# Proposed Method to Encrypt Images to Mobile Device Based on the Principles of Shannon

**Dr. Hanna M .A .Salman**
Department of Computer Science, University of Technology/Baghdad
Email: salman.hanaa@yahoo.com
**Anwar Abbas Hattab**
Email: anwarabbas76@gmail.com

**Received on:15/3/2016 & Accepted on:24/11/2016**

## ABSTRACT

In the proposed research, it has been proposed image encryption method in the mobile device based on the principles of Shannon (diffusion and confusion). Where: a large group of keys is used. The process of entering the keys by the user is a very difficult In the proposed method; all the keys are extracted from the mathematical image properties, by a process of summation operation and the value of the mean. Image processing passes in to two phases, the first phase by using the output of the process of summation as a key to achieve the diffusion. In the second phase, the value of the mean is used as a seed to LFSR (Linear feedback register) to generate akey equal to the block of the image. Then process of the x or-operation (XOR) between the key and the block of image should be treated the output of these two phases is an image with the same of the original image size. Then by applying calculated time of encryption and decrypted are found the proposed method is simple, fast, and sensitive to the key. The suggested method meets the performance analysis examinations such as histogram, correlation, power spectrum, NPCR, UACI, Entropy and acceptable encryption speed; and it is resistant to statistical, brute force, and differential attacks.

**Keyword:** Image cipher, Permutation operation, LFSR.

## INTRODUCTION

Cryptography is one of the technical ways to supply security to input being conveyed on information and communications schemes Cryptography is particularly valuable in the cases of financial and private information regardless of the reality that the information is being transferred over a channel or is saved on a storage device [1]. It supplies a robust means of confirmative the legitimacy of information and recognizing the culprit, if the confidentiality and integrity of the information are profaned because of the progression of electronic trade cryptographic procedures are radically crucial to the progression and use of protection data methods and communications networks. On the other side, in all these situations there is an enlarging requirement for defense data to the protection economic advantages to avoid swindler and to certify confidentiality [2]. Dissimilar text, image data have their special characteristics such as majority of capacity, bigger redundancy, and extra associations between pixels, not to reference that they generally are huge which together execute conventional encryption approaches difficult to carry out and slow to operation. As a result, more conventional such as DES IDEA, Blowfish, AES, are



https://doi.org/10.30684/etj.34.6B.11
2412-0758/University of Technology-Iraq, Baghdad, Iraq

thereby unacceptable for functional digital image encryption due to the drawback of low-level efficiency while Digital image communication over a mobile network needs are liable, fast and powerful secure system. The needs to accomplish the security needs of digital images have steered to the advancement of effective image encryption algorithms.[3, 4]

In this paper, we propose a new cipher method deal with energy spending for encryption of the large-volume visual data. So we are transactions with simple and less complication method for cipher image. In this method executed, permutation operation and XOR operation not need any keys, although using a set of keys, which deduce from summation value and mean value, it method simple, fast and less complexity. H. Shuihuain[5]formed an asymmetric encryption method based on the matrix change scheme which is greatly efficient to quickly decrypt and cipher images. Bibhudendra in [6] displayed an Advanced Hill encoding method to encrypt images which applies an involuntary matrix. The complication would be decreased by preventing the process of result reverse of the matrix through decryption. Each image is connections between the bits, pixels and blocks. This perceivable information could be decreased by decreasing the connection between the bits, block and pixels by using certain combinational shift methods [7].

The rest of this paper is arranged as follows: Section 2 explains proposed image encryption method by using a combination of permutation operation and XOR operation. In Section 3 described permutation, XOR operation and key generation. In section 4 explain performance analysis. This paper is concluded present in Section 5.

**Proposed Method**

In this paper, we proposed new method for encryption image of mobile device. In this method, we don't need any key from the user for any operation, but each key deduces from mathematic properties for image by using summation operation and mean value. In our method, we divide image to blocks, which has size (256 bit) and performs set operations (permutation and linear mixing (xor)) show in flowchart in fig(1), and each operation described in detail later.

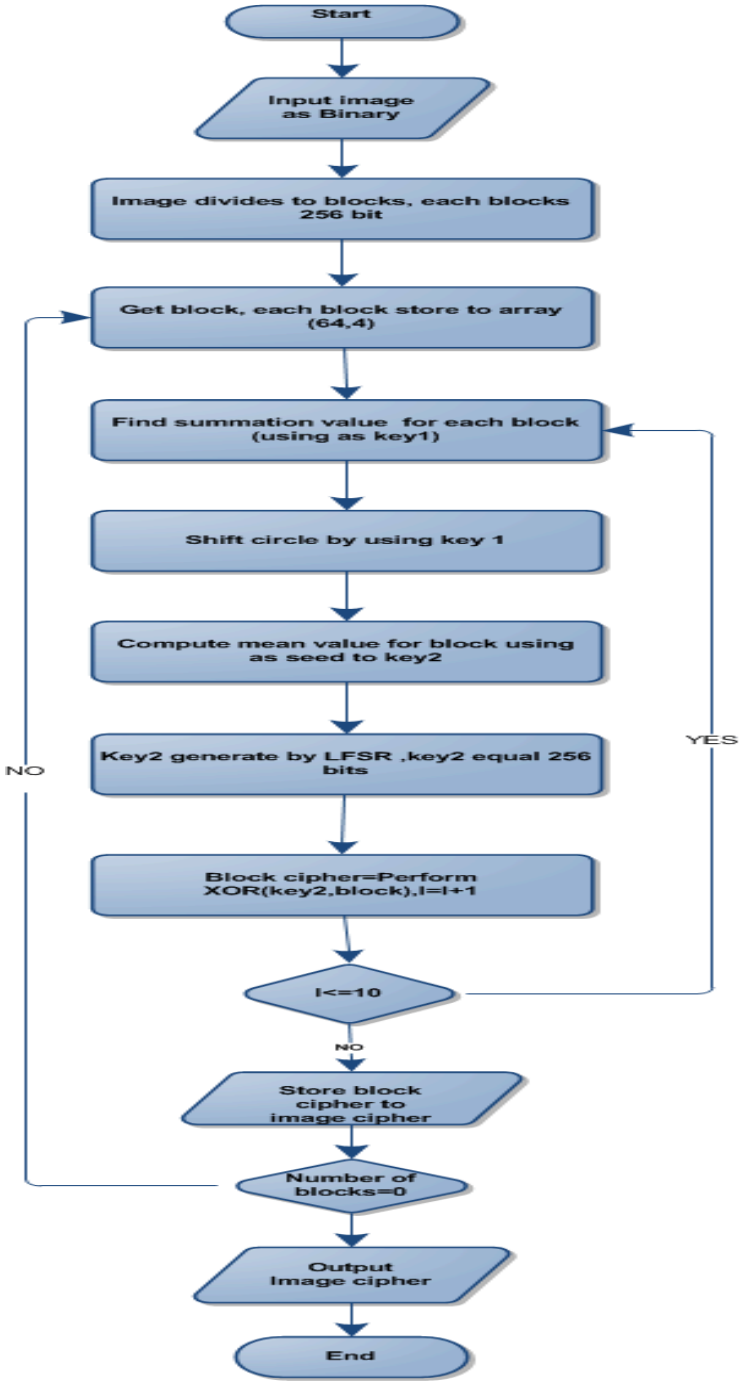


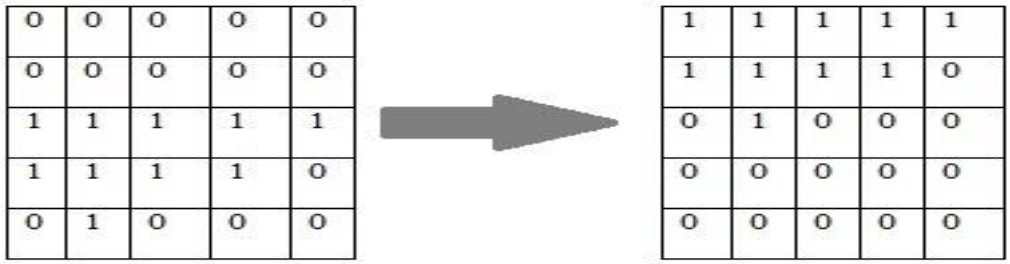

**Figure (1) Flowchart proposed method**

**Permutation Operation**

In our method, we use block (256 bit) which store to array has size (64, 4) and perform summation operation for each column, determine large summation value which is used as a key for

shift circle for each row and column. This operation makes diffusion in image. Figure (2) show example of our permutation operation on an array (5, 5), algorithm (1) described our permutation operation.

Example: let A =




SUM= 2, 3 2 2 1

A. Array (A), large sum is 3 B. After shift circle (3, 3)

**Figure (2) a. array (5, 5) with sum value b. array after shift circle (3, 3)**

**Algorithm (1) permutation operation**

1. Input image as binary.
2. Output image after permutation.
3. Image (x) divides to number of blocks, each block has 256 bits, I=1.
4. While I <= number of blocks
5. Each block store to array p= (64, 4).
6. Perform summation operation for each column in the array P.
7. Let K largest summation, which is used as a key of permutation operation.
8. If K=0 or K=64, then go to step 10.
9. Shift circle each row and column at same time, shift by using (K) as the key.
10. I=I+1.
11. End while.
12. End.

**Linear mixing**

Linear mixing function uses 256 bits as input and produces 256 bit output. The input block (256 bits) are arranged as vector 256 bit which applies x or operation between input vector and key. Key is generated from algorithm (2) which produce block (key) as vector 256 bit, explain in figure (3) linear mixing.

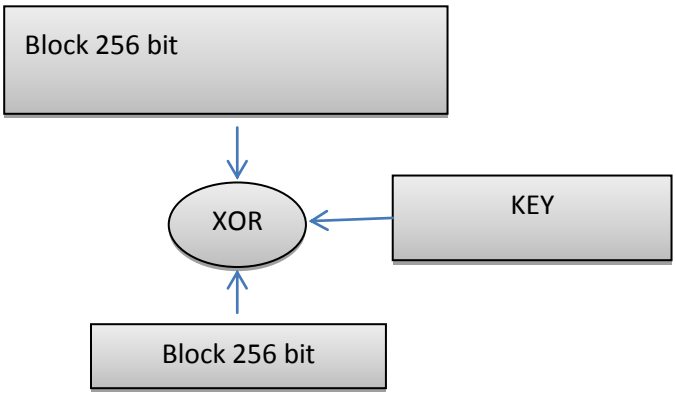



**Figure (3) XOR operation**

**Key generation method**

In suggested algorithm, multi keys are required to apply in encryption and decryption. In permutation operation which uses maximum summation value for each part as the key, the total key in 10 round equal 10 keys, the same key is used in inverse permutation. The key which is used in X-OR function is 256 bits key to increase confusion; the total number for size of keys of all rounds is 2560bits.in our method used new method to generate key, therefore not need any key to enter by user. Those keys generation method will be explained below: the machine consists of two parts: LFSR 1 has 31 bits and LFSR2 has 19 bit show in figure(4) .We must find mean value for each block ( mean equal summation all elements of block and divide summation value to size of block(256)), mean value if fraction between[0,1] and pull out the first four digits of fraction(mean value),first two digits are used as a seed to LFSR1 and another two digits are used as a seed to LFSR2, register 1 and register 2 are used to produce key which has length 256 bits . LFSR1 has polynomial ($x^3+x^{31}$) andLFSR2 has polynomial ($x^1+ x^2+x^5 +x^{19}$).


**Figure (4).LFSR (Register 32bit and Register 19 bit)**

**Algorithm (2) Key Generation**

**Input: block of data.**

1. **Output: key**.
2. Find mean value, it is used for each block, as the fraction number have four digits.
3. Two digits are used as a seed to the LFSR1, and another two digits are used as a seed to LFSR2.
4. While (I< = 256)
5. Get a bit (31) from LFSR1 and bit (19) from LFSR2 and perform XOR operation between them.

6. Perform XOR operation between bit (31) and bit (3) in the same register (result1) and perform XOR operation between bit (19, 5, 2) and bit (1) in the same register (result2).
7. Shift LFSR1 bits (1-13) and shift LFSR2 bits (1-19).
8. Results from step (5) store to LFSR1 in bit (1) and result (2) store to LFSR2 bit (1).
9. Result from step (4) is stored in array call key. I=I+1.
10. End while
11. End.

**Algorithm (3)XOR operation**
**Input: plain block, key.**

1. **Output: cipher block**.
2. While (I <= number of blocks)
3. Store each block(X) as the vector one dimension.
4. Find (S) as a result summation operation for all elements of the array (p).
5. Calculate mean value, divide S with size of block (256).
6. If S=0 **or** S=256, then mean =0.256.
7. Use the algorithm (2) to generate Key.
8. Perform XOR operation between Key and block(x).
9. I=I+1,
10. End while
11. End.

**Decryption Operation**

In decryption operation must perform XOR operation by using seed to generate a key as in cipher algorithm, after that, inverse permutation must perform by using summation value of block as a key to this operation, these operations perform 10 rounds to produce the original block or the original image. Decryption operation explained in figure (5) and inverse permutation algorithm (4) described below.

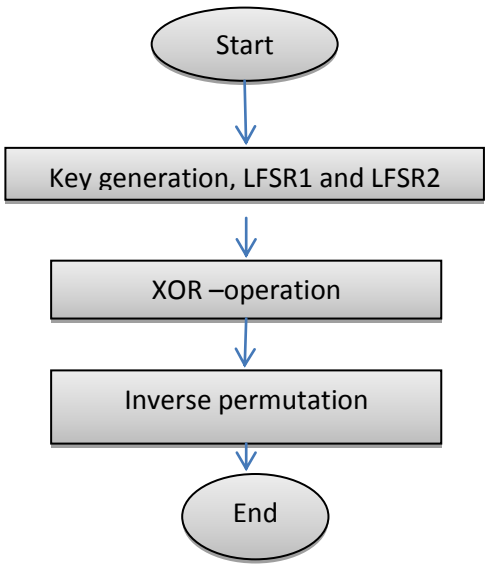



**Figure (5). Decryption operation**

**Algorithm (4) Inverse _permutation operation**

1. **Input: block of data.**
2. **Output: block of data**.
3. Image (x) divides to number of blocks, each block has 256 bits.
4. While (I ~= number of blocks)
5. Block store to the array p= (64, 4).
6. Perform summation operation for each column in array P.
7. Let K largest summation, which is used as a key of permutation operation.
8. If K=0 or K=64, then go to step 8.
9. Shift circle each row and column at same time, shift by using (-K,-K)asa key.
10. I=I+1.
11. End.

**Performance Analysis:**

**1. Key examination:**

The key space of our method is over than $2^{256}$ because the key space equal 2^50 for each block, if image has size 10 blocks. Therefore, this image has key space 2^ 500 bit or If image has 20 blocks, it has 2^1000bit respectively as well as the number of blocks are huge, the key's space of image will be increased respectively. Therefore, this method has strong against brute force attacked

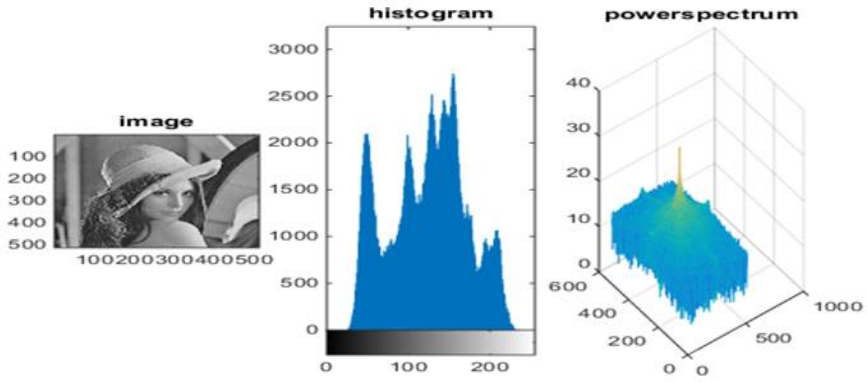
**2. Statistical Analysis:**

Image cipher scheme should be strong against any statistical attack. In order to prove the security of the proposed image encryption scheme, the following statistical tests are performed:

**Image Histogram & Power Spectral Density**

The image histogram explains the number of pixels in an image at various intensity values. Gray scale image use 8_bits for each pixel. The 2-D power spectrum appearances the power of image intensity, where x and y are coordinates couple of an image, m and n are the size of image; f(x, y) is the image value at the pixel (x, y). Fig (6) explains the histograms and 2D power spectrums of original images. The original image is Lena's image with 256x256 image sizes and Mandrill with 512x512 size of image. In figure (6) show the histogram and power spectrums with various value as specific form is not plane but histogram and power spectrums for encryption images are plane. These results guarantee that the image is secured. Eq (1) represent equation of power spectral F.

$$F = \sum_{x=0}^{m-1} 1 \sum_{y=0}^{n-1} f(x,y)\exp(-j(\pi/m)ux)\exp(-j(2\pi/n)vy \quad \text{---- (1)}$$




**a**

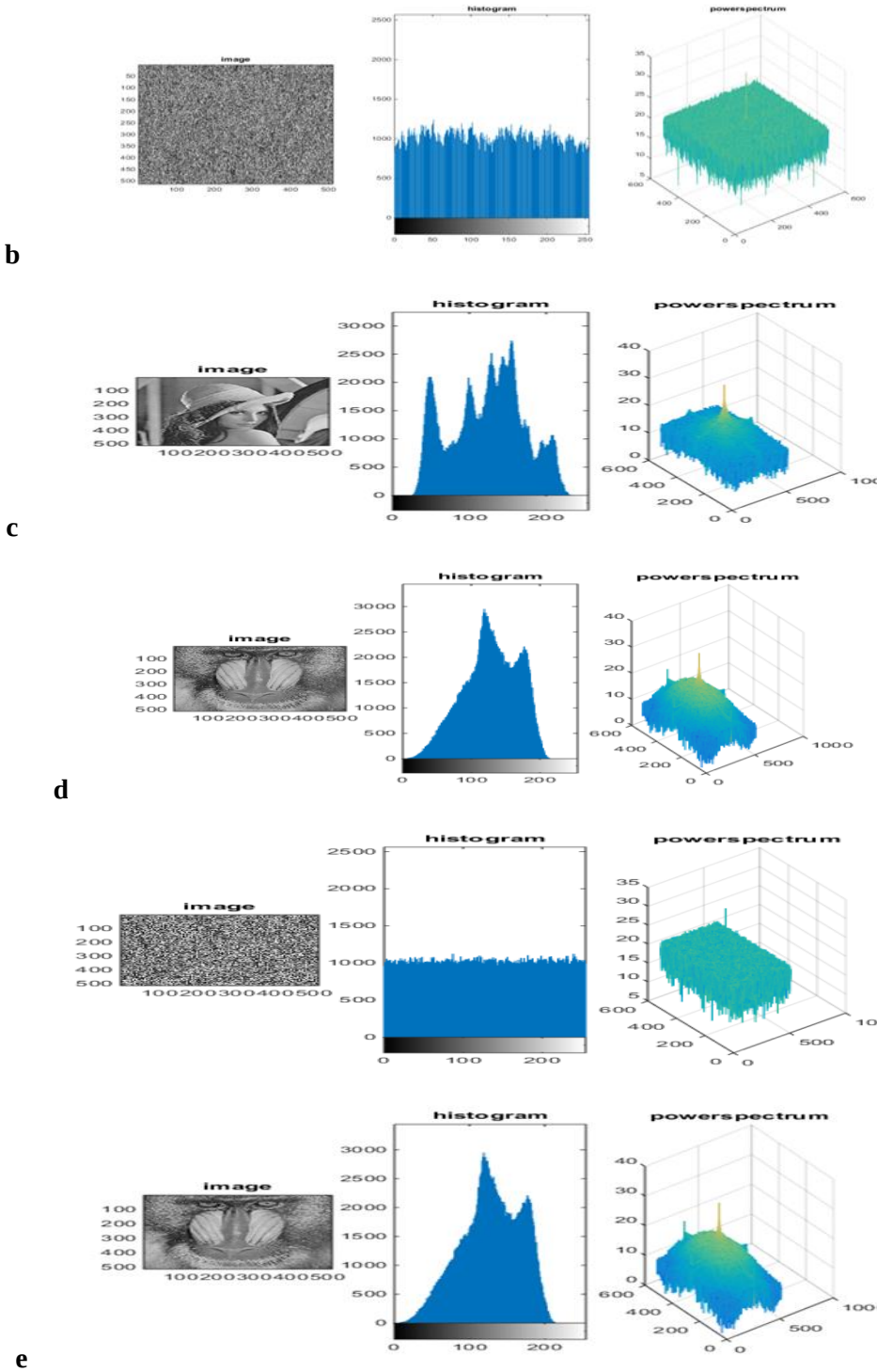



**Figure (6) a and d histogram and power spectrum of plain images ( Lena and Mandrill), in b ,d histogram and power spectrum of cipher images ( Lena and Mandrill), c and e histogram and power spectrum of images decryption ( Lena and Mandrill) with true key.**

**Correlation Coefficient examination**

We will study the correlation between image pairs in order to specify the key sensitivity and encryption performance which is use as scale of bonds between two pixels. The CV and correlation coefficient COR and x and y represent value of pixels. COR take value between [1,-1], if COR in rang (-1,0) that mean negative relation ,if COR take value between(0,1) that mean positive relation. Table (1) describes image correlation in encrypted and original images include diagonally, vertically and horizontally adjacent pixels. Correlation coefficient (COR) defines in eq (2) as:

CV= $1/n \sum_{i=0}^{n}(h\,i - E(h))(ki - E(k))$

COR=$\frac{cov(h,k)}{\sqrt{D(h)\sqrt{D(h)}}}$ ---- (2)

Function E (h) and E (k) are defined as:

E (h) =$\frac{1}{n}\sum_{i=1}^{n} hi$ and D (h) =$\frac{1}{n}\sum_{i=1}^{n}(hi - E(h))$^2

**Table (1).Correlation coefficients for original and cipher image.**

| Image | Correlation coefficients for original image(it=1) | | | Correlation coefficients for cipher Image(it=1) | | |
|---|---|---|---|---|---|---|
| | X-Horizontal | Y-Vertical | Diagonal | X-Horizontal | Y-Vertical | Diagonal |
| Mandrill | 0.9337 | 0.9123 | 0.8669 | 0.0015 | 0.0031 | 0.0011 |
| Lena | 0.9258 | 0.9593 | 0.9037 | 0.0107 | 0.0044 | -0.0043 |

**Differential Analysis**

Differential analysis use two familiar scales: **NPCR** and **UACI.** NPCR means the "Number of Pixels Change Rate" of encrypted image while one pixel of plain-image is changed. UACI which is the "Unified Average Changing Intensity" scales the average intensity of the differences between the basic and Encrypted image. Let h, h2, whose corresponding plain images have only one pixel difference. Table (2) show NPCR and UACI for Lena and Mandrill, and the **NPCR** of two images are defining in:

W, H represents width and high of image. And M (I, j) is defining as:

M (Imp) =$\begin{cases}1 & if\ h(i,j) \neq h2(i,j)\\ 0 & if\ h(i,j) = h2(i,j)\end{cases}$

**UACI** define as:

UACI=$\frac{1}{W*H}$ $\sum ij$ $\left(\frac{h(I,J)-h2(i-j)}{255}\right) * 100$ ---- (4)

**Table (2). NPCR and UACI for Mandrill and Lena**

| Lena | | | |
|---|---|---|---|
| | it=2 | it=3 | It=5 |
| NPCR | 99.6384 | 99.6170 | 99.6399 |
| UACI | 27.51 | 27.33 | 27.42 |
| Mandrill-image | | | |
| NPCR | 99.6140 | 99.6216 | 99.6346 |
| UACI | 38.68 | 39.00 | 38.78 |

**Image Entropy**

Image entropy denoted the degree of uncertainties in the image. Entropy (k) can be defined:

Entropy (k) =$\sum$p ($k_i$) log $\frac{1}{p(ki)}$ ---- (5)

$P(k_i)$ is present the emergence probability of $k_i$. If every symbol has an equal probability, i.e., m={k0,k1,k2,…k2 -$1^8$} and $P(k_i)=1/2^8$ (i=0,1,…255), then the entropy is H(k)=8 which corresponds to an perfect l value. The entropy of encrypted image close to the perfect value is expected. In Table (4) explain time encryption and decryption time we concluded that our method is a quick and simple way.

**Table (3) NPCR, UACI, Entropy for many iteration**

| Image | | It=1 | It=2 | It=3 | It=5 | It=7 | It=8 | It=10 | It=12 |
|---|---|---|---|---|---|---|---|---|---|
| *Lena* | NPCR | 99.5651 | 99.6384 | 99.6170 | 99.6399 | 99.5865 | 99.6475 | 99.5987 | 99.6140 |
| | UACI | 28.87 | 27.51 | 27.33 | 27.42 | 27.43 | 27.64 | 27.51 | 27.37 |
| | Entropy | 7.4429 | 7.9968 | 7.9974 | 7.9974 | 7.9971 | 7.9971 | 7.9972 | 7.9970 |
| Mandrill | NPCR | 99.5869 | 99.6140 | 99.6216 | 99.6346 | 99.6033 | 99.6334 | 99.6033 | 99.6056 |
| | UACI | 37.17 | 38.68 | 39.00 | 38.78 | 38.69 | 38.88 | 39.03 | 38.89 |
| | Entropy | 7.2925 | 7.9925 | 7.9992 | 7.9993 | 7.9992 | 7.9992 | 7.9993 | 7.9992 |

**Table (4) Cipher time and Decryption time for Lena (256x256) Mandrill(512x512)**

| Image | Time | It=1 | It=2 | It=3 | It=5 | It=7 | It=8 | It=10 |
|---|---|---|---|---|---|---|---|---|
| *Lena* | Encryption | 5.9309 | 11.3152 | 16.9309 | 27.3820 | 37.2907 | 43.3870 | 53.01 |
| | Decryption | 5.8321 | 11.2469 | 16.9382 | 26.7240 | 36.9724 | 42.5610 | 52.83 |
| Mandrill | Encryption | 22.7254 | 43.4145 | 64.9978 | 106.6131 | 149.0728 | 170.3110 | 211.60 |
| | Decryption | 22.8832 | 44.2216 | 65.5523 | 107.1847 | 151.0796 | 170.4845 | 213.04 |

## CONCLUSION

In our paper, we suggest new method to encryption image for mobile device by using permutation operation and xor operation to make confusion and diffusion for image and proposed new method to generate keys based on image properties as summation value and mean value (can use anther properties in future work), in method, we use set of keys and no need to enter any key by user. LFSR is use to generate keys for each block. The results from performed analysis prove our method which is simple, fast and have resistance to differential, brute force, statistical attacks. It seems that, the proposed encryption method can be an actual nominee for image encryption for mobile device.

## REFERENCES

[1] Schneider B., 1996, "Applied Cryptography, Second Edition: Protocols, Algorithms and Source Code in C", John Wiley & Sons, Inc., USA.

[2] William S., "Cryptography and Network Security Principles and Practices, Fourth Edition", Prentice

[3] Borie J., Puech W., Dumas M., 2004, "Crypto-Compression System for Secure Transfer of Medical Images", 2nd International Conference on Advances in medical Signal and Information Processing (MEDSIP 2004).

[4] J. Qayyum, M. Lal, F. Khan, and M. Imad, "SURVEY & ASSESSMENT OF WIMAX, ITS SECURITY THREATS AND THEIR SOLTUIONS", International Journal of Video & Image Processing and Network Security, Vol. 11, No. 3, 2011, pp. 36-47.

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

[6] Bibhudendra Acharya, 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, pp. 663-667, 2009.

[7] A. Mitra, Y.V Subba Rao, and S.R.M Prasanna, ―A New Image Encryption Approach using Combinational Permutation Techniques‖, International Journal of Electrical and Computer Engineering, vol. 1, no. 2, pp.127–131, 2006.