Selective Image Encryption using Singular Value Decomposition and Arnold Transform

Kshiramani Naik[1], Arup Kumar Pal[1], and Rohit Agarwal[2]
[1]Department of Computer Science and Engineering, Indian School of Mines, India
[2]Department of Computer Science and Engineering, JSS Academy of Technical Education, India

Abstract: *Selective image cryptosystem is a popular method due to its low computational overhead for enciphering the large volume of digital images. Generally selective cryptosystem encrypts the significant part of the data set while the insignificant part is considered in compression process. As a result, such kind of approaches reduces the computational overhead of encryption process as well as properly utilizes the limited bandwidth of communication channel. In this paper the authors have proposed an image cryptosystem for a compressed image. Initially, the original image was compressed using Singular Value Decomposition (SVD) and subsequently, the selective parts of the compressed image are considered for enciphering purpose. We have followed the confusion-diffusion mechanism to encrypt the compressed image. In encryption process, the Arnold Cat Map (ACM) is used and the associated parameters of ACM are kept secret. The scheme is tested on a set of standard grayscale images and satisfactory results have been found in terms of various subjective and objective analysis like the visual appearance of cipher image, disparity of histogram with original one, computation of Peak Signal to Noise Ratio (PSNR), Number of Pixel Change Rate (NPCR), correlation coefficient and entropy.*

Keywords: *Arnold transform; confusion-diffusion mechanism; selective image cryptosystem; singular value decomposition.*

Received November 10, 2014; accepted September 22, 2015

1. Introduction

With the rapid development in the digital world, the usage of multimedia data like audio, image and video over the Internet have attracted more and more among people. Conversely, the important data transmission over open communication channel is vulnerable due to lack of inherent security and is easily intercepted by various passive or active attacks. As a result, the protection of the important data against different attacks has been considered as a major challenge among researchers. Day by day, numerous security mechanisms have been devised to meet the challenges of ensuring the confidentiality and access control of the important data during transmission. One of the effective mechanisms to secure the multimedia data is encryption of the data before transmission. Encryption is a process by which the multimedia data change into an unrecognized form using the secret key [21]. The original data can be recovered only by the authorized entities in the reverse way of the encryption process with the same secret key, where the process is known as decryption. Although several well accepted standard symmetric block cipher like Data Encryption Standard (DES), Advanced Encryption Standard (AES), International Data Encryption Algorithm (IDEA), CAST, Blowfish, RC5 etc., [18] have been used for protecting the textual data where those encryption algorithms work on the small size of input block like 64 bits or 128 bits. In general, the volume of multimedia data is enormously larger than the block of size 64 bits or 128 bits. So those data encryption algorithms are not suitable to employ directly on large-volume of multimedia data due to the constraint of high computational overhead for encrypting them. Also the conventional symmetric data encryption techniques are sometime defeated to encrypt the multimedia data significantly due to the presence of high correlation among the adjacent data elements. So there is a need of some different approaches to encrypt the multimedia data in efficient way compare to the textual data. Several researchers have suggested a number of encryption techniques on image, audio or video data which are broadly categorized as image cryptosystem, audio cryptosystem and video cryptosystem [10] respectively. Digital image is one of the popular multimedia data which is used in several real time applications. So in this paper, we have studied and developed cryptosystem for image data. Image data is in general manipulated or processed either in spatial or frequency/transform domain. Several image cryptosystems have been devised in both spatial and frequency/transform domain. Since each element of the image data does not carry the same amount of information like textual data, so the significant information part may be encrypted with high priority compare to the less significant part. Based on this property, image encryption is generally carried out in either in whole data set, i.e. known as full/total encryption or in partial data set i.e., classified as selective/partial encryption [2, 13].

Spatial domain refers to the image plane itself and the image cryptosystem based on spatial domain related to the direct manipulation of the pixels of the image. In these algorithms, the general encryption usually destroys the correlation among the pixels and thus makes the encrypted images incompressible. The image cryptosystem based on this type of algorithm is known as a lossless image cryptosystem. In full image cryptosystem, the whole data set is considered in the encryption process. But for various important applications like any real time application, it is considered as unsuitable as it is computationally high and time consuming. While the partial or selective encryption works on a subset of the entire data so its computational overhead is less compared to the full encryption process and hence this method is widely accepted. In Zhou *et al*. [24] proposed a full image cryptosystem using four rounds of encryption structure. Each round includes five steps: the random pixel insertion, row separation, 1D substitution, row combination and image rotation. The proposed algorithm produces a completely different encrypted image each time using the same set of secret keys. Zhang and Xiao [23], proposes a block based image encryption scheme using bit-level permutation. Firstly, divide a plain image into non-overlapping square blocks with a random matrix, then transform each block into three dimensional (3-D) binary matrixes, which has six directions just as a cube. Permutation is performed by multiplying the 3-D matrix by the rotation matrix that relies on plain image according to different direction. Again block based diffusion is performed to change the statistical characteristics of the image. In Naik and Pal. [15] proposed a selective encryption algorithm where the scrambled image is divided into bit planes. Only the significant bit-planes are encrypted using the different binary key matrices to achieve a higher level of security. Bhatnagar and Wu [2] proposed a lossless selective encryption technique, presented in spatial domain. The confusion is done globally to the image using the Saw-tooth space filling curve, and the confused image is divided into the significant and insignificant part using Pixel of Interest method. Only the significant part is diffused to reduce the computational overhead. Then the diffusion process is done on the significant part using a secret key matrix generated from non-linear chaotic map and singular value decomposition. Chen *et al*. [5], proposed a method to encrypt a color image based on the Arnold transform and the interference method. In their work, a color image is decomposed into three independent channels (i.e., red, green, and blue), and each channel is then encrypted into two random phase masks. The merit of the spatial domain method is simple, but for the low bandwidth communication channel and for transmission efficiency sometimes data need to be reduced before transmission. In this case frequency domain methods are better utilized. In frequency domain methods, the input images are decomposed into the transform coefficients initially, which facilitate to distinguish the image into significant and insignificant parts. The encryption on the significant data introduces a desired level of degradation in the image data while the insignificant data are sometimes discarded for compression purpose. This can be achieved using various transformation tools like DCT [1, 6], DWT [8, 20], SVD [16, 19] etc. The cryptosystems include this type of algorithm are referred as a lossy image cryptosystem. In Liu *et al*. [12] proposed an image encryption scheme based on the Fractional Fourier transform and Arnold Cat Map. The original image is first multiplied by a random phase generated by logistic map and subsequently transformed by the fractional Fourier transform. Then the pixels of the transformed image are scrambled using two- dimensional cat map. Khashan and Zin [7] presented a partial encryption scheme using symmetrical ciphers. Furthermore, to reduce the perceivable information for other unencrypted parts, the transformation technique is proposed to shuffle the image blocks and to decrease the correlation among image elements. Samson and Sastry [17] proposed an approach for image encryption supported by lossy compression using multilevel wavelet transform. The input image is decomposed using multilevel 2-D wavelet transform, and then the thresholding is applied to the decomposed structure to get the compressed image. Encryption is performed by decomposing the compressed image by multi-level 2-D Haar Wavelet transform.

The proposed article utilizes the Singular Value Decomposition (SVD) transformation tool with the intention of reduced data set to facilitate low computational overhead and proper bandwidth utilization. During encryption of the reduced data set Arnold Transformation Arnold Cat Map (ACM) has utilized. Nowadays Arnold transformation has been considered as a popular encoding method as it disturbs the tight relationship of the matrix values by changing their positions and let the image be unrecognized. By taking this advantage of the ACM, already various transform domain based image cryptosystems have been devised. In Chen *et al*. [3] proposed an image encryption algorithm based on singular value decomposition and Arnold transform in fractional domain. An original image is first transformed into the fractional domain by Fractional Fourier Transform (FRFT). Then it is decomposed into three segments by SVD. All these three parts are transformed using Arnold Cat Map to produce three encoded image components. In order to avoid the opponent to obtain the correct image in correct order, the three encoded image parts are kept in several places. This scheme is based on permutation-only image cipher. However, this kind of image cipher is vulnerable to known/chosen plain text attack and statistical attack. In

Taneja *et al*. [20] proposed a selective image encryption scheme based on fractional wavelet domain. This scheme encrypts only significant sub bands which are selected using the relationship between normalized information energy and perceptual information of sub bands. The significant sub bands are then Arnold transform numbers of times. As compared to the former methods, the proposed method is an effective and a new image encryption method with enhanced secrecy. Before encryption, first the authors have incorporated SVD during transformation of the secret image, which helps to distinguish the secret image into significant and insignificant part. Subsequently the secret image is truncated by discarding the insignificant coefficients in order to avoid computational overhead and for utilization of limited bandwidth during communication. For the sake of security, the selected significant parts of the SVD transformed image are fed into encryption process. The encryption process is carried out considering both the confusion and diffusion process simultaneously. In the confusion process, a key sequence is incorporated with the generalized ACM while the confused dataset is further used to produce large key space for the diffusion process. The proposed scheme is capable to encrypt the image data efficiently.

The rest of this paper is organized as follows. Section 2 presents some fundamentals related to the proposed scheme. In section 3, the proposed image cryptosystem is discussed in detail. The simulation results and security analysis are presented in section 4. Finally the conclusions are stated in section 5.

2. Preliminaries

In this section, a model of image cryptosystem, SVD and ACM are described in briefly for the purpose of understanding the subsequent discussions.

2.1. Confusion-Diffusion based Image Cryptosystem

The Confusion and diffusion are two basic techniques, mainly used during the encryption process of secret message. The confusion, changes the positions of the pixels so that the relationship between the key and the cipher image become very complex and it discourages all the attempts to observe the cipher image looking for redundancies and statistical patterns. The confusion is done by various techniques like magic square transform [11], chaos system [9], gray code [25], ACM [3] etc., But the original image can be obtained by performing reverse operations if the key is known. Hence, to make the process more complicated and to enhance the security, confused image then undergoes diffusion phase. In diffusion, the confused image is then passed through some cryptographic algorithms like scan based methods [14], chaos based methods [4] and other miscellaneous methods. Diffusion dissipates the redundancy of the original image by spreading it out over the whole cipher image. A classical model of confusion-diffusion based image cryptosystem is shown in Figure1.

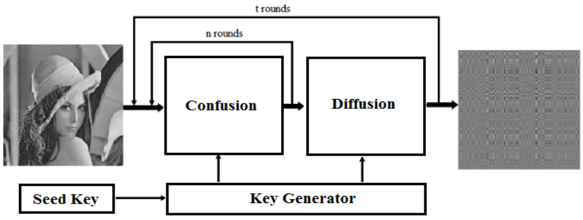


Figure 1. Classical image cryptosystem.

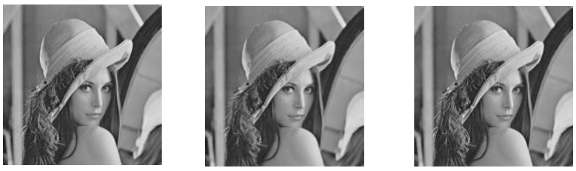
In the confusion phase several numbers of rounds are performed to decorrelate the adjacent pixels. The whole process i.e., confusion followed by diffusion is repeated a number of rounds to achieve a satisfactory level of security.

2.2. Singular Value Decomposition (SVD)

In linear algebra, the SVD is able to reduce the dimension of the matrices effectively. Let *A* be a general real (complex) matrix with m×n, with rank *r* and $r \leq n \leq m$. Then A can be factorized into three matrices as follows:

$$A = USV^T \qquad (1)$$

Where U and V are orthogonal (unitary) matrix, and S = $diag(\sigma 1, \sigma 2, \ldots, \sigma r)$, where σi, $i = 1$ to r are the singular values of the matrix with $r = min(m,n)$ and satisfying $\sigma 1 \geq \sigma 2 \geq \ldots.. \geq \sigma r$. SVD has many applications in digital image processing due to some advantages. First, it can be applied to any square or rectangular matrix. Secondly, the significant Eigen vectors can be chosen based on singular values. Generally, in case of selective image cryptosystem, the data need to minimize before transmission over the communication channel. Among the various compression tools, SVD is an effective tool for image compression. When an image is transformed using SVD, the data of the image take a form in which the first singular value has a great amount of the image information. With this, only a few singular values can be used to represent the image with little differences from the original. Figure 2-b shows the reconstructed image with consideration of first 128 eigenvalues and its corresponding 128 eigenvectors from each orthogonal matrices and the computed PSNR value with respect to the original image is around 38.01 dB. Since, all the coefficients are real valued so in general for their efficient storage purpose, those coefficients are quantized and stored as eight bits integer form. Although this quantization process causes some distortion in reconstructed image but it preserves satisfactory visual quality with good PSNR value 30.15 dB as shown in Figure 2-c.



a) Original Lena Image. b) Reconstructed Image from truncated SVD . c) Reconstructed Image from quantized SVD.

Figure 2.SVD transformation of image.

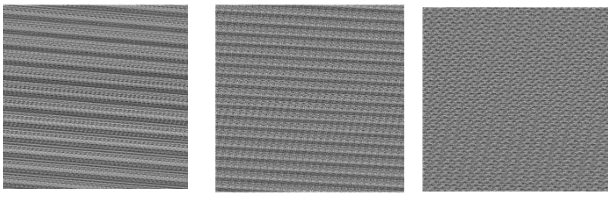
2.3. Arnold Cat Map (ACM)

In various image cryptosystems, confusion methods are applied prior to diffusion in order to achieve high level of security. One of these confusion methods, ACM has applied in most of the cryptosystem. ACM can confuse any 2-dimensional matrix directly whereas a gray scale image intensity is stored as a form of 2-dimensional array. So ACM is usually used for confusion of image data directly. In theoretically, ACM shifts the positions of the pixels of an image instead of changing their values. ACM for a matrix of size $N \times N$ is expressed as follows:

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = A \begin{bmatrix} x \\ y \end{bmatrix} \mathrm{mod}(N) \qquad (2)$$

Where $A = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix}, (x, y) \in [1, N]$ and det(A)=1,

Therefore making it area preserving, which will keep the size of the image the same throughout the iterations; (x, y) and (x', y') represent the position vector of image pixel shifted before and after respectively. Figure 3 shows the ACM confused images obtained from the original Lena image. Although the images shown in Figure 3 imply that the randomness has been increased along with a number of rounds of ACM increases, but the ACM holds the periodicity property. As per the periodicity property, the original matrix can be reappeared after applying ACM up to a particular number of rounds. That number of rounds is known as the periodicity value and this value depends on the dimension of the matrix. Table 1 shows how the periodicity values have changed with respect to image size.



a) After 1 Round of ACM. b) After 4 Rounds of ACM. c) After 64 Rounds of ACM.

Figure 3. Lena Image.

Table 1. Periodicity of Arnold transform (T) versus different dimension of matrix (N×N).

N	2	3	4	5	6	7	8	9	10
T	3	4	3	10	12	8	6	12	30
N	32	64	128	256	512	1024	2048	4096	8192
T	24	48	96	192	384	768	1536	3072	6144
N	33	65	100	257	513	1025	2049	4097	8193
T	20	70	150	258	1432	100	684	360	780

The above 2D Cat map Equation (2) can be generalized by introducing two control parameters, *p* and *q*, as follows:

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = A \begin{bmatrix} x \\ y \end{bmatrix} \mathrm{mod}(N) \qquad (3)$$

where $A = \begin{bmatrix} 1 & p \\ q & 1+pq \end{bmatrix}$ and *p, q* are positive integers.The generalized ACM provides three keys, the two parameters *p, q* and the number of iterations, n to encode the image. So in our work, the ACM parameters *(p,q,n)* are selected from a secret parameter. This secret parameter will be considered as a cryptographic key and prior to encryption-decryption process; both the sender and receiver will establish or share this key through some key agreement protocol. In decryption phase the inverse ACM is applied to get back the original positions of the image. Mathematically, the inverse ACM for a matrix of size N×N is expressed as follows:

$$\begin{bmatrix} x \\ y \end{bmatrix} = A^{-1} \begin{bmatrix} x' \\ y' \end{bmatrix} \mathrm{mod}(N) \qquad (4)$$

Where $A^{-1} = \begin{bmatrix} 1+pq & -p \\ -q & 1 \end{bmatrix}$

We can prove as follows:

Proof:

Since $A = \begin{bmatrix} 1 & p \\ q & 1+pq \end{bmatrix} \times \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} x+py \\ qx+pqy+y \end{bmatrix}$

Hence $\begin{bmatrix} x' \\ y' \end{bmatrix} = A \begin{bmatrix} x \\ y \end{bmatrix} \mathrm{mod}(N)$ can be rewritten as

$\begin{bmatrix} x \\ y \end{bmatrix} = A^{-1} \begin{bmatrix} x' \\ y' \end{bmatrix} \mathrm{mod}(N)$

Suppose $\begin{cases} x' = x + py - a_1 N \\ y' = qx + pqy + y - bN \end{cases}$

Now $A^{-1} \begin{bmatrix} x' \\ y' \end{bmatrix} \mathrm{mod}(N) = \begin{bmatrix} pq+1 & -p \\ -q & 1 \end{bmatrix} \begin{bmatrix} x+py-aN \\ qx+pqy+y-bN \end{bmatrix} \mathrm{mod}(N)$

$= \begin{bmatrix} x+(Pb-a(pq+1))N \\ y+(qa-b)N \end{bmatrix} \mathrm{mod}(N)$

Therefore $A^{-1} \begin{bmatrix} x' \\ y' \end{bmatrix} \mathrm{mod}(N) = \begin{bmatrix} x \\ y \end{bmatrix}$

3. Proposed Image Cryptosystem

As illustrated in the previous section, the confusion is done on the image data followed by diffusion and several numbers of overall rounds is taken to achieve the satisfactory level of security. The proposed cryptosystem follows the classical mechanism with some motivating factors to design a selective image encryption. The methodology used in this work provides a better solution for secure and efficient transmission of confidential message over the limited bandwidth communication channel. The detailed methodology is discussed below.

3.1. Encryption Procedure

Image data have strong correlations among adjacent pixels forming intelligible information. To encrypt the image, this intelligible information needs to be reduced by decreasing the correlation between the pixels and hence the perceptual information. The proposed selective encryption technique does this by scrambling the image first and then changing the pixel values. Figure 4 depicts the schematic diagram of the proposed encryption scheme. The complete encryption process consists of the following steps.

Algorithm: Image_Encryption

Input: A secret image A of size M×N and a binary key of length L

Output: Encrypted U_{ui}'', V_{ui}' *and associated unencrypted parameters like* S_T, $Min(U_T)$, $Min(V_T)$, $Max(U_T)$ *and* $Max(V_T)$

Begin

Step 1: Apply SVD on the secret image as given in Equation (1), $A=USV^T$ *where U and V are orthogonal matrix and S is diagonal matrix.*

Step 2: Select the number of eigenvalues i.e. S_T *from S matrix. Based on* S_T *truncate U and V matrices into* U_T *and* V_T *respectively in such way that each truncated matrix may be reshaped into a square matrix.*

Step 3: Convert U_T *and* V_T *matrices into* U_{ui} *and* V_{ui} *as an 8-bits unsigned integer matrix form.*

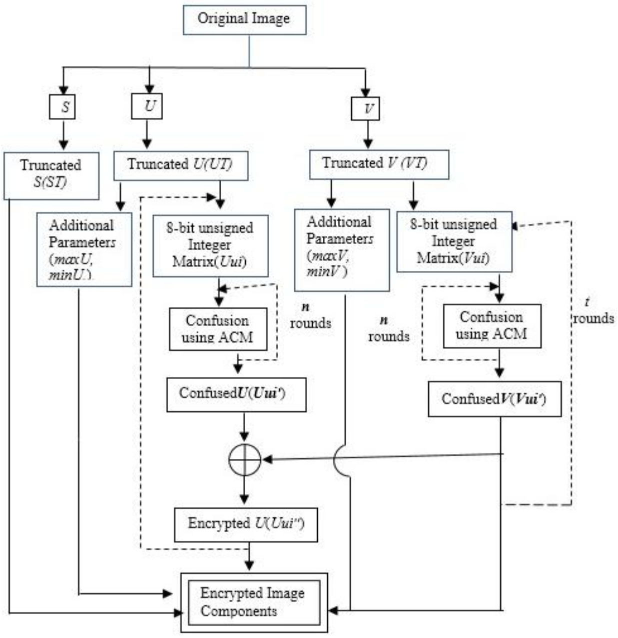


Figure 4. Block diagram of the proposed encryption process.

The U_{ui} and V_{ui} are derived as follow:

$$U_{ui} = \left\lfloor \frac{U_T - Min(U_T)}{Max(U_T) - Min(U_T)} \times 255 \right\rfloor \quad (5)$$

$$V_{ui} = \left\lfloor \frac{V_T - Min(V_T)}{Max(V_T) - Min(V_T)} \times 255 \right\rfloor \quad (6)$$

Where $Min(\bullet)$ *and* $Max(\bullet)$ *denote the derivation of minimum and maximum value respectively.*

Step 4: Create $(6t+1)$ *numbers of sub-keys from the binary key of length L where t is the number of overall rounds in the encryption process. Each sub*-keys, K_i *should satisfy* $K \in \left[1, \frac{T}{2}\right]$ *where T is the periodicity of ACM.*

Step 5: Scramble U_{ui} *and* V_{ui} *matrices into* U_{ui}' *and* V_{ui}' *matrices, respectively, by employing ACM as given in Equation 3, where p, q are the ACM parameters and n is the number of permutation rounds. For each encryption round different sub-keys are used as p, q and n.*

Step 6: The confused U segment (i.e., U_{ui}' *) is diffused with the confused V segment (i.e.* V_{ui}'*) using XOR operation:* $U_{ui}'' = U_{ui}' \oplus V_{ui}'$

Step 7: Repeat Step 5 to Step 6 for t times.

End

3.2. Decryption Procedure

The stressed motive of the decryption process is to obtain the approximate image from the encrypted compress image as perfectly as possible. Owing the value of ACM parameters (*p*,*q*,*n*) and number of iterations(*t*) along with encrypted image at the receiver end, decryption is performed perfectly. Figure 5 shows the proposed decryption process. The algorithmic steps of the decryption process are summarized as follows.

Algorithm: Image_Decryption

Input: Encrypted U_{ui}'', V_{ui}' *and associated unencrypted parameters like* S_T, $Min(U_T)$, $Min(V_T)$, $Max(U_T)$, $Max(V_T)$ *and a binary key of length L*

Output: A reconstructed approximate image $\tilde{A}$ *of* size $M \times N$

Begin

Step 1: Produce $(6t+1)$ *number of sub-keys from the binary key of length L where t is the number of overall rounds in encryption process. Each sub-keys,* K_i *should satisfy* $K \in \left[1, \frac{T}{2}\right]$, *where T is the periodicity of ACM.*

Step 2: Perform Inverse diffusion operation to obtain $U_{ui}' = U_{ui}'' \oplus V_{ui}'$

Step 3: Perform Inverse confusion operation on U_{ui}' *and* V_{ui}' *using Inverse ACM (Eq.4) where appropriate sub-keys are used.*

Step 4: Repeat Step 2 to Step 3 for t times.

Step 5: Derive $\tilde{U}_{ui}$ *and* $\tilde{V}_{ui}$ *using the following Equation*

$$\tilde{U}_{ui}=\left[\frac{U'_{ui}}{255}\times\left\{Max\left(U_T\right)-Min\left(U_T\right)\right\}\right]+Min\left(U_T\right) \tag{7}$$

$$\tilde{V}_{ui}=\left[\frac{V'_{ui}}{255}\times Max\left(V_T\right)-Min\left(V_T\right)\right]+Min\left(V_T\right) \tag{8}$$

Step 6: The approximate original image is reconstructed by multiplying the segments.

$$\tilde{A}=\tilde{U}_{ui}S_T\tilde{V}_{ui}^{\ T}$$

End

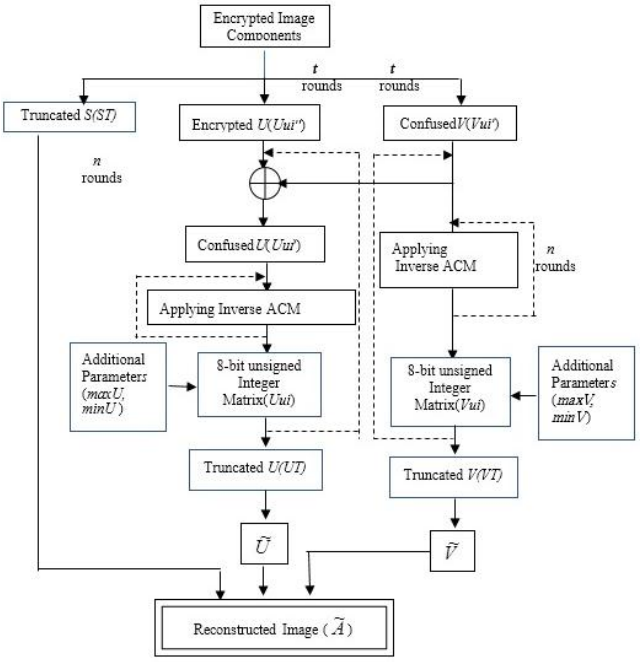

Encrypted Image Components
t rounds
t rounds
Truncated S(ST)
Encrypted U(Uui')
Confused V(Vui')
n rounds
Confused U(Uui')
Applying Inverse ACM
Applying Inverse ACM
n rounds
Additional Parameters (maxU, minU)
8-bit unsigned Integer Matrix(Uui)
8-bit unsigned Integer Matrix(Vui)
Additional Parameters (maxV, minV)
Truncated U(UT)
Truncated V(VT)
Ũ
Ṽ
Reconstructed Image (Ã)

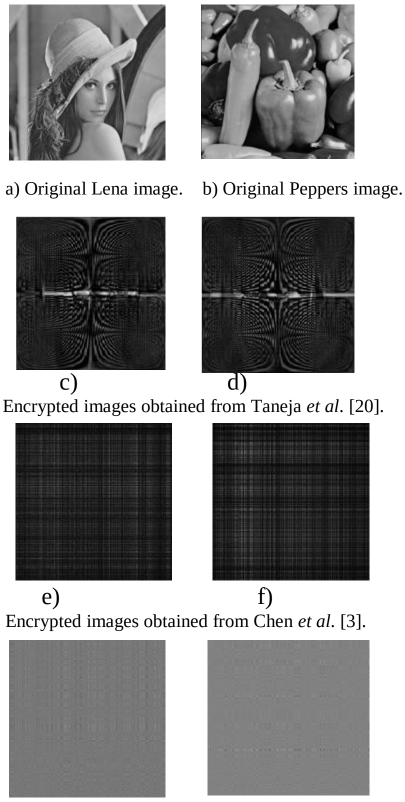
Figure 5. Block diagram of the proposed decryption process.

4. Experimental Results

The crucial measure of the quality of a cryptosystem is its capability to resist various types of cryptographic attacks. Some security analysis has been performed on the proposed scheme, including the most important ones like Peak Signal to Noise Ratio (PSNR), key space analysis, Number of Pixel Change Rate (NPCR) and statistical analysis (including histogram, correlation of adjacent pixels and entropy analysis), which has demonstrated the satisfactory security of the proposed scheme, as discussed in the following. The performance of the proposed selective image encryption technique is demonstrated using MATLAB platform. A number of experiments are performed on various grayscale images of size 512×512. In the proposed technique, three ACM parameters (*p*,*q* and *n*) and total encryption rounds (*t*) are used as keys. Although a single round of ACM operation on a particular matrix is not secure but the high level of security can be achieved when the generalized ACM with different set of ACM parameters will be deployed on same block matrix a number of times. The multi round generalized ACM operation build the encryption process more complex and attain the desire level of security.

4.1. Perceptual Security and Peak Signal to Noise Ratio (PSNR)

Subjective evaluation of the encrypted image is performed to assess the amount of information leakage. Figure 6 shows the encrypted output for the four test images. It is observed that the obtained images are completely unintelligible, and do not reveal any information about the original image.


a) Original Lena image. b) Original Peppers image.

c) d)

Encrypted images obtained from Taneja *et al*. [20].

e) f)

Encrypted images obtained from Chen *et al*. [3].

g) h)

Encrypted images obtained from the proposed scheme.

Figure 6. Encrypted output for test images.

Also the degradation introduced is objectively evaluated using PSNR as follows:

$$PSNR=10\log_{10}\frac{255^2}{MSE} \tag{9}$$

Where $MSE=\left(\sum_{i-1}^{W}\sum_{j-1}^{H}x_{i,j}-\tilde{x}_{i,j}\right)/\left(W\times H\right)$,

$x_{i,j}$ and $\tilde{x}_{i,j}$ denotes the original and encrypted pixel, respectively, and the images are of size *W*×*H*.

Table 2 shows the PSNR value of two test images supplied to the proposed technique. Lower PSNR values indicate better performance. The resultant values are slightly higher than the values obtained in Taneja *et al*. [20] and Chen *et al*. [3] but less than 15db which indicates good performance for perceptual security.

Table 2. Calculated PSNR values of the proposed techniqe and references.

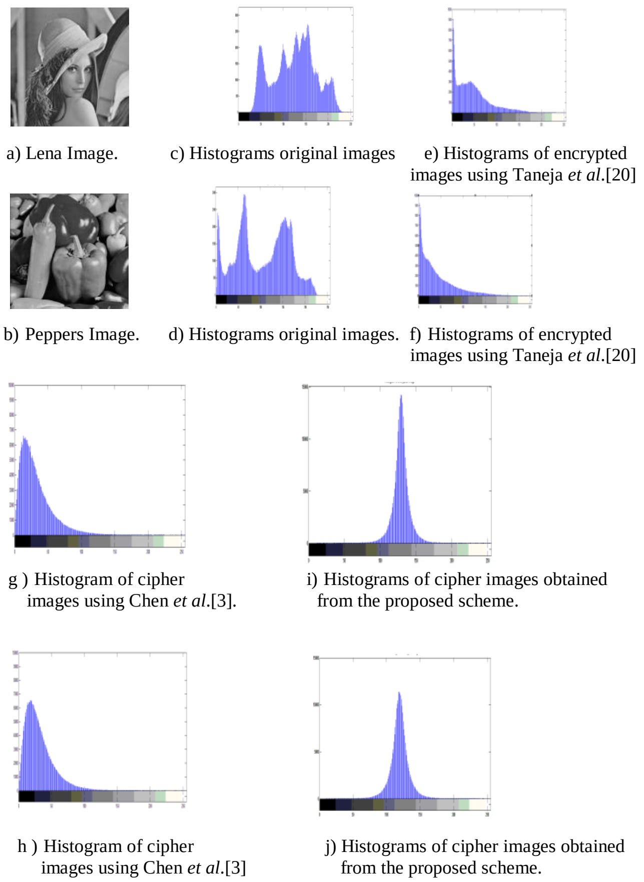
Image	Taneja *et al.* [[20]	Chen *et al.* [3]	Proposed
Lena	8.0350	7.5426	**13.9499**
Peppers	8.7258	8.554	**11.6215**

4.2. Statistical Analysis

An ideal cipher should be resistant to any statistical. To prove the robustness of the proposed encryption scheme, we have performed statistical analysis by calculating the histogram and the correlation of two adjacent pixels in the ciphered image.

4.2.1. Histogram Analysis

It is well known that an ideal cipher-image should have a uniform histogram to prevent the opponent from extracting any meaningful information from the fluctuating histograms of the cipher-image. The histogram for the original and the encrypted image is indicated in Figure 7. It is clear that the histograms of the cipher image are fairly uniform and significantly different from the respective histograms of the plain image and hence the proposed image cipher produces cipher images having uniform pixel distribution over the all possible intensity values. It is clear that the histograms of the cipher image are fairly uniform and significantly different from the respective histograms of the plain image and hence the proposed image cipher produces cipher images having uniform pixel distribution over the all possible intensity values.



a) Lena Image.

c) Histograms original images

e) Histograms of encrypted images using Taneja *et al.*[20]

b) Peppers Image.

d) Histograms original images.

f) Histograms of encrypted images using Taneja *et al.*[20]

g) Histogram of cipher images using Chen *et al.*[3].

i) Histograms of cipher images obtained from the proposed scheme.

h) Histogram of cipher images using Chen *et al.*[3]

j) Histograms of cipher images obtained from the proposed scheme.

Figure 7. Original images and their histograms.

4.2.2. Information Entropy Analysis

Information entropy is an important feature for measuring of randomness. It quantifies the amount of information contained in the data, usually in bits or bits/symbol. This is defined as follows:

$$H(m) = \sum_{i=0}^{2^{N-1}} P(m_i)\log_2 \frac{1}{P(m_i)} \qquad (10)$$

Where *m* be the information source and *P*(m_i) represents the probability of the symbol m_i. If each symbol has an equal probability, then the maximum entropy will be 8 for a gray scale with 256 intensity level. Table3 shows the entropy values of the two encrypted images. As we find that the entropy values of the encrypted images obtained from the proposed scheme are closer to 8 and better than the Taneja *et al.* [20] and Chen *et al.* [3]. It means that the information in the proposed algorithm is better randomized and less possible to reveal the information

Table 3. Calculated Entropy values for the proposed technique and references.

Image	Taneja *et al.*[20]	Chen *et al.* [3]	Proposed
Lena	6.8497	6.2808	**7.6503**
Peppers	6.7590	6.2033	**7.6307**

4.2.3. Correlation Analysis

For an ordinary image having definite visual content, each pixel is highly correlated with its adjacent pixels either in horizontal, vertical or diagonal direction. However, an efficient image cryptosystem should produce the cipher image with sufficiently low correlation in the adjacent pixels. We select pairs of two adjacent pixels horizontally, vertically and diagonally followed by correlation coefficient computation as follows:

$$r_{x,y} = \frac{\mathrm{cov}(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \qquad (11)$$

Where

$$\mathrm{cov}(x,y) = \frac{1}{N}\sum_{i=1}^{N}\left(x_i - \frac{1}{N}\sum_{j=1}^{N}x_j\right)\left(y_i - \frac{1}{N}\sum_{j=1}^{N}y_j\right)$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}\left(x_i - \frac{1}{N}\sum_{j=1}^{N}x_j\right)^2,$$

$$D(y) = \frac{1}{N}\sum_{i=1}^{N}\left(y_i - \frac{1}{N}\sum_{j=1}^{N}y_j\right)^2$$

Table 4. Correlation coefficients of two adjacent pixels in plain-image and cipher image.

Image	Scan Direction	Taneja *et al.*[20]	Chen *et al.*[3]	Proposed
Lena	Horizontal	0.6520	0.4659	**-0.0472**
	Vertical	-0.4030	0.5102	**-0.0076**
	Diagonal	-0.4250	0.1640	**8.6106e-004**
Peppers	Horizontal	0.6011	0.3723	**-0.0126**
	Vertical	-0.3533	0.3972	**-0.0082**
	Diagonal	-0.3393	0.0702	**4.2003e-004**

Table 4 shows the result of correlation coefficients of the original image and encrypted image in each direction. The result indicates that the correlation of two adjacent pixels of the encrypted image is very small. Also, it shows better result as compared to Taneja *et al*. [20] and Chen *et al*. [3], which indicate that the encryption effect is rather good.

4.3. Differential attack Analysis

In order to resist the differential attack, a minor alteration of the plain-image should cause a substantial change in the cipher-image. To test the influence of a one pixel change in the cipher-image, one of the common quantitative measures is the Number of Pixels Change Rate (NPCR). The NPCR is defined as follows:

$$NPCR = \frac{\sum_{i,j} D(i,j)}{W \times H} \times 100\% \qquad (12)$$

Where $D(i,j) = \begin{cases} 0 & if\ C_1(i,j) = C_2(i,j) \\ 1 & f\ C_1(i,j) \neq C_2(i,j) \end{cases}$

and C_1, C_2 are two cipher images corresponding to two plain images with only one pixel difference. From the Table 5, it has observed that after altering one pixel in the plain image it gives a completely different encrypted image which indicates a good resistance to differential attack

Table 5 . Calculated NPCR values of the proposed techniqe and references.

Image	Taneja *et al*.[20]	Chen *et al*.[3]	Proposed
Lena	89.1124	95.9793	**96.8578**
Peppers	91.0873	97.4842	**94.2570**

4.4. Key Space Analysis

In security analysis, the key space represents all possible number of keys that may be used in the encryption procedure. The brute force attacks of any cryptosystem become infeasible when the key space is reasonably large enough. In the proposed scheme, for enciphering the U and V Components, we have used two set of ACM parameters, i.e. p, q and n at each round. We have also carried out this enciphering mechanism overall t times. Hence, in the proposed scheme, the total key space is $2^{2(p+q+n)t}$ .If we consider the typical value of of p, q, n are 8 bits each and the minimum overall round, t is 4, , then the total key space will be 2^{192}which is larger than 2^{100}. In Xu *et al*.[22] suggested that the key space should be at least 2^{100} for ensuring the sufficient security level against brute-force attacks. The proposed cryptosystem has fulfilled this requirement even for the minimum number of overall round.

5. Conclusions

This paper presents a selective image encryption technique based on SVD and ACM. SVD is incorporated to compress the image and further it has utilized to select the significant part of the compressed image which can enhance the reduction of computational overhead and efficient transmission in the bandwidth limited channel. The confusion-diffusion architecture has followed for the encryption process. ACM has employed to confuse significant part of the image following diffusion. In diffusion process, the simple XOR operation has incorporated in the significant part. Various security analyses are given to demonstrate that the proposed scheme is the efficient one for secure transmission of the image in the open communication channel. The scheme is suitable for any kind of gray scale image which can be further extended for color images by applying proposed scheme on each color components. The proposed scheme is a good candidate for real-time secure image communication applications.

References

[1] Bahrami S. and Naderi M.,“ Encryption of Multimedia Content in Partial Encryption Scheme of DCT Transform Coefficients using a Lightweight Stream Algorithm,” *Optik-International Journal for Light and Electron Optics*, vol. 124, no. 18, pp. 3693-3700, 2013.

[2] Bhatnagar G. and Wu Q., “Selective Image Encryption based on Pixels of Interest and Singular Value Decomposition,” *Digital Signal Processing*, vol. 22, no. 4, pp. 648-663, 2012.

[3] Chen L., Zhao D., and Ge F., “Image Encryption based on Singular Value Decomposition and Arnold Transform in Fractional Domain,” *Optics Communications*, vol. 291, pp. 98-103, 2013.

[4] Chen J., Zhu Z., and Yu H., “ A Fast Chaos-based Symmetric Image Cryptosystem with an Improved Diffusion Scheme,” *Optik-International Journal for Light and Electron Optics*, vol. 125, no. 11, pp. 2472-2478, 2014.

[5] Chen W., Quan C., and Tay C., “Optical Color Image Encryption based on Arnold Transform and Interference Method,” *Optics Communications*, vol. 282, no. 18, pp. 3680-3685, 2009.

[6] Gupta M. and Garg A., “Analysis Of Image Compression Algorithm using DCT,” *International Journal of Engineering Research and Applications*, vol. 2, no. 1, pp. 515-521, 2012.

[7] Khashan O. and Zin A., “An Efficient Adaptive of Transparent Spatial Digital Image Encryption” *Procedia Technology*, vol. 11, pp. 288-297, 2013.

[8] Kong D. and Shen X., “Multiple-image Encryption based on Optical Wavelet Transform and Multichannel Fractional Fourier Transform,” *Optics and Laser Technology*, vol. 57, pp. 343-349, 2014.

[9] Kumar A. and Ghose M., “Extended Substitution-diffusion based Image Cipher using Chaotic Standard Map,” *Communications in Nonlinear Science and Numerical Simulation*, vol. 16, no. 1, pp. 372-382, 2011.

[10] Lian S., *Multimedia Content Encryption: Techniques and Applications*, Taylor and Francis Group, 2009.

[11] Lin K., “Hybrid Encoding Method by Assembling the Magic-matrix Scrambling Method and the Binary Encoding Method in Image Hiding,” *Optics Communications*, vol. 284, no. 7, pp. 1778-1784, 2011.

[12] Liu Y., Lin J., Fan J., and Zhou N., “Image Encryption Based on Cat Map and Fractional Fourier Transform,” *Journal of Computational Information Systems*, vol. 8, no. 18, pp. 7485-7492, 2012.

[13] Lookbaugh T., “Selective Encryption, Information Theory and Compression,” *in Proceedings of Asilomar Conference on Signals, Systems and Computers*, Pacific Grove, pp. 373-376, 2004.

[14] Maniccam S. and Bourbakis N., “Lossless Image Compression and Encryption using SCAN,” *Pattern Recognition*, vol. 34, no. 6, pp. 1229-1245, 2001.

[15] Naik K. and Pal A., “An Image Cryptosystem based on Diffusion of Significant Bit-planes of Scrambled Image with Generated Binary Key Matrices,” *International Conference on Computational Intelligence and Computing Research*, Enathi, pp. 1-4, 2013.

[16] Sadek R., “SVD Based Image Processing Applications: State of The Art, Contributions and Research Challenges,” *International Journal of Advanced Computer Science and Applications*, vol. 3, no. 7, pp. 26-34, 2012.

[17] Samson C. and Sastry V., “A Novel Image Encryption Supported by Compression using Multilevel Wavelet Transform,” *International Journal of Advanced Computer Science and Applications*, vol. 3, no. 9, pp. 178-183, 2012.

[18] Schneier B., *Cryptography: Theory and Practice*, CRC Press, 1995.

[19] Li G. and Wang Y., “A Privacy-Preserving Classification Method Based on Singular Value Decomposition,” *The International Arab Journal of Information Technology*, vol. 9, no. 6, pp. 529-534, 2012.

[20] Taneja N., Raman B., and Gupta I., “Selective Image Encryption in Fractional Wavelet Domain,” *International Journal of Electronics and Communications*, vol. 65, no. 4, pp. 338-344, 2011.

[21] Uhl A. and Pommer A., *Image and Video Encryption: from Digital Rights Management to Secured Personal Communication*, Springer Science and Business Media, 2005.

[22] Xu S., Chen X., Zhang R., Yang Y., and Guo Y., “An Improved Chaotic Cryptosystem based on Circular bit Shift and XOR Operations,” *Physics Letters A*, vol. 376, no. 10-11, pp. 1003-1010, 2012.

[23] Zhang Y. and Xiao D., “An Image Encryption Scheme based on Rotation Matrix Bit-level Permutation and Block Diffusion,” *Communications in Nonlinear Science and Numerical Simulation*, vol. 19, no. 1, pp. 74-82, 2014.

[24] Zhou Y., Bao L., and Chen C., “A New 1D Chaotic System for Image Encryption,” *Signal Processing*, vol. 97, pp. 172-182, 2014.

[25] Zhou Y., Panetta K., Agaian S., and Chen C., “(n; k; p)-Gray Code for Image Systems,” *IEEE Transactions on Systems, Man and Cybernetics Part b: Cybernetics*, vol. 43, no. 2, pp. 515-529, 2013.

Kshiramani Naik is currently working as a full time Research Scholar in the Dept. of Computer Science & Engineering, Indian school of Mines, Dhanbad, India. She received her BE in CSE and M.Tech in CSE from BPUT Rourkela and NIT Rourkela respectively. Her research interest includes Image Cryptosystem, Steganography and Watermarking.

Arup Kumar Pal is presently working as an Assistant Professor in the Dept. of Computer Science and Engineering, Indian School of Mines, Dhanbad, India. He did his Ph.D in Computer Science and Engineering from Indian School of Mines, Dhanbad in 2011. His main research interest includes Vector Quantization, Image Compression, Image Cryptosystem, Steganography, Watermarking and CBIR.

Rohit Agarwal is currently working as an Assistant Professor at the Dept. of Computer Science & Engineering, JSS Academy of Technical Education Noida (U.P.), India. He has completed his M.Tech degree in Computer Application from the Indian School of Mines Dhanbad (India) in 2013. His research interests include Digital Image Processing and Numerical Linear Algebra.