Implementation and Comparison of a Secure Lossless Image Encryption-then-Compression Algorithms

Asma Banu. S
Department of Electronics &Communication,
Bangalore University,
U.V.C.E, Bangalore-01.

Dr. A. Sreenivas Murthy
Associate Professor,
DOS in Electronics & Communication Engg.,
U.V.C.E, Bangalore-01.

***Abstract* — Image Encryption is important in the field of information security. In some of the practical scenario images are needed to be encrypted prior to compression. Most of image encryption techniques have some performance issues, so there is a need to determine performance of each method. In this paper we implement and compare three image Encryption algorithms. The Encryption algorithms are Arnolds transform, Combination of different permutations and Random Permutation of Clusters of Prediction errors. In Arnolds transform method, shuffling of pixel positions is by iteratively performing a linear transformation. In Combinational Random Permutation method, encryption is achieved by considering the combination of bits, pixels and blocks permutations to reduce perceivable information. In Random Permutation of Clusters of Prediction errors method, encryption is achieved in prediction error domain. Arithmetic coding is used to achieve Compression. Comparative analysis is performed based on performance evaluation factors. Sequential Decompression and Decryption is performed.**

Keywords*:- *Arnolds transform, Clustering, Random permutations, Gradient adjusted Prediction and Arithmetic coding.

I. INTRODUCTION

One of the main goals that must be achieved during the transmission of information over the network is protection from the unauthorized access of information. Image or video encryption has applications in many fields including the internet communication, transmission, medical imaging, Tele-medicine and military communication, etc. In general, there are two ways to achieve security- one is watermark and the other is encryption. The watermark-based techniques embed an invisible signal into the media to form a watermarked version. The method of transforming the original information into an unreadable format is called encryption and the reverse process is called Decryption of information. The study of encryption and decryption is known as Cryptography. In this work, we focus on image encryption also called image scrambling produces an unintelligible or disorder image from the original image. The encryption can be performed either using Symmetric key or by Asymmetric key. If same key is used for encryption and decryption then it is called as Symmetric key cryptography and if the different key is used for encryption and decryption then it is called as Asymmetric key cryptography. Image encryption algorithms can be classified into two kinds. One is spatial-based method and the other is frequency-based method. The spatial-based algorithms are usually achieved by swapping the pixel positions or altering pixel values. Under this there are three kinds of encryption techniques namely substitution, transposition or permutation techniques that include both transposition and substitution. Substitution schemes change the pixel values while permutation schemes just shuffle the pixel values based on the algorithm. In some cases both the methods are combined to improve security.

Image encryption using Arnolds Transform discussed in [1], explores the properties of Arnold’s cat map. Arnold's cat map is a simple discrete system that stretches and folds the trajectories in phase space. Scrambling effect is relatively best in Arnold's Cat Map and therefore, works efficiently for encryption of images of same size. In [2], the author has used exclusive OR operation along with Arnold Transform to produce scrambled images by which the multiple diffusions in the encryption scheme makes the cryptosystem more secure and robust. Also in [3], the author has exploited Logistic map to improve the security of Arnold transform method. Logistic map is general form of the chaotic map. Conventional Arnold transform based schemes in [1-3] have a common weakness that image height and width must be equal. To overcome the weaknesses of Arnold transform, in [4] the author combines Arnold transform and three random strategies like random division, iterative number generation and encryption order generation to design an image encryption scheme without size limitation.

The work in [5], focus on development of improved private key cryptographic methods for providing security i.e., designing private key cryptographic techniques based on permutation methods. And in [6], the author proposes designing of pseudo random sequence generators for generating binary sequences for cryptographic purpose which plays important role in effective information coding performance. The paper [7], proposes an image encryption using a combination of different permutation techniques that is using a random combination of all the three permutations [bit, block, and pixel] techniques.

In [8], a Context based adaptive Lossless Image Coding [CALIC] is proposed. CALIC employs a simple new gradient based non-linear predictor [GAP] which adjusts prediction coefficients based on estimates of local gradients. The work in [9], showed that stream cipher encrypted data is compressible through the use of coding with side information principles, without compromising either the compression efficiency. Furthermore, an approach of [9] was applied in the prediction error domain and achieved better lossless compression performance on the encrypted gray scale/ color images is described in [10]. And in [11] an image encryption scheme via pixel-domain permutation was designed and demonstrated that the encrypted file can be efficiently compressed by discarding the excessively rough and fine information of coefficients in the transform domain.

Following works [8]-[11], inspired the author for proposed work in [12], for designing an Image encryption then compression system via prediction error clustering and randomly permuting these clusters. The prediction of original image is made by using GAP to obtain prediction errors so that encryption algorithm is applied to prediction errors rather on original image. A Lossless Compression is achieved by standard Entropy Coding i.e., Arithmetic Coding. Comparative analysis of encryption algorithms based on performance parameters are discussed in [13-14].

Existing Compression-Then-Encryption [CTE] system:

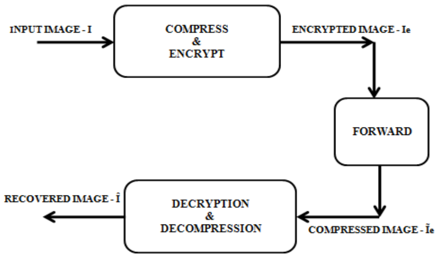


Fig. 1 shows block diagram of CTE system.

The Compression-then-Encryption (CTE) paradigm meets the requirements in many secure transmission scenarios. But in some situations the order of applying compression and encryption needs to be reversed, when a transmitter is always interested in protecting the privacy of the image data through encryption. Nevertheless, transmitter has no incentive to compress data or run a compression algorithm before encrypting the data. Then the channel provider, to maximize the network utilization compresses all the network traffic, therefore compression task is done at channel which has abundant computational resources this is called ETC system.

Proposed ETC system

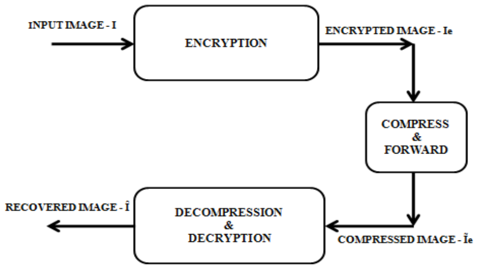


Fig. 2 shows block diagram of ETC system.

The primary focus of this project is to design a pair of image encryption and compression system, for an 8-bit greyscale images such that, compressing the encrypted images is almost equally efficient as compressing their original image. Meanwhile, reasonably high level of security needs to be ensured.

II. OVERVIEW OF PROPOSED WORK

In this section, a brief outline on implementation of three encryption methods employed to a grey-scale image as discussed in [1], [7] and [12] are explained –

A. Arnolds Transform

The Arnolds transform, also called cat map transform in [1]-[3], is only suitable for encrypting N×N images. An image is hit with a transformation that apparently randomizes the original organization of its pixels.

It is defined as:-

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = A \begin{bmatrix} x \\ y \end{bmatrix} (\mathrm{mod} N) \quad \text{--- (1)} \quad \text{where} \quad A = \begin{bmatrix} 1 & p \\ q & pq+1 \end{bmatrix}$$

Where p and q are positive integers, determinant (A) = 1, (x, y) and (x', y') are the pixel coordinates of the original image and the encrypted image, respectively. Hence, size of the image and parameters p, q of Arnold cat map may be treated as secret keys for image encryption. Image encryption using Arnolds transform, calculated for ‘n’ number of iterations can be written as:

$I(x', y')^{(k)} = A.\ I(x, y)^{(k-1)}$ (mod N) --- (2)

where k = 1, 2, ..., n

The encrypted image can be decrypted by equation (3) :

$J(x', y')^{(k)} = A^{(-1)}.\ J(x, y)^{(k-1)}$ (mod N) ---- (3)

where J(x', y') is a pixel of the decrypted image and J(x, y) is an encrypted pixel.

Arnold cat map rearranges the positions of image pixels. But after iterating a certain number, same pixels positions as original image are achieved. Due to this periodicity or repeatability makes the encryption algorithm unsecure, this is because without decryption one can easily obtain the original image just by iterative computations if the encryption algorithm is known. In our proposed work, we have implemented Arnolds transform along with additional key XOR ed with final iterated output of Arnolds transform to achieve more security and overcome periodicity.

B. Combination of Random Permutations

There are three basic Permutations techniques

1. Bit permutation

The image can be seen as an array of pixels, each with eight bits for 256 gray levels. In the bit permutation technique the bits in each pixel taken from the image are permuted with the key. The histogram of encrypted image will be uniformly distributed.

2. Pixel permutation

In this scheme a group of pixels are taken from the image. The pixels in each group are permuted using the secret key such that the positions of pixels within the group are changed. Therefore, histogram of encrypted image will be similar to the original image.

3. Block permutation:

In this technique the image can be decomposed into blocks. A group of blocks taken from the image are permuted same as bit and pixel permutations. For better encryption the block size should be lower. In encrypted image, as the position of pixels blocks are changed the histogram of it is similar to original image. Decryption is obtained by the inverse permutation of the blocks. By Combination of all 3 permutations, efficient image encryption can be achieved''.

4. Combinational permutation techniques

A random combination [7] of bit, pixel and block permutations are considered in our project. Due to the combination of these three approaches the visual intelligence reduces. In this method the order of the bit, pixel and block permutations are random.

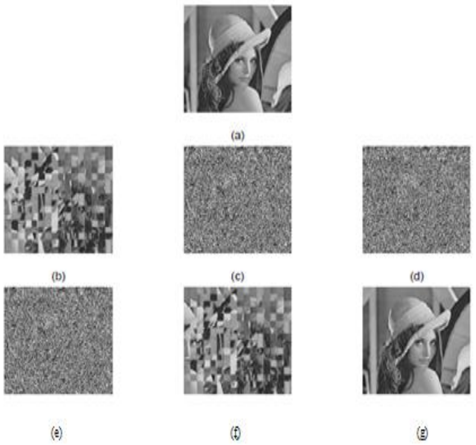


Fig 2.2a Results of the proposed technique with [block, bit, pixel] combination, (a) Original image. (b), (c), (d) Encrypted images with the above sequential combination in order. (e), (f), (g) are Decrypted images by inverse permutations with [pixel, bit, block] combination sequentially.

Fig 2.2a shows, the results with the combination of [block, bit, pixel] permutation respectively where encrypted image is a noisy image. Generally after the bit permutation the encrypted image will be appeared as a noisy image. But the pixel and block permutation methods make much stronger from the security point of view. To get back the original image at the receiver, the order of the permutation processes should be exactly reverse to the order at the transmitter i.e., [pixel, bit, block] combination only.

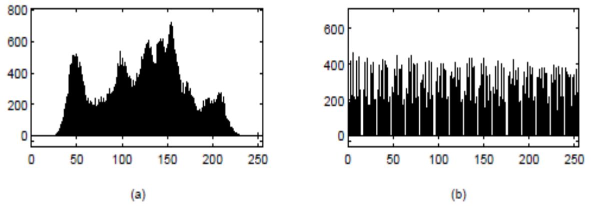


Fig 2.2b Histograms of combinational permutation (a) original image (b) Encrypted image

C. Random permutation of Clusters of Prediction Errors

Implementation of this method is divided into 3 sections:

1) Transmitter section represents Encryption process.
2) Channel section represents Compression process.
3) Receiver section represents Decompression & Decryption processes.

GAP (GRADIENT ADJUSTED PREDICTOR)

GAP [8] is a simple, adaptive, nonlinear predictor that can adapt itself to the intensity gradients near the predicted pixel 'P' shown in Fig 3.1a by estimating local gradients. Three heuristic thresholds are defined for 8-bit data to detect edges. Local gradient functions (vertical and horizontal gradients) are estimated by equation (3). Then the value has to be predicted to the pixel 'P' as given in [8].

$$d_h = |W - WW| + |N - NW| + |N - NE|$$
$$d_v = |W - NW| + |N - NN| + |NE - NNE| \quad \text{---- (3)}$$

			NN	NNE	
		NW	N	NE	
	WW	W	P=?		

Fig 3.1a shows the context of pixel'P'

where N, W, NE, NW, NN,WW and NNE represents north, west, northeast, northwest, north-north, west-west, and north-north-east neighbours of current pixel 'P', respectively.

Implementation of Clustering of Prediction errors-

In this method [12], for each pixel of original image I(i, j) is predicted as $\tilde{I}$ (i, j) by a GAP predictor. Prediction error is obtained from the difference between Original Image I(i,j) and predicted image $\tilde{I}$(i,j) is given by equation (4).

i.e., $e(i, j) = I(i, j) - \tilde{I}(i, j)$ ------ (4)

This prediction error e(i,j) may take any value between [-255,255], then this e(i,j) is mapped to $\bar{e}(i,j)$ ranging [0,255] by considering the fact that $\hat{I}.\tilde{I}(i,j)$ is available at decoder side.

i) At Transmitter section

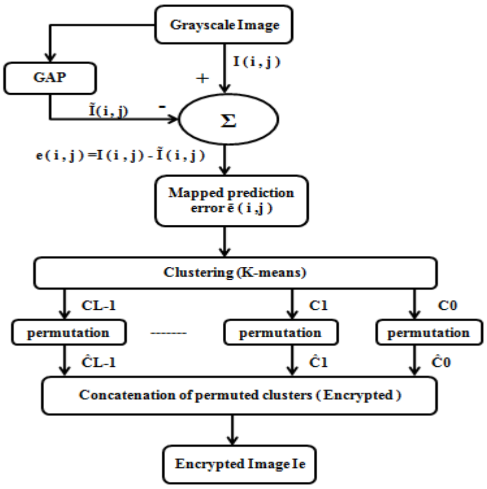
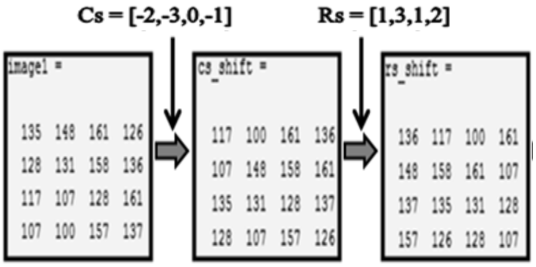


Fig. 3.1b shows block diagram of Image Encryption at Transmitter section

Steps to be carried out for image encryption are

1. Mapped prediction errors ē(i, j) are clustered into 'L' number of clusters $C_0, C_1, C_2 \ldots \ldots \ldots .\ C_{L-1}$. Clustering is based on K-means. Each cluster is grouped into size of 4X4 and then randomly permuted by cyclic shift operation.
2. A Rs (row shift) key and Cs (cyclic shift) key is chosen to perform cyclic shift in raster scan order to get permuted clusters as shown in figure 3.1b.
3. These permuted clusters $C_0, C_1, C_2 \ldots \ldots \ldots .\ C_{L-1}$ are concatenated to get Encrypted Image 'Ie'.



```
image1 =

  135  148  161  126
  128  131  158  136
  117  107  128  161
  107  100  157  137
```

```
cs_shift =

  117  100  161  136
  107  148  158  161
  135  131  128  137
  128  107  157  126
```

```
rs_shift =

  136  117  100  161
  148  158  161  107
  137  135  131  128
  157  126  128  107
```

Fig. 3.1b shows an example of cyclic shift operation.

ii) At Channel section

Steps carried out for image Compression are

1. A De-assembler is used to parse Ie into L segments as shown in fig 3.2b i.e., $\hat{C}_0, \hat{C}_1, \hat{C}_2 \ldots \ldots \ldots .\ \hat{C}_{L-1}$

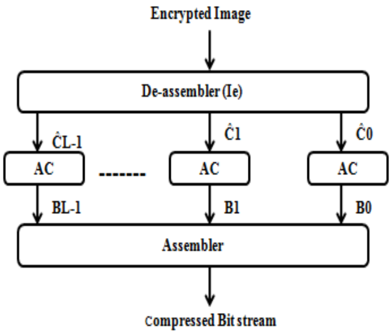


Fig. 3.1d shows block diagram of image compression at channel section

1. An AC is employed to losslessly encode each permuted clusters $\hat{C}_k$ into a binary bit stream B_k.
2. An assembler concatenates all B_k, to produce the final compressed and encrypted bit stream i.e., $B = B_0, B_1, B_2 \ldots \ldots \ldots .\ \mathbf{B_{L-1}}$.
3. The Length of Compressed Bit stream 'B' is transmitted to Receiver.

iii) At Receiver section:

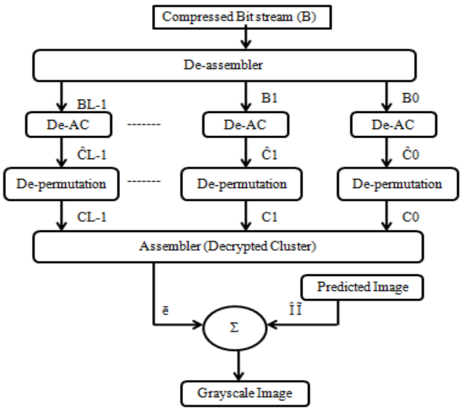


Fig.3.1e shows block diagram of sequential image Decompression & Decryption at Receiver

Steps carried out for image de-Compression and decryption

1. For each $\boldsymbol{B_k}$, an adaptive arithmetic decoding can be applied to obtain the corresponding permuted prediction error sequence $\hat{C}_{\boldsymbol{k}}$.
2. As the secret key K is known, the corresponding permutation operation can be employed to get back the original $\boldsymbol{C_k}$. With all the $\boldsymbol{C_k}$, the decoding of the pixel values can be performed.
3. The reconstructed pixel value is computed by Ī (i, j) = Ĩ (i, j) + e (i, j). Note in lossless compression, no distortion occurs that implies Ī(i, j) =I(i,j), i.e., Error-free decoding is achieved.

III. SECURITY ANALYSIS AND COMPRESSION PERFORMANCE

A comparative analysis based on performance evaluation factors are computed for any Encryption algorithm is described in [13-14].

Comparison criteria is based on -

1. Visual Analysis
2. Statistical Analysis
3. Compression Friendliness
4. Differential Analysis
5. Computation Speed Analysis

A. Visual Analysis

Observation is an important factor for testing an encrypted image. A good encryption algorithm should mix image so that features are not visually detectable and no information should be observed in comparison with original image.

B. Statistical Analysis

The statistical analysis on encrypted image is of crucial importance for a cryptosystem that means an ideal encrypted image should be strong against any statistical attacks. To prove the security of any Image Encryption Algorithm, following statistical tests are performed –

1) Histogram Analysis

To prevent the access of information to attackers, it is important to ensure that the encrypted and original images do not have any statistical similarities. Histogram analysis expresses the way of the distribution of pixels in the image.

2) Correlation Coefficient

Correlation is a measure that computes degree of similarity between two variables. Correlation coefficient is a useful measure to judge encryption quality of any cryptosystem. Any image cryptosystem is said to be good, if encryption algorithm hides all attributes of an original image and encrypted image is totally random and highly uncorrelated.

i. If encrypted image and original image are completely different then their corresponding correlation coefficient must be very low, or very close to zero.
ii. If correlation coefficient is equal to one, then two images are identical and they are in perfect correlation.
iii. If correlation coefficient is -1, encrypted image is negative of original image.

3) Mean Square Error (MSE)

Mean square error is the difference between the original image and the encrypted image. This difference must be very <u>high</u> for a better performance. It is given as:

$$\mathrm{MSE} = \frac{\sum_{i,j}^{M,N}[I(i,j) - Ie(i,j)]^2}{MXN}$$

Where I(i,j) is original image and Ie(i,j) is encrypted image, both with a size of MXN.

4) PSNR

Peak signal-to-noise ratio reflects the encryption quality. For a good encrypted image the value of PSNR must be <u>low</u>. Mathematically, it is computed as:

$$\mathrm{PSNR} = 10 \times \log_{10}\left[\frac{(256^2)}{\mathrm{MSE}}\right] \mathrm{dB}$$

C. Compression Friendliness

Multimedia compression has a vital role in the field of cryptography, since compression reduces storage space and transmission bandwidth. An encryption algorithm is compression friendly if it has small impact on data compression efficiency. By entropy based coding methods, multimedia data can be compressed.

1) Compression ratio= $\frac{\text{Number of bits representing Original image}}{\text{Number of bits representing Compressed image}}$
2) Bit rate = $\frac{(\text{No. of bits in Original image} - \text{No. of bits in compressed Image}) \times 8}{\text{No.of rows} \times \text{No.of columns}}$

D. Differential Analysis:

In general, a desirable property for an encrypted image is being sensitive to the small changes in original image (e.g., modifying only one pixel). If one small change in the original image can cause a significant change in the encrypted image then the differential attack actually loses its efficiency and becomes practically useless.

Common measures used for differential analysis are:

1) NPCR [Number of pixels change rate]

This measures the Number of Pixels change rate of encrypted image while one pixel of original image is changed. Generally NPCR value should ranges between 0 and 1. Let C_1 and C_2 be two different encrypted images whose corresponding original images are differ by only one pixel. D(i,j) is determined by: if $C_1(i,j) = C_2(i,j)$ then D(i,j) = 0 , otherwise, D(i,j) = 1.

$$\mathrm{NPCR} = \left[\frac{1}{M \times N}\right] \sum_{j=1}^{M} \sum_{i=1}^{N} D(i,j) * 100\%$$

2) MAE [Mean absolute error]

Let C (i, j) and P (i, j) be the gray level of the pixels at the ith row and jth column of an MXN encrypted and original image respectively. The larger value of MAE means that the encryption system is more secure upon attacks. The MAE between these two images is defined as

$$\mathrm{MAE} = \left[\frac{1}{M \times N}\right] \sum_{i,j=1}^{M,N} \mathrm{abs}(C(i,j) - P(i,j)]$$

where $C(i,j)$ = Encrypted image and
$P(i,j)$ = Original image of size M X N.

E. Computation Speed Analysis

Apart from the security consideration, the encryption speed is also important for real-time processes. In general, encryption speed is highly dependent on the CPU structure, memory size, OS platform, the programming language and also on the compiler options. For mentioned three image encryption algorithms, an analysis for the comparison of encryption speeds had been evaluated.

IV. SIMULATION RESULTS

This section shows the simulation results for the aforementioned Encryption Algorithms.

1) Visual analysis and Histogram Analysis of an 256X256 Pepper Image

A. Arnolds Transform Method

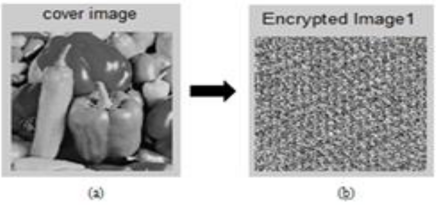


Fig 4.1a shows results of Arnolds transform method (a) Original image (b) Encrypted image

From analysis of Fig 4.1a, we infer that the encrypted image so obtained by Arnold transform method is visually not predictable. Histograms of the encrypted image and original image are significantly different i.e., have no statistical similarity in appearance. Therefore, this algorithm does not provide any clue for statistical attack.

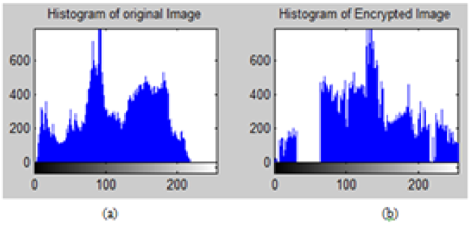


Fig 4.1b shows Histograms results of Arnolds transform method
(a) Original image (b) Encrypted image

B. *Combinational Permutations Method*

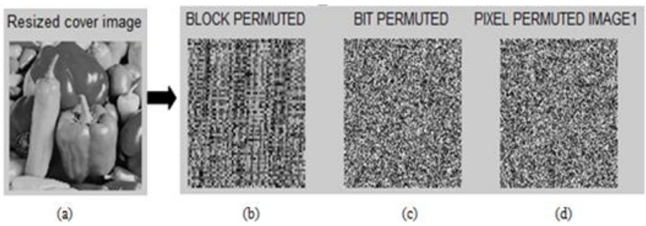


Fig 4.1c shows Combinational permutation method (a) Original image (b),(c),(d) Encrypted image [block, bit, pixel] respectively

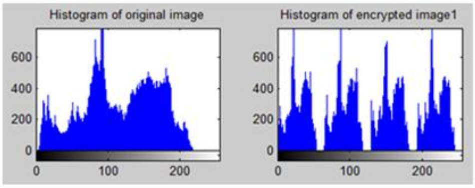


Fig 4.1d shows Histograms of Combinational permutation method
(a) Original image (b) Encrypted image

From analysis of Fig 4.1c, we infer that the encrypted image obtained from this method is also visually not predictable. Histogram of the encrypted image is uniformly distributed. Therefore, does not provide any clue for statistical attack especially Frequency analysis attack.

C. *Clustering Of Prediction Errors Method*

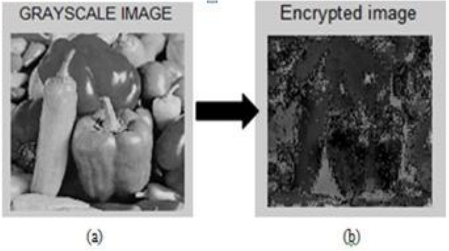


Fig 4.1e shows results of clustering of prediction errors method
(a) Original image (b) Encrypted image

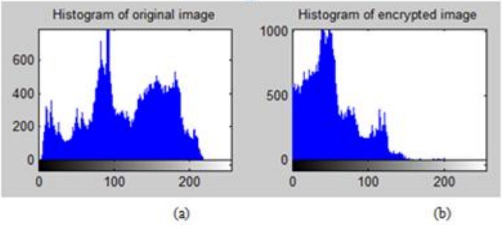


Fig 4.1f shows Histograms of clustering of prediction errors method
(a) Original image (b) Encrypted image

From analysis of Fig 4.1e, we infer that the encrypted image so obtained by Clustering of Prediction errors method is visually predictable but still histograms of the encrypted image and original image as shown in Fig 4.1f are significantly different i.e., have no statistical similarities in appearance. Hence, does not provide any clue for statistical attack

2) *Statistical Analysis Results*

IMAGES

Fig 4.2a shows sample images of size 256X256, (1) Pepper (2) Camera man (3) Jet plane (4) House (5) Living Room (6) Pirate (7) Women with dark hair (8) Flower.

Table 1: Shows the statistical parameters measured for the images shown above –

Images	Arnolds Transform		Combinational Permutation		Prediction error Clustering	
	Corr. Coeff	PSNR	Corr. Coeff	PSNR	Corr. Coeff	PSNR
1	0.001	10.2	-0.004	9.07	-0.16	8.73
2	-0.002	9.64	-0.001	8.51	-0.55	7.43
3	-0.001	5.12	-0.005	8.78	0.34	6.52
4	-0.002	8.38	-0.006	9.41	0.68	8.78
5	0.003	11.1	0.003	9.66	0.49	9.83
6	-0.004	9.48	-0.004	9.40	-0.11	9.04
7	0.001	7.35	-0.018	8.37	0.14	10.1
8	0.003	6.71	-0.003	9.24	0.63	13.0

From the results of Statistical analysis shown in table 1, we conclude as:-the Correlation Coefficient in method I & II is almost zero which shows quality of image encryption is good compare to method III. Weaker the Correlation Coefficient, best is the Algorithm. PSNR and MSE are calculated for Encrypted image with respect to Original image. In all the methods shown in table 1, are < 15 db therefore, efficient encryption is achieved from all the three algorithms.

3) *Compression Friendliness:*

Table 2: shows parameters measured for images which signifies compression friendliness

Images	Arnolds Transform		Combinational Permutation		Prediction error Clustering	
	C R	Bit rate	C R	Bit rate	C R	Bit rate
1	1.06	3.59	1.06	3.59	1.02	1.47
2	1.14	7.60	1.13	7.60	1.04	2.30
3	1.19	10.2	1.19	10.3	1.03	2.23
4	1.39	18.0	1.39	18.0	1.23	11.8
5	1.08	4.79	1.08	4.79	1.02	1.18
6	1.09	5.67	1.09	5.67	1.02	1.04
7	1.10	5.85	1.10	5.85	1.04	2.31
8	1.13	7.66	1.13	7.66	1.06	3.67

From table 2, the comparison of methods I, II and III reveals that: Methods I and II gives similar Compression ratios (C R), and Bit rate. Experimental results demonstrate that our coding scheme outperforms the conventional arithmetic encoders in terms of compression ratios. In method III, due to clustering the compression of each encrypted cluster requires more number of bits. Hence Compression ratio is less as a result the Bit rate is also less.

4) Differential Analysis Results

Table 3: shows parameters measured, which exhibits Diffusion characteristics

Images	Arnold's Transform		Combinational Permutation		Prediction Error Clustering	
	NPCR	MAE	NPCR	MAE	NPCR	MAE
1	99.494	2219.5	99.566	3294.0	99.777	8174.0
2	99.624	2463.7	99.614	3622.4	99.835	10269.0
3	99.905	12314.0	99.754	5784.0	99.824	11336.0
4	99.859	4904.0	99.572	4293.2	99.708	8586.3
5	99.607	2285.1	99.610	3277.1	99.751	7577.1
6	99.691	1723.9	99.578	2971.6	99.795	7663.7
7	99.688	2132.9	99.690	3281.0	99.677	6607.3
8	99.777	2928.7	99.704	1981.3	99.694	5085.0

In table 3, results based on differential analysis are tabulated from which we infer that:

Mean absolute Error (MAE) values in method III are more than the other two methods therefore larger value of MAE means that the encryption system is more secure upon differential attacks.

If the value of NPCR is high, proves a good diffusion characteristic which shows the encryption scheme is sensitive to small changes in the input image. Then algorithm proposed has good ability to anti differential attack.

5) Computation Speed Results

We test all the encryption schemes using MATLAB version R2013a. Performance was measured on a machine with Intel(R) core (TM) i3-2328 CPU @ 2.20 GHz with 4 GB of RAM, 64-bit operating system, x64 based processor running on Windows 8. The computation of average time used for Image Encryption then compression and recovering original image is tabulated in table 4. Therefore, from the Speed analysis it is found that method 2 takes less time for the whole process and method 3 takes more time compare to other methods.

Table 4: shows the computational speed of three Encryption then compression algorithms

Images	Arnold's Transform	Combinational Permutation	Prediction Error Clustering
	Time (sec)	Time (sec)	Time (sec)
1	114.96	68.520	130.27
2	128.67	69.285	156.24
3	129.38	67.087	142.24
4	135.25	66.604	154.12
5	124.09	69.065	145.48
6	110.86	65.958	168.03
7	137.33	65.839	158.99
8	133.26	66.429	147.58

V. CONCLUSION

In this project work, we have implemented three image encryption algorithms to encrypt grey-level images and then compress the encrypted images using Arithmetic coding. Experimental analysis is performed based on Statistical and Differential evaluation parameters, which demonstrate security, flexibility, effectiveness, reliability and robustness of the encryption algorithm.

Arnolds transform method is implemented by performing exclusive OR operation on the scrambled image. Arnolds transform performs efficiently demonstrate the features listed above such as security, flexibility, reliability etc. However, the applications are limited to images of same size and also computation speed.

Combination of different permutations method was simple-to-implement, where permutation of bits reduces the correlation and permutation of pixels and blocks produces high level of security. Therefore, random combination of all the three permutations decreases the perceptual information. The results shows, the graphical shape of encrypted image histogram is uniformly distributed which reveals that proposed algorithm is secure from frequency analysis attack. Experimental results, allow concluding that this algorithm outperforms other schemes, both in terms of speed and security. Working on the prediction error gave better results for spatial de-correlation, but reduces the bit rate while keeping the quality of the reconstructed image acceptable. Compression of encrypted image by prediction error clustering is slightly worse, in terms of compression efficiency. From the performance analysis it is found that this technique takes more time for the whole process compare to other two schemes.

To sum up, all the techniques are useful for real-time encryption. Each technique is unique in its own way, which might be suitable for different applications. To achieve better Lossless compression, Transform coding scheme like DWT based Lifting scheme can be applied after encryption.

REFERENCES

[1] Gabriel Peterson, “Arnold’s Cat Map”, Math 45 – Linear Algebra, Fall 1997.

[2] L. Zhu, W. Li, L. Liao, and H. Li, “A novel algorithm for scrambling digital image based on cat chaotic mapping,” In: Proc. of IIH-MSP '06, pp.601–604, 2006.

[3] Z. Shang, H. Ren, and J. Zhang, “A block location scrambling algorithm of digital Image based on Arnold transformation,” In: Proc. of the 9th International Conference, pp. 2942–2947, 2008.

[4] Zhenjun Tang, Xianquan Zhang, “Secure Image Encryption without Size Limitation using Arnold transform and Random Strategies,” Journal of Multimedia, Vol. 6, No. 2, April 2011.

[5] P.P. Dang and P. M. Chau, “Image Encryption for Secure Internet Multimedia applications,” IEEE Trans. Consumer Electronics, vol. 46, no. 3, pp. 395-403, Aug. 2000.

[6] A. Fuster and L. J. Garcia, “An efficient algorithm to generate binary sequences for cryptographic purposes,” Theoretical Computer Science 259, pp. 679-688, 2001.

[7] 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, 1:2 2006.

[8] X. Wu and N. Memon, “Context based adaptive lossless image codec,” IEEE Trans. Communication, vol. 45, no. 4, pp. 437– 444, Apr. 1997.

[9] M. Johnson, P. Ishwar, V. M. Prabhakaran, D. Schonberg, and K. Ramchandran, “On Compressing encrypted data,” IEEE Trans. Signal Process., vol. 52, no. 10, pp. 2992–3006, Oct. 2004.

[10] A. Kumar and A. Makur, “Distributed source coding based encryption and lossless Compression of gray scale and color images,” in Proc. MMSP, 2008, pp. 760–764.

[11] X. Zhang, “Lossy compression and iterative reconstruction for encrypted image,” IEEE Trans. Inf. Forensics Security, vol. 6, no. 1, pp. 53–58, Mar. 2011.

[12] J. Zhou, X. Liu, and O. C. Au, “Designing an Efficient Image Encryption then Compression via Prediction error clustering and Random Permutation,” IEEE Trans, Vol. 9, No. 1, January 2014.

[13] A. Jolfaei and A. Mirghadri, “A New Approach to Measure Quality of Image Encryption,” International Journal of Computer Network Security, vol. 2, no. 8, pp. 38 –44, 2010.

[14] G. Alvarez and S. Li, “Some basic cryptographic requirements for chaos-based Cryptosystems”, International Journal of Bifurcation and Chaos, vol. 16, no. 8, pp. 2129– 2151, 2006.