confidentiality service for image data transmitted over public network. Since the output of KL transform is treated as cipher image, it uses only one key for decryption and does not use any key for encryption. The decryption key ( $k$ ) is derived from the input image and it is used only once per image. For secure use of key matrix ( $k$ ), it is encrypted with receiver's public key, so that the concerned receiver only can decrypt and know the value of key ( $k$ ). For a high scrambled image the histogram is flat as much as possible [2]. In the proposed method, the histogram of the encrypted image is almost flat and different from that of the original image and hence offers good security. The correlation values show that there is no relationship between the original and encrypted images. This method of image cryptosystem is suitable for tiny and highly confidential images.

## 7. REFERENCES

- [1] Bibhudendra, Soraj Kumar Panigrahy, Sarat Kumar Patra and Ganapati Panda, "Image Encryption using Advanced Hill Cipher Algorithm", *International Journal of Recent Trends in Engineering*, Vol.1, No.1, 2009.
- [2] Douglas R Stinson, *Cryptography: Theory and Practice*, Chapman and Hall, New York, 2002.
- [3] Dr.S.Sridharan, E.Dawson, and B.M Goldburg, "Speech Encryption Using Discrete Orthogonal Transforms", *IEEE*, 1990.
- [4] G.A.Sathishkumar, Dr.K.Bhoopathy, bagan and Dr.R.Sriraam, "Image Encryption Based on Diffusion and Multiple Chaotic Maps", *International Journal of Network Security & Its Applications*, Vol.3, No.2, 2011.
- [5] Han Shuihua and Yang Shuangyuan, "An Asymmetric Image Encryption Based on Matrix Transformation", *ECTI Transactions on Computer and Information Technology* Vol.1, No.2, November, 2005.
- [6] Haojiang Gao, Yisheng Zhang, Shuyun Liang and Dequn Li, "A New Chaotic Algorithm for Image Encryption", *Elsevier Science Direct*, 2005.
- [7] Hongjun Liu, Xingyuan Wang, and Abdurahmankadir, "Image encryption using DNA complementary rule and chaotic maps", *Elsevier*, January 2012.
- [8] Huaqian Yang, Kwok-Wo Wong, Xiaofeng Liao, Wei Zhang, Pengcheng Wei, "Fast image encryption and authentication scheme based on chaotic maps", *Elsevier*, 2010.
- [9] Ismet Ozturk and Ibrahim Sogukpinar, "Analysis and Comparison of Image Encryption Algorithms", *World Academy of Science, Engineering and Technology*, 2005.
- [10] K.Sumathy 1, R.Tamilselvi, "Comparison of Encryption Levels for Image Security Using Various Transforms", *International Conference on Information and Network Technology*, IACSIT Press, Singapore, 2011.
- [11] Kanso, M. Ghebleh, "A novel image encryption algorithm based on a 3D chaotic map", *Elsevier*, December 2011.
- [12] Liu Hongjun and Wang Xingyuan, "Color image encryption based on one-time keys and robust chaotic maps", *Computers and Mathematics with Applications – Elsevier*, 2010.
- [13] Mohammad Ali BaniYounes and AmanJantan, "Image Encryption using Block-Based Transformation Algorithm", *International Journal of Computer Science*, 35:1, *IJCS\_35\_1\_03*, 2008.
- [14] Nooshin Bigdeli, Yousef Farid n, Karim Afshar, "A novel image encryption/decryption scheme based on chaotic neural networks", *Elsevier*, 2012.
- [15] S.S. Maniccam, N.G. Bourbakis, "Image and video encryption using SCAN patterns," *Journal of Pattern Recognition Society*, vol. 37, no. 4, pp.725–737, 2004.
- [16] S.V. Sathyanarayana, M. Aswatha Kumar and K.N. HariBhat, "Symmetric Key Image Encryption Scheme with Key Sequences Derived from Random Sequence of Cyclic Elliptic Curve Points", *International Journal of Network Security*, Vol.12, No.3, PP.137 -150, May 2011.
- [17] Seyed Mohammad Seyedzadeh, and Sattar Mirzakhaki, "Fast Color Image Encryption Algorithm Based on Coupled 2D Piecewise Chaotic Map", *Elsevier*, 2011.
- [18] Tzung-Her Chen, Kuang-Che Li, "Multi-image encryption by circular random grids", *Elsevier*, November 2011.