Selective Combinational Encryption of Gray Scale Images using Orthogonal Polynomials based Transformation

R. Krishnamoorthi[†] and P. D. Sheba Kezia Malarchelvi[††]

[†] Professor, Department of Information Technology, Bharathidasan Institute of Technology, Anna University, Tiruchirapalli, Tamil Nadu, India, 620024.
[††] Research Scholar, Department of Information Technology, Bharathidasan Institute of Technology, Tiruchirapalli, Tamil Nadu, India, 620024.

Summary

In this paper, we propose a new image encryption technique in orthogonal polynomials based transformation domain (OPT) with selective combinational scrambling for secure transmission of images. Normally, the values of the neighboring pixels are highly correlated in most of the images. In order to de-correlate the intelligible information present in the image we propose the use of orthogonal polynomials based transformation. Also, the proposed technique exploits the energy preserving property of the orthogonal polynomials based transform coding which compacts energy in a few low frequency coefficients. These low frequency coefficients are selected as candidates for encryption which significantly reduces the number of bits to be encrypted. Then shuffling of these coefficients and their bits are performed. In addition, the sign bits of the selected low frequency coefficients are encrypted and randomly selected transformed blocks are shuffled. A symmetric key based cryptographically secure pseudo random process controls the entire encryption process. Experimental results reveal that the proposed OPT domain encryption scheme provides very low encryption PSNRs implying effective encryption. Also, security analyses prove that the proposed technique is robust to brute force, statistical and differential attacks.

Key words:

Image encryption –Orthogonal Polynomials – Selective combinational Scrambling.

1. Introduction

With the rapid development of the Internet and communication technologies, the transmission of image data takes place frequently. Consequently, the security of image data is gaining much importance. However, traditional text encryption schemes are unaffordable to encrypt images due to the bulky size of images. Also the decrypted image need not exactly be the same as the original image. Due to the characteristic of human perception, a decrypted image containing small distortion is acceptable as long as it does not affect the content of the image. To satisfy the emerging demand, a large number of image encryption schemes have been proposed in the past decade. Selective encryption is an encryption scheme that protects only the visually most important parts of an image or video to minimize computational efforts in real-time applications. The first attempts in this direction secured DCT-based multimedia [1, 2, 3].In [4] a partial encryption of the significant information related to pixels or sets in the two highest pyramid levels of a SPHIT (set portioning in hierarchical trees) bit stream is proposed. Marc *et al* have proposed the encryption of the sign and magnitude of the no-zero DCT coefficients, in [5]. In [6] a selective encryption technique for JBIG encoded visual data is proposed. This scheme encrypts only the lowest resolution of five layers for all bit planes. A scheme for selective encryption of wavelet-packet encoded image data is proposed in [7]. In this scheme header information of a wavelet packet image coding is protected using Advanced Encryption Standards to encrypt only the sub-band decomposition structure. In [8], Fridrich suggests a chaos-based image encryption scheme. This scheme is composed of two processes: chaotic confusion and pixel diffusion. The former permutes the pixels of a plain image with a 2D chaotic map while the latter alternates the value (gray-level) of each pixel in a sequential manner. This architecture forms the basis of a number of chaos-based image ciphers proposed subsequently. Chen and his research group employ a three-dimensional (3D) cat map [9] and a 3D baker map [10] in the confusion stage. Guan *et al.* propose the use of a 2D cat map for pixel position permutation and Chen's discretized chaotic system for pixel value masking [11]. In [12], Lian *et al.* pointed out that the key space of these two maps is not as large as that of the standard map. Therefore they suggest using a standard map for confusion while keeping the logistic map for pixel value diffusion. To achieve a satisfactory level of security, Lian *et al.* have proposed to perform four overall rounds of confusion and diffusion. In each confusion stage, 4 permutation rounds were performed. These led to a total of 16 permutation rounds and 4 diffusion rounds.

Hossam *et al.* have proposed a chaos-based feedback stream cipher which is based on the use of a logistic map and an external secret key of 256-bits in [13]. In this method, the initial conditions for the chaotic logistic map are derived using the external secret key by providing weights to its bits corresponding to their position in the

Manuscript received May 5, 2008
Manuscript revised May 20, 2008

key. A symmetric image encryption scheme based on a simple two-dimensional map is proposed in [14]. This scheme is based on image stretch-and-fold and a simple diffusion mechanism.

In [15], A. Sinha and K. Singh have proposed an encryption scheme using digital signature wherein the digital signature of the original image is added to the Bose-Chaudhuri Hochquenghem (BCH) encoded version of the original image to produce the encrypted image. A. Mitra *et al.* have proposed an approach for image encryption using a combination of different permutation techniques in [16]. The idea behind this work is that the perceivable information in the image can be reduced by decreasing the correlation among the bits, pixels and blocks using certain permutation techniques. An asymmetric image encryption based on matrix transformation is proposed in [17]. First a pair of keys is generated using matrix transformation and then the image is encrypted using the private key in the DCT domain. Finally the receiver uses the public key to decrypt the encrypted image. Chang *et al.* have proposed a gray-level image encryption scheme using full phase encryption and phase-encoded exclusive-OR operations in [18]. The gray-level image is sliced into binary images which have the same pixel level, and each of them is encrypted by phase-encoded XOR operations with a phase-encoded binary random image. In [19], M. Zeghid *et al.* have modified the AES for image encryption by adding a key stream generator to improve the encryption performance for images characterized by reduced entropy. A phase-only encryption and a single path decryption system using phase-encoded exclusive OR rules is presented in [20]. To generate phase-only encrypted data, a zero-padded original image, multiplied by a random phase image, is Fourier transformed and its real-valued data is encrypted with key data using phase-encoded XOR rules.

Yumnam *et al.* have proposed a new transform called Simplet in [21] and have used the property that the reconstructed signal in Simplet is perceptually unintelligible when the decomposed components have noise in them, for encryption. They have also used a sequence called Meitei Lock Sequence which is generated from a non-zero key vector of arbitrary length. Once a signal is encrypted with an MLS, it can be decrypted only with that particular MLS and since the MLS is generated from an arbitrary vector, the search space for finding a particular MLS is very large.

In this paper we introduce selective combinational scrambling in orthogonal polynomials based transform domain with the goal of accelerating frequency domain encryption speed. The orthogonal polynomials based transform is configured as an integer transform with lesser complexity. In addition selective scrambling of bits, coefficients and blocks are proposed in order to reduce the encryption time. This paper is organized as follows. In Sections 2 and 3 the Orthogonal Polynomials based transformation is presented. The encryption scheme based on the proposed transformation is described in Section 4. In Section 5, the measure of performance used for evaluating the proposed algorithm is described. In Section 6 the experimental results and security analysis are presented.

2. Orthogonal Polynomials based Transformation

The Discrete Cosine Transform and Discrete Wavelet Transform are the most widely used transforms for frequency domain encryption of images. However the computational complexity of the transforms that involve floating point operations is quite high. Motivated by the fact that integer transforms lower the computational complexity, we propose the use of orthogonal polynomials based transformation for image encryption in this section by analyzing the image formation system. Here, a linear 2-d image formation system is considered around a Cartesian coordinate separable, blurring, point spread operator in which the image *I* results in the superposition of the point source of impulse weighted by the value of the object *f*. Expressing the object function *f* in terms of derivatives of the image function I relative to its Cartesian coordinates is very useful for de-correlating the image. The point spread function M(x, y) can be considered to be real valued function defined for (x, y) $\in$ X x Y, where X and Y are ordered subsets of real values. In case of gray-level image of size (n*n) where X (rows) consists of a finite set, which for convenience can be labeled as {0, 1, …, n-1}, the function M(x, y) reduces to a sequence of functions.

$$M(\, i, t) = \; u_i(t), i = 0, 1, \ldots, n\text{-}1 \qquad \ldots (1)$$

The linear two dimensional transformation can be defined by the point spread operator $M(x, y)(M(i, t) = u_i(t))$ as shown in Eq. (2).

$$\beta'(\zeta,\eta) = \int_{x\in X}\int_{y\in Y} M(\zeta,x)\; M(\eta,y)\; I(x,y)\; dxdy \quad \ldots (2)$$

Considering both X and Y to be a finite set of values {0, 1, 2 … n –1}, Eq. (2) can be written in matrix notation as follows

$$\left|\beta'_{ij}\right| = \left(\left|M\right| \otimes \left|M\right|\right)^t \left|I\right| \qquad \ldots (3)$$

where $\otimes$ is the outer product, $|\beta'_{ij}|$ are n^2 matrices arranged in the dictionary sequence, $|I|$ is the image , $|\beta'_{ij}|$ are the coefficients of transformation and |M| is

$$|M| = \begin{vmatrix} u_0(t_1) & u_1(t_1) & \cdots & u_{n-1}(t_1) \\ u_0(t_2) & u_1(t_2) & \cdots & u_{n-1}(t_2) \\ & \vdots & & \\ u_0(t_n) & u_1(t_n) & \cdots & u_{n-1}(t_n) \end{vmatrix} \quad \ldots (4)$$

We consider the set of orthogonal polynomials $u_0(t)$, $u_1(t)$, …, $u_{n-1}(t)$ of degrees 0, 1, 2, …, n-1, respectively to construct the polynomial operators of different sizes from Eq. (4) for $n \geq 2$ and $t_i = i$.

3. The orthogonal polynomial basis

In order to construct the orthogonal polynomial basis, we first propose a set of orthogonal polynomials in Eq. (4)

$$u_{i+1}(t) = (t - \mu)u_i(t) - b_i(n)u_{i-1}(t) \text{ for } i \geq 1, \quad \ldots(5)$$

$$u_1(t) = t - \mu, \text{ and } u_0(t) = 1,$$

where

$$b_i(n) = \frac{\langle u_i, u_i \rangle}{\langle u_{i-1}, u_{i-1} \rangle} = \frac{\sum_{t=1}^{n} u_i^2(t)}{\sum_{t=1}^{n} u_{i-1}^2(t)}$$

and

$$\mu = \frac{1}{n}\sum_{t=1}^{n} t$$

Considering the range of values of t to be $t_i = i$, $i = 1, 2, 3, \ldots n$, we get

$$b_i(n) = \frac{i^2(n^2 - i^2)}{4(4i^2 - 1)},$$

$$\mu = \frac{1}{n}\sum_{t=1}^{n} t = \frac{n+1}{2}$$

As shown in Eq. (4), we construct the orthogonal polynomial operator $|M|$ based on the orthogonal polynomials in Eq. (5). $|M|$ can easily be made an integer transform by scaling its elements appropriately.

For the sake of computational simplicity, the finite Cartesian coordinate set X, Y is labeled as {1,2,3}. The point spread operator in eq. (3) that defines the linear orthogonal transformation for image coding can be obtained as $|M| \otimes |M|$, where $|M|$ can be computed and scaled from Eq. (4) as follows.

$$|M| = \begin{vmatrix} u_0(x_0) & u_1(x_0) & u_2(x_0) \\ u_0(x_1) & u_1(x_1) & u_2(x_1) \\ u_0(x_2) & u_1(x_2) & u_2(x_2) \end{vmatrix} = \begin{vmatrix} 1 & -1 & 1 \\ 1 & 0 & -2 \\ 1 & 1 & 1 \end{vmatrix} \quad \ldots (6)$$

The set of polynomial operators O_{ij}^n ($0 \leq i, j \leq n-1$) can be computed as

$$O_{ij}^n = \hat{u}_i \otimes \hat{u}_j^t$$

where $\hat{u}_i$ is the (i + 1) st column vector of |M|. The complete set of basis operators of sizes (2 X 2) and (3 X 3) are given below.

Polynomial Basis Operators

Polynomial basis operators of size (2 * 2) are

$$\left[O_{00}^{2}\right] = \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}, \left[O_{01}^{2}\right] = \begin{bmatrix} -1 & 1 \\ -1 & 1 \end{bmatrix}, \left[O_{10}^{2}\right] = \begin{bmatrix} -1 & -1 \\ 1 & 1 \end{bmatrix},$$

$$\left[O_{11}^{2}\right] = \begin{bmatrix} 1 & -1 \\ -1 & 1 \end{bmatrix} \text{ where } |M| = \begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix}$$

Polynomial basis operators of (3 * 3) are

$$\left[O_{00}^{3}\right] = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix}, \left[O_{01}^{3}\right] = \begin{bmatrix} -1 & 0 & 1 \\ -1 & 0 & 1 \\ -1 & 0 & 1 \end{bmatrix},$$

$$\left[O_{02}^{3}\right] = \begin{bmatrix} 1 & -2 & 1 \\ 1 & -2 & 1 \\ 1 & -2 & 1 \end{bmatrix}, \left[O_{10}^{3}\right] = \begin{bmatrix} -1 & -1 & -1 \\ 0 & 0 & 0 \\ 1 & 1 & 1 \end{bmatrix},$$

$$\left[O_{11}^{3}\right] = \begin{bmatrix} 1 & 0 & -1 \\ 0 & 0 & 0 \\ -1 & 0 & 1 \end{bmatrix}, \left[O_{12}^{3}\right] = \begin{bmatrix} -1 & 2 & -1 \\ 0 & 0 & 0 \\ 1 & -2 & 1 \end{bmatrix},$$

$$[O_{20}^3] = \begin{bmatrix} 1 & 1 & 1 \\ -2 & -2 & -2 \\ 1 & 1 & 1 \end{bmatrix}, [O_{21}^3] = \begin{bmatrix} -1 & 0 & 1 \\ 2 & 0 & -2 \\ -1 & 0 & 1 \end{bmatrix},$$

$$[O_{22}^3] = \begin{bmatrix} 1 & -2 & 1 \\ -2 & 4 & -2 \\ 1 & -2 & 1 \end{bmatrix}$$

In the next section, the scheme that is used for encrypting the OPT transformed blocks is described.

4. Proposed Selective Combinational Scrambling in OPT domain

The proposed technique employs three levels of permutation on selected blocks and coefficients. All the three levels of permutation make use of a cryptographically secure random number generator whose seed value is derived from a key as described in section 4.5. At the lowest level, bits of selected coefficients are scrambled. The next level of scrambling involves permutation of selected low frequency OPT coefficients. At the topmost level, shuffling of randomly chosen blocks is performed. Also in order to diffuse statistics, the sign bits of the transformed coefficients and the DC components are encrypted using a user key in a random manner.

4. 1 Bit scrambling

The first basic approach scrambles selected bits in the transformed coefficients to encrypt an image. For example, we can randomly change the sign of each coefficient. A key-based cryptographically secure pseudo random process controls the sign change process. Because the sign-inverted coefficients distribute their energy over the entire block they are derived from, sign bit scrambling is very effective at producing notable degradation in image quality. The remaining bits of the chosen coefficients are also scrambled. This is done using a sequence of bit rotation operations where the number of rotations and the direction of rotation are derived from the secret key. Such a scrambling of bits, adds another level of image degradation and security with little complexity.

4.2 Shuffling of block coefficients

To increase the level of security, we shuffle selected coefficients of all the blocks. The Transformed coefficients to be shuffled are first selected using a pseudorandom sequence generated from the secret key. Then these coefficients are shuffled according to a shuffling sequence generated using a sub key derived from the secret key. The shuffling sequence varies from block to block. The visual effect of the shuffling on an uncompressed image is dramatic. The DC coefficients in the transformed blocks are easily identifiable though they are shuffled, due to their huge magnitude compared to the AC coefficients. Due to this, an attacker can easily spot the DC coefficients and reconstruct an approximate image supplying constant values for the unknown AC coefficients. So we propose to render the DC coefficients unidentifiable by scaling them using a constant value derived from the secret key.

4.3 Block Shuffling

A third level of security is achieved in our proposed technique by performing a global shuffling of selected transformed coefficient blocks. A global shuffling of the transformed coefficient blocks is much more secure than a local shuffling of coefficients of different frequencies. The blocks to be shuffled are first selected according to a pseudo-random sequence generated using a secret sub-key as the seed. These blocks are then split into subsets and are shuffled. This shuffling changes the high-level spatial configuration of the content, which is much harder for an attacker to analyze than the local shuffling of coefficients of different frequencies where statistics of different frequency components can be exploited for an efficient attack.

The proposed encryption algorithm combining the above mentioned shuffling schemes in orthogonal polynomials based transformation domain is presented in the following section.

4.4 The Proposed Encryption algorithm

The steps involved in the proposed encryption process are given below.

Input : Cover image of size *H* x *W*, secret key
Output : Encrypted image

Step 1: Divide the input cover image of size *H* x *W* pixels into non-overlapping blocks of size *N* x *N* where *N*<*H*, *W* . Let each block be denoted as $[I_{ij}]$ $(0 \le i < H/N,\ 0 \le j < W/N)$.

Step 2: Apply the proposed Orthogonal Polynomials based transform and compute the block of OPT coefficients $[\beta'_{ij}]$ as described in Eq. (4).

Step 3: Perform the steps 4 thro’ 9 for all the OPT coefficient blocks, $\{ [\beta'_{ij}] \mid 0 \le i < H/N,\ 0 \le j < W/N \}$.

Step 4: Arrange the elements of $[\beta'_{ij}]$ in a 1-D zig-zag sequence to form the feature vector *fv*.

Step 5: Choose the first *n* low frequency OPT coefficients from *fv* to form *lfv,* where *n* is calculated using the block size and the secret key *k*.

Step 6: Select coefficients from *lfv* using the pseudo-random sequence S_1 generated using the sub-key k_1 and encrypt their sign-bits.

Step 7: Scale the magnitude of the DC coefficient using the scaling factor *S* generated from the secret key *k.*

Step 8: Using the pseudo-random sequence S_2 generated using the sub-key k_2, select the coefficients to whose bits are rotated in the irection *dr* for *np* number of positions to get the bit permuted feature vector [lfv_{bi}]. Here,

$$dr = \begin{array}{l} left \ : k_2(0) = 0 \\ right : k_2(0) = 1 \end{array}$$

where $k_2(0)$ is the first bit of k_2

$$np = \sum_{i=0}^{2} k_2(i+1) \times 2^i$$

Step 9: Shuffle the elements $Elfv_{bi}$ of [lfv_{bi}] to get [lfv_{co}] using M_{S3} ($Elfv_{bi}$) where M_{S3} ($Elfv_{bi}$) is a mapping defined by S_3 generated from the sub-key k_3

Step 10: Select the blocks [lfv_{co}] to be shuffled using S_{41} and Perform permutation using M_{S42} ([lfv_{co}]) where M_{S42} (lfv_{co}) is a mapping defined by S_{42}

Step 11: Reconstruct the image using the basis function described in Section 3 to get the encrypted image.

Step 12: End.

The process of the proposed OPT domain encryption is depicted in Figure 1. Here,

S is theScaling factor derived from the secret key *k*.

S_1, S_2 , S_3 , S_{41}, S_{42} are the Pseudo-random sequences generated from the secret key *k.*

dr is the direction in which bits are rotated.

np is the number of rotations performed.

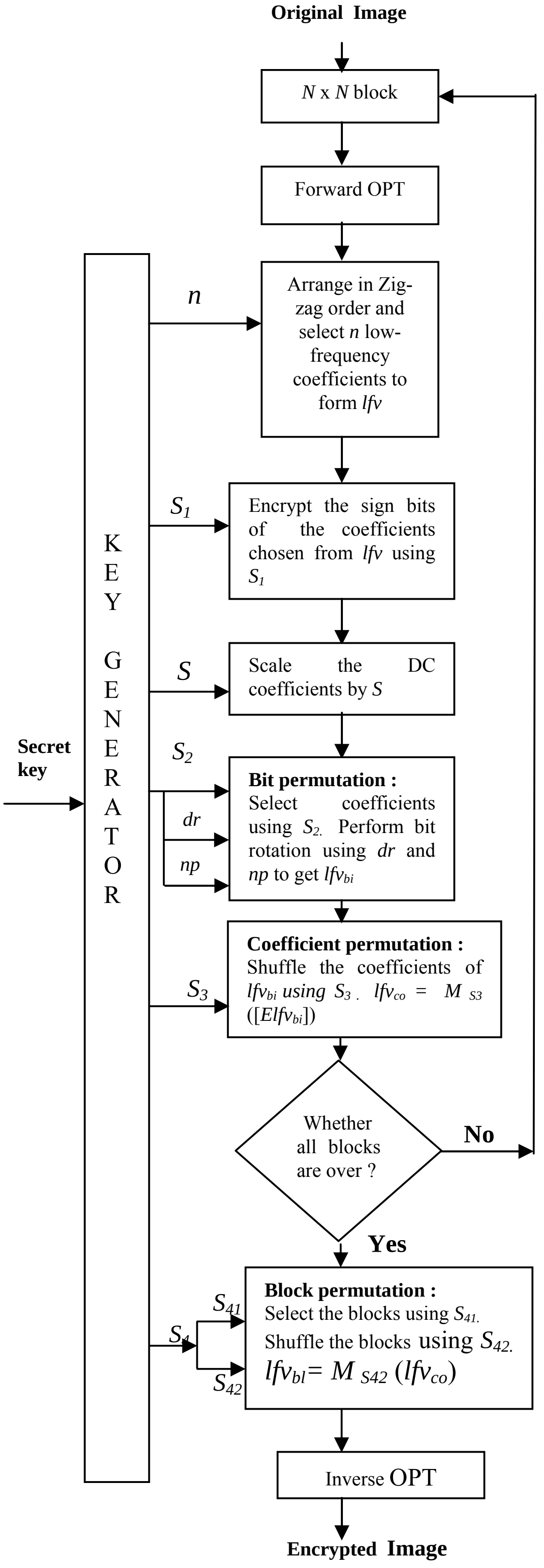

Original Image
N x N block
Forward OPT
Arrange in Zig-zag order and select n low-frequency coefficients to form lfv
n
Encrypt the sign bits of the coefficients chosen from lfv using S1
S1
Scale the DC coefficients by S
S
S2
dr
np
Bit permutation : Select coefficients using S2. Perform bit rotation using dr and np to get lfvbi
Coefficient permutation : Shuffle the coefficients of lfvbi using S3 . lfvco = M S3 ([Elfvbi])
S3
Whether all blocks are over ?
No
Yes
Block permutation : Select the blocks using S41. Shuffle the blocks using S42. lfvbl= M S42 (lfvco)
S4
S41
S42
Inverse OPT
Encrypted Image
Secret key
K E Y G E N E R A T O R

Figure 1. Flowchart for proposed OPT domain encryption

The decryption process is the reverse of the encryption process described above. In the next section we present the key generation procedure.

4.5 Key Generation Procedure

Since the security of the proposed encryption algorithm lies in the secret key, we propose a new key generation technique in which a 256 bit user pass phrase *k* is split into four sub-keys k_1, k_2, k_3 and k_4 of 32 bits each. The scaling factor *S* for the DC coefficients is derived from *k*. The value *n,* which is calculated from the block size and the sub-key k_1, are used to select the low frequency coefficients from the transformed block. A cryptographically secure pseudo-random number generator (PRNG) is used to generate the sequences S_1, S_2 and S_3 with k_1, k_2 and k_3 as seed values respectively. The sequence S_1 is used for sign-bit encryption while S_2 *is* used for pixel permutation and S_3 is used for coefficient permutation. The sequence S_4 generated using k_4 as the seed value is split into two subsequences S_{41} and S_{42} and are employed in block selection and block permutation. The proposed key generation process is depicted in Fig. 2.

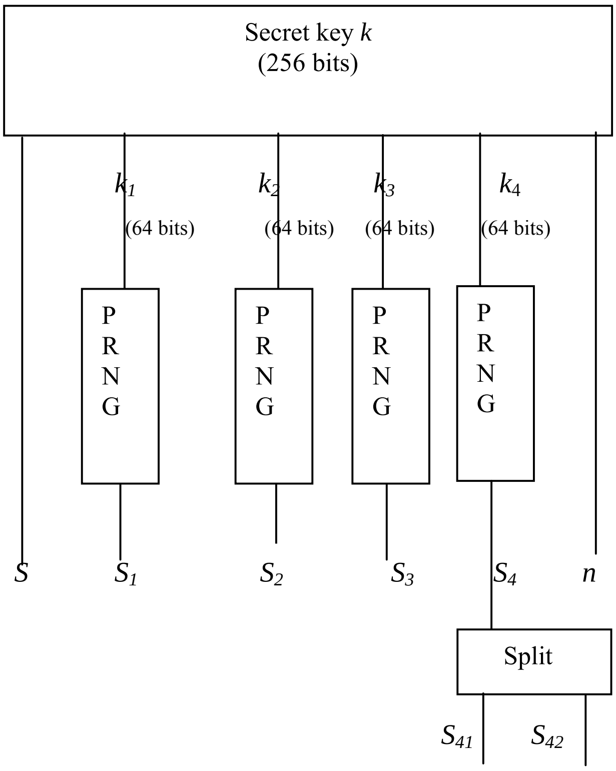


Fig. 2. Key Generator

5. Measures of Performance

The performance of the proposed selective combinational encryption scheme in orthogonal polynomials based transform domain is measured by computing the peak signal-to-noise ratio (PSNR), which is defined as

$$PSNR = 10\log_{10}\frac{(255)^2}{e_{ms}^2}$$

...(7)

where the average mean-square error, e_{ms} is,

$$e_{ms}^2 = \frac{1}{NM}\sum_{i=1}^{N}\sum_{i=1}^{M}E(u_{i,j} - u_{i,j}^{'})^2$$

where $u_{i,j}$ and $u'_{i,j}$ represent the N x M original and reproduced images respectively. The Encryption-PSNR is expected to be very low for a good encryption scheme.

The correlation between adjacent pixels are analyzed by calculating the correlation coefficients using the following formula

$$r_{xy} = \frac{\operatorname{cov}(x,y)}{\sqrt{D(x)}\sqrt{D(y)}}$$

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

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

$$\operatorname{cov}(x,y) = E(x_i - E(x))(y_i - E(y))$$

…(8)

where E(x) is the estimation of mathematical expectations of x, D(x) is the estimation of variance of x and cov(x, y) is the estimation of covariance between x and y, where x and y are grey-scale values of two adjacent pixels in the image.

To test the influence of one-pixel change on the whole image encrypted by the proposed algorithm, two common measures are used: Number of Pixels Change Rate (NPCR) and Unified Average Changing Intensity (UACI). NPCR and UACI are defined by the following formulas:

$$\text{NPCR} = \frac{\sum_{i,j} D(i,j)}{W \times H} \times 100\%$$

…(9)

$$\text{UACI} = \frac{1}{W \times H}\left[\sum_{i,j}\frac{\left|c_1(i,j) - c_2(i,j)\right|}{255}\right] \times 100\% \qquad \ldots(10)$$

where W and H are the width and Height of the image. $C_1(i, j)$, $C_2(i, j)$ are the grey scale values of the pixels at position (i,j). D(i, j) is determined by $C_1(i, j)$ and $C_2(i, j)$, that is, if $C_1(i, j) = C_2(i, j)$, then, D(i, j) = 1; otherwise, D(i, j) = 0.

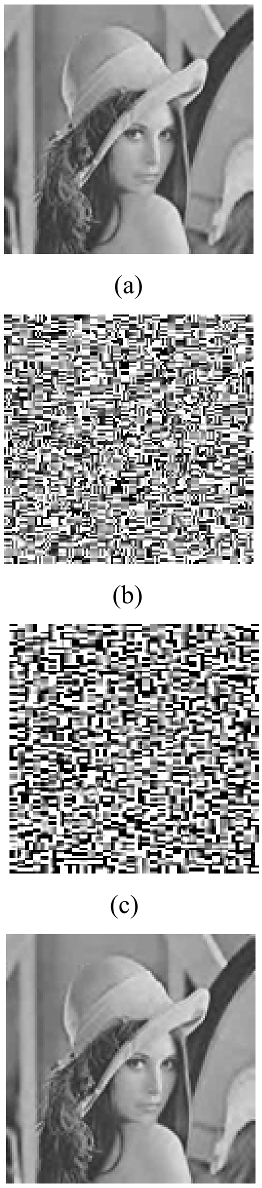
6. Experimental results and Security analysis

The proposed encryption process described in section 4 has been experimented with several images and the results are reported in this section. The test images are gray scale of size (128 x 128) with pixel values in the range 0 - 255. One such standard image namely Lena image is shown in Fig. 3(a).

The original images are first divided into 4 x 4 non-overlapping blocks and the proposed OPT transform is applied on each block as described in section 2. Then the resulting 2-D transform coefficients are re-arranged into a 1-D zigzag sequence and *n* low frequency non-zero OPT coefficients are chosen to form the feature vector. We choose low-frequency components of OPT as these components tend to have large energies and encrypting these components renders the image unintelligible. Then the image is encrypted using a combination of the shuffling approaches described in section 4 using the sub-keys derived from a 256-bits secret key, in the OPT domain. In our experiments we have selected only 4096 coefficients (25%) for encryption. The encrypted version of the test image Lena is shown in Fig. 3b. The Peak Signal to Noise Ratio (PSNR) between the original and the encrypted Lena images is computed as described in Section 5 and is found to be 7.89 dB which signifies effective encryption. The encrypted image is then decrypted using the symmetric secret key along with the basis function defined in section 3, to get the original image and is shown Fig. 3(d). The original image is also encrypted in DCT domain and is shown in Fig. 3(c). The PSNR is computed for the same and is found to be 9.23 dB which is greater than the OPT domain encryption PSNR.

6.1 Key space analysis

The key space should be large enough in order to render an image cryptosystem secure against brute force attack. The proposed algorithm makes use of a key of length 256 bits and therefore an attacker has to try out 2^{256} ($1.158 \text{ X } 10^{77}$) combinations of the secret key. An image cipher with such a large key space is sufficient for reliable practical use.


(a)

(b)

(c)

(d)

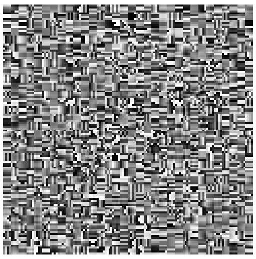
Fig. 3. Encryption and Decryption (a) Original Image (b) Encrypted image using the proposed scheme (c) Encrypted image using DCT (d) Decrypted image

6.2 Key sensitivity analysis

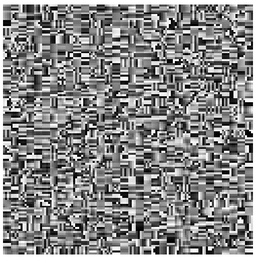
A key sensitivity test is performed by first encrypting the test image using a 256- bits test key (Sk1) to get the encrypted image shown in Fig. 4(a). Then the least significant bit of the test key is changed to form another key (Sk2) and is used to encrypt the same test image to get the encrypted image and the same is shown in Fig. 4(b). Finally the images encrypted using the slightly different keys, are compared. It is observed that the image shown in Fig. 4(a) is different from the image shown in Fig. 4(b) and the difference image is presented in Fig. 4(c). The same experiment is repeated for another key (Sk3) obtained by changing the most significant bit of the test key and the encrypted image is presented in Fig. 4(d). It is not easy to compare the encrypted images by simply observing these images. So for comparison, the correlation between the corresponding pixels of the three encrypted images is calculated using the formula given in Eq. (8). In Table 1, the results of the correlation coefficients between the corresponding pixels of the three images encrypted using the aforementioned slightly different keys, is presented. It is clear from the table that no correlation exists among three encrypted images even though these have been produced by using slightly different secret keys.

Furthermore, when a secret key SK1 is used to encrypt an image and a slightly modified key SK2 obtained by changing the LSB of SK1, is used to decrypt the ciphered image, the decryption completely fails as shown in Fig. 4(e).

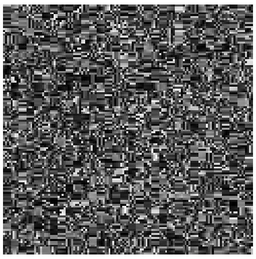
To test the influence of one-pixel change on the plain image, encrypted by the proposed scheme, two common measures NPCR and UACI described in Section 5 are used. Here C1 and C2 are the encrypted images whose corresponding plain images have only one pixel difference. The NPCR and UACI values obtained are 0.214 and 0.396 respectively which indicates that the proposed algorithm has fairly good ability to resist differential attacks.



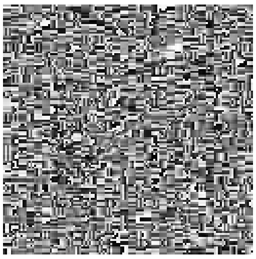
(a)



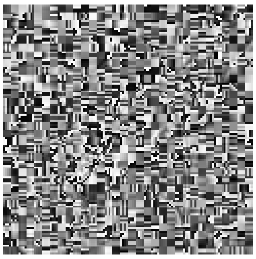
(b)



(c)



(d)



(e)

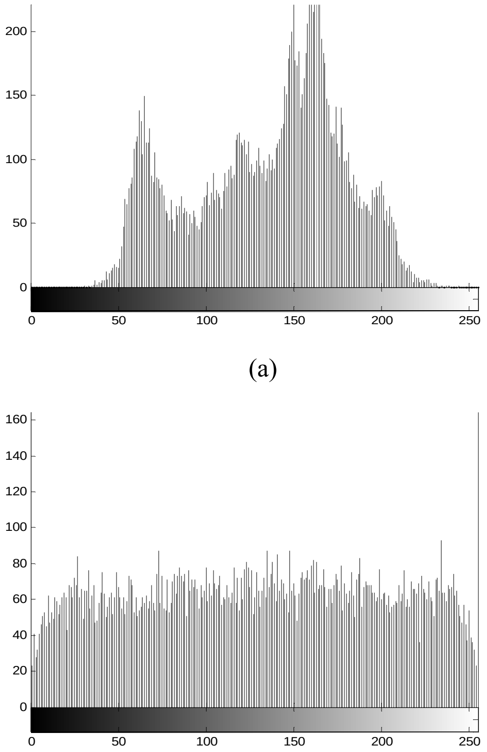
Fig. 4. Key sensitivity test (a) Test image encryptedusing key Sk1. (b) Test image encrypted using Sk2. (c) Difference between Fig. 4(a) & Fig. 4(b). (d) Test image encrypted using Sk3 (e) Failed Decryption using slightly modified key.

Image1 obtained using key	Image 2 obtained using key	Correlation coefficient	
		Lena	Peppers
Sk1	Sk2	0.0366	0.0381
Sk2	Sk3	0.0325	0.0427
Sk1	Sk3	0.0312	0.0412

Table 1. Correlation coefficients between the corresponding pixels of the two encrypted images (Image1 & Image2) obtained by using slightly different secret keys on Lena and Peppers images

6.3 Statistical analysis

To demonstrate that our proposed algorithm has strong resistance to statistical attacks, test is carried out on the histogram of enciphered image. Several gray-scale images of size 128 X 128 are selected for this purpose and their histograms are compared with their corresponding ciphered image. One typical example is shown in Fig. 5. The histogram of the plain image contains large spikes as shown in Fig. 5(a) but the histogram of the cipher image as shown in Fig. 5(b), is more uniform. It is clear that the histogram of the encrypted image is, significantly different from the respective histogram of the original image and bears no statistical resemblance to the plain image. Hence statistical attack on the proposed image encryption procedure is difficult.



(a)

(b)

Fig. 5 Histograms of original and encrypted images (a) Histogram of Original image shown in Fig. 3(a) (b) Histogram of encrypted image shown in Fig. 3(b)

7. Conclusion

In this paper, we have proposed a simple but effective method of selective encryption of gray scale images using combinational permutation in orthogonal polynomials based transform domain. The proposed scheme selects high energy coefficients after de-correlating the image pixels using the proposed orthogonal polynomials based transformation. Then a combination of bit shuffling, coefficient shuffling and block shuffling is employed to further reduce the correlation. In addition we perform scaling of DC coefficients and sign bit encryption in order to diffuse statistics. A cryptographically secure pseudo-random number generator whose seed values are the sub-keys generated from a 256-bits secret key is used to perform the encryption. From the experimental results, it is evident that the proposed encryption scheme offers very low encryption PSNRs and is resistant to statistical analysis. This scheme achieves the advantages of selective encryption as well as all the individual permutation techniques and overcomes their limitations. The proposed encryption technique can be used in applications where protection is needed against casual observer. The level of security can be further increased if necessary, by increasing the number of bits in the secret key and by performing a number of permutation rounds with a random combination of permutation techniques for each round.

References

[1] Shi C., Bhargava B., “A Fast MPEG video encryption algorithm,” Proceedings of the sixth ACM International Multimedia conference,” Bristol, U.K., pp. 81-88, 1998.

[2] Zeng W., Lei S., “Efficient frequency domain video scrambling for content access control,” Proceedings of the seventh ACM International Muultimedia conference,” pp. 285-293, 1999.

[3] Mark M. Fisch, Herbert Stogner and Andreas Uhl, “ Layered encryption techniques for DCT-coded visual data,” Proceedings of the European Signal Processing Conference, EUSIPCO ’04, Vienna, Austria, 2004.

[4] Cheng H., Li X., “Partial encryption of compressed images and videos,” IEEE Transactions on Signal Processing vol. 48, no. 8, pp. 2439-2451, 2000.

[5] Marc Van Droogenbroeck and Raphael Benedett, “ Techniques for a selective encryption of uncompressed and compressed images,” Proceedings of ACIVS (Advanced Concepts for Intelligent Vision Systems), Belgium, pp. 90-97, 2002.

[6] Roman Pfarrhofer and Andreas Uhl, “Selective Encryption Using JBIG,”, International Federation for Information Processing, LNCS 3677, pp. 98-107, 2005.

[7] Andreas Pommer and Andreas Uhl, “Selective encryption of wavelet-packet encoded image data: efficiency and security,” Multimedia Systems, Springer Verlag, vol. 9, pp. 279-287, 2003.

[8] Fridrich J., “Symmetric Ciphers Based on Two-dimensional Chaotic Maps,” International Journal of Bifurcat Chaos vol. 8, no. 6, pp. 1259-1284, 1998.

[9] Chen G. , Mao Y.B. and Chui C. K., "A symmetric image encryption scheme based on 3D chaotic cat maps," Chaos, Solitons & Fractals, vol. 12, pp. 749-761, 2004.

[10] Mao Y. B., Chen G., Lian S.G., "A novel fast image encryption scheme based on the 3D chaotic baker map," International Journal of Bifurcat Chaos, vol. 14, no. 10, pp. 3613-3624, 2004.

[11] Guan Z. H. , Huang F. J. and Guan W. J. , "Chaos-based image encryption algorithm," Physics Letters vol. 346, pp. 153-157, 2005.

[12] Lian SG, Sun J and Wang Z., "A block cipher based on a suitable use of chaotic standard map," Chaos, Solitons and Fractals, vol. 26, no. 1, pp. 117-129, 2005.

[13] Hossam El-din H. Ahmed, Hamdy M.kalash and Osama S. Farag Allah, " An Efficient Chaos- based Feedback Stream Cipher (ECBFSC) for Image Encryption and Decryption," Informatica, vol. 31, pp. 121-129, 2007.

[14] Feng Huang,Yong Feng and Xinhuo Yu, " A Symmetric Image Encryption scheme based on a simple novel Two-dimensional Map," International Journal of Innovative Computing, Information and Control, vol. 3, no. 6(b), pp. 1593-1602, 2007.

[15] A. Sinha and K. Singh, "A Technique for Image Encryption using Digital Signature," Optics Communications, vol. 218, pp.229-234, 2003.

[16] Mitra A., Subba Rao Y. V. and Prasanna R. M., "A New Image Encryption Approach using Combinational Permutation Techniques," International Journal of Computer Science, vol. 1, no. 1, pp. 127-131, 2006.

[17] Han Shuihua and Yuang Shuangyuan, "An Asymmetric Image Encryption Based on Matrix Transformation," ECTI Transactions on Computer and Information Technology vol.1, no. 2, pp. 126-133, 2005.

[18] Chang-Mok Shin, Dong-Hoan Seo and Soo-Joong Kim, "Gray-level Image Encryption scheme using Full Phase Encryption and Phase-Encoded Exclusive-OR Operations," Optical Review, vol. 11, no. 1, pp. 34-37, 2004.

[19] M. Zeghid, M. Machhout, L. Khriji, A. Baganne and R. Tourki, " A Modified AES Based Algorithm for Image Encryption", International Journal of Computer Science and Engineering vol. 1, no. 1, pp. 70-75, 2006.

[20] Chang-Mok Shin and Soo-Joong Kim, " Phase-Only Encryption and Single Path Decryption System using Phase-Encoded Exclusive-OR Rules in Fourier Domain," Optical Overview, vol. 13, no. 2, pp. 49-52, 2006.

[21] Yumnam Kirani Singh and Swapan Kumar Parui, "Simplet and its Application in Signal Encryption," Mutimedia Systems and Signal Processing, vol. 15, pp. 375-394, 2004.

About the authors

Dr. R. Krishnamoorthi is the Professor and Head of the Department of Information Technology at Bharathidasan Institute of Technology, Anna University, Tiruchirapalli. He obtained his Ph.D. in Image processing from the Indian Institute of Technology, Karaghpur in the year 1995 and M.Tech., in Computer Science and Engineering from the Indian Institute of Technology, Kanpur, in the year 1992. He has authored several books in Computer Science and has published many research papers in reputed journals, international and national conferences. He has to his credit several sponsored projects in Image Processing. His areas of interest include Image Compression, Digital Watermarking, Steganography, Image encryption and authentication, Content based image retrieval, Iris authentication and Software Testing. He has produced six doctorates in image processing and is currently guiding eight research scholars.

Mrs. Sheba Kezia Malarchelvi is a research scholar in the department of Information Techonology at Bharathidasan Institute of Technology. She completed B. E. in Mepco Schlenk Engineering College, Madurai Kamaraj University, TamilNadu, India, in the year 1991 and M. E. in Computer Science and Engineering in the Regional Engineering College, Tiruchirapalli, TamilNadu, India, in the year 1995. Her areas of interest include Network Security, Digital Watermarking, Steganography, Image Encryption and Authentication.