A Novel Image Encryption Algorithm Based on Chaotic AES Algorithm Related with Arithmetic Encoding

S.Suresh Raja[1], Dr. V.Mohan[2], Dr.S.Vijayalakshmi[3]
[1]Faculty of Computer Applications, K.L.N.College of Engineering, Tamil Nadu, India.
[2] Dean, Faculty of Mathematics, Thiagarajar College of Engineering, Tamil Nadu, India.
[3]Faculty of Computer Applications, Thiagarajar College of Engineering, Tamil Nadu, India

Abstract: In the recent decades, many image encryption algorithms based on chaotic systems had been proposed. In most of image security system, designing of image security is based on diffusion and confusion which will not able to salvage by attackers. There are lot existing methods are used to protect the image. In that AES and blowfish plays a vital role. In this proposed system, a chaotic based hybrid model is proposed for the security of image transaction.The proposed method is composed with new form AES and Arithmetic encoding. In the first step of the proposed method, the image pixels are shuffled with a random key in diagonal form by a modified AES shifting Algorithm. The key for shuffling is obtained from the coefficient of pixel intensities. Finally the shifted image is compressed with an arithmetic encoding for better transmission and storage. The proposed method produces a better PSNR value and MSE value with the compression efficiency than the existing image security systems.

Keywords:*AES cross shifting, Encryption* andCompression*, Arithmetic Encoding*.

I. INTRODUCTION

With the growingcondition for image transmission in public network, image Security becomes a very dominantquestion in communication science. To answer all kinds of security problemsabout image data emerged, such as unauthorized access [1, 2] and forge detection [3]. Encryptingimage is the most direct way to protect image.Encryption method can be segregated as asymmetrical and symmetrical. Symmetrical method of encryption achieves better quality than asymmetrical. By collecting advantages of various encryption methods and compression, a new system is proposed. It is a new form of chaotic image encryption to increase the complexity of the encrypted output image. For this, AES method is enhanced by the new form of shuffling, the starting position for shuffling is obtained from the intensity of the image pixels and finally, the encrypted image is compressed with arithmetic encoder. Since this proposed algorithm is highly sensitive becauseof new method of AES shuffling and compression.

The rest of this work is segmented as follows. Section II explainsthe existing survey. Section III elaborates the techniques of image compression and encryption. Section IV presents the description of the proposedwork. Section V shows the performance of the proposed work by experimental results along with a brief conclusive remark and discussion on future works.

II. RELATED WORK

The paper [4]has proposed a new image encryption method focused on rotating in matrix bit-level permutation diffusion in blocks. The proposed technique divides the plain image into 8 9 8 pixels blocks with a random matrix, then shuffles each one block into a 8 9 8 9 8 three dimensional parallel matrix, which has six sides as a cube. Permutation is performed by rotating the 3-D matrix that depends on plain image as per various heading. Further, the proposed technique diffuses the pixel block to further change that measures the attributes of image after confusion.In paper [5], the author proposed an image encryption with arithmetic coding technique to compress the data in blocks and achieved thecorrelation of each block.In [6], in this paper a cross chaotic map is proposed for different image formats like JPEG, TIFF, GIF, etc. which performs a block dividing of 3D baker. First it performs image decoding with respect to its format. Then,by cross chaotic map algorithm, a random key formed, finally by using 3D baker method, image gets permuted and encoded. This forms encrypted output. At decryption stage, the same process is applied reverse to get original reconstructed image for various format of image encoding. This method reduces the amount of data storage after encrypted result. In the past decades, a large number of systems have been proposed for image encryptionby exploiting all kinds of optical techniques [7-9], which own separate advantages of processingtwo-dimensional (2D) image data with parallel transmission mode.Compression in two stages is implemented in [10]. In that first, image binary shifting of 8 bit sequence is performed which equal lengths as like generated password. Then from that result, it is added to carrier image. The security is mainly based on choosing of carrier image to encrypt. Since this application of image encryption can easily retrieve the data by getting carrier image at decryption stage. A new scheme of image encryption is introduced [11] which is specific for the image data type to transmit at limited bandwidth range. For this, partial image encryption method is proposed using SCAN mapping method. This reduces the amount of image to encrypt and provide secure data transmission. These techniques provide sufficient range of security to image than other than the traditional SCAN method.

From these references, information about image encryption andcompression is collected to provide secure data transmission for recent usage of algorithms and methods.

III. IMAGE ENCRYPTION TECHNIQUE

This section describes the traditional encryption algorithm. In image encryption, two major types of images are used. One is RGB color image, and the other one is Gray scale image which is constructed as pixel in matrix. Here, encryption can do for both gray scale image and RGB color image and then compression technique is performed to secure image in transmission.

a) AES Algorithm

AES algorithm is asymmetrical image encryption technique. There are various types of AES algorithms which can rearrange the pixels in predefined / random location of image matrix. These rearrangementsof pixels can be done by either row- shifting or column shifting is called encryption.Also by using a randomized key matrix which is generated from the size of the image, bit-XOR operation can be performed to make an encrypted image form. For decryption process, this encrypted image is made bit-XOR with the generated key to extract original image.

This shifting performs withn-1 times. ‘n’ represents the size of image matrix. This shifting can be represent as, For Row shifting,

$$I_{out} = I_{in}\left(Row_{shift}\right)|_{(n=1,2,\ldots,R)} \qquad (1)$$

For Column shifting,

$$I_{out} = I_{in}\left(Column_{shift}\right)|_{(n=1,2,\ldots,C)} \qquad (2)$$

Where, 'I_{out}' represents AES shifted output, 'I_{in}' represents input original image and 'R' and 'C' represents Row and column size respectively.

Algorithm-1 describes the step-by-step process of Traditional AES algorithm.

Algorithm – 1: Traditional AES Shifting Algorithm

```
Inputs: I– Input image,
        R– Row of the image,
        C– Column of the image.
  1. Initialize l=0
  2. for i = 1 to R
       a. I(1 to C) = RShift // Row Shift, l times the ith row of I
       b. l=l+1;
  3. end loop;
  4. Initialize l=0
  5. for j = 1 to C
       a. I(1 to R) = CShift // Column Shift, l times the jth column of I
       b. l=l+1;
  6. end loop;
```

From the result of this sifting, image gets encrypted. This has made the image data in random pixel variation according to the random key generation.

b) *Image compression*

Image compression is a technique to reduce the storage quantity of data for low space image transmission. There is more number of image compression methods to reduce the size of image content.

The size of data compressed can be represented as compression ratio,

$$CR = \frac{\text{Size of Compressed data}}{\text{Total size of original data}} \qquad (5)$$

c) *Arithmetic Encoding technique*

In general, Arithmetic encoding technique is used to encode the data from the entropy value of given data. Thus, this method of image compression is named as an entropy encoding method which encodes the data in the form of symbols. This method is used in both lossy and lossless type of image compression method. This technique encodes the data by the features of probability estimated from image data. In the data sequence, the average length of an arithmetic code for a sequence of length m is given by,

$$E[l(\mathbf{X})] = \sum_{\mathbf{x}} P(\mathbf{x})l(\mathbf{x}) \qquad (8)$$

Where, $(x) = \left\lceil \log \frac{1}{P(x)} \right\rceil + 1$, length of bit sequence.

$P(\boldsymbol{x})$ – Probability of given data.

Here, it first converts the input data to bit stream and forms source modelling. Further, entropy data are extracted and compressed. At reconstruction stage, these data are decoded by entropy decoding method and remodelled into binary bit streams. Finally, the bit streams are transformed into decimal value to get original data.

IV. PROPOSED IMAGE ENCRYPTION AND COMPRESSION

This sectiondescribesthe proposed method of modified AES shifting image encryption method. The proposed novel image encryption technique shifts the pixels in the diagonal form. It gives a better result of diagonal shifting in forward and reverse direction as like RLE encoding method. In traditional method, the AES shifts the pixel from the starting point (1,1) or at end (end, end) of the image. This may reduce complexity by fixing the starting position as a standard location for shifting. This can be overcomes in proposed image encryption algorithm, where the starting location for shifting is obtained by the key, and the key is generated by intensities of the image pixel randomly. The shifted image is finally encoded by RLE for secure transmission.

i. *Key extraction*

In this stage, key is extracted to initialize the random shifting of proposed Cross mapped AES algorithm. For this, key value is extracted from the image pixel intensity of given input image. Therefore, key value depends upon image pixel matrix of image.

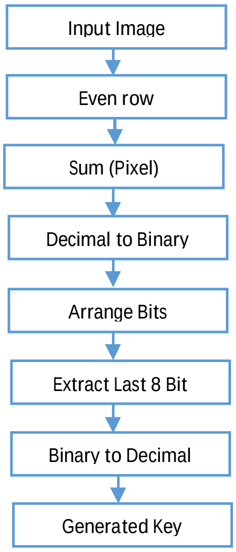


Fig 1.Block Diagram for Key Generation

Figure 5 shows the flow diagram of proposed key extraction method. In that, first pixel information is extracted by collecting the values of even columns of each row and summing the values. The summed decimal is converted into binary value. The least 8-bit of binary number is extracted and it is converted to decimal to generate a key. This is used as a starting point for image pixel shuffling by CS-AES algorithm. This can be expressed as,

$$Key = Decimal_{last8bit}\left(Binary\left(\sum_{i=2,4,\ldots even}^{n}\left(I(1,i)\right)\right)\right) \quad (6)$$

Where, ‘I’ denotes input image and ‘n’ denotes number of column of image (I).

Algorithm 3 shows step by step procedure for generating key value from input image matrix.

Algorithm – 3: Key value extraction

```
Inputs: I– Input image,
        C– Column of the image.
    Initialize sum = 0
    For i =2 to n  //Even column number
    Sum=sum+(I(1,i));
    End loop;
    Binary conversion of 'sum' value.
    Kl = Extract last 8-bit of binary bit stream.
    Key = Binary to Decimal of Kl.
```

Modified AES encryption method

The main contribution of this work is a novel AES shifting method is applied with a random key point. The key is formed, based on pixel intensities of input image. With the key as a starting point the shifting is performed over the diagonal cross mapping performing a reverse and forward shifting.

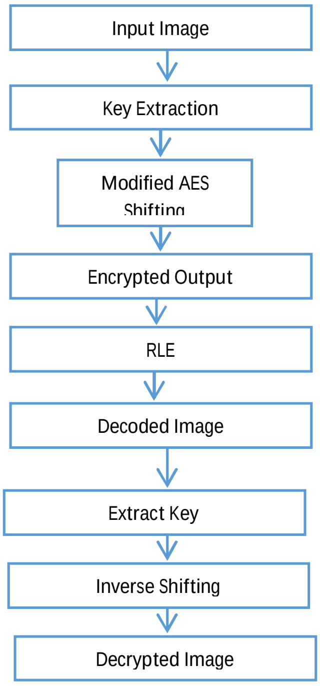


Fig. 2 Block diagram of proposed technique

The above figure shows block diagram of the proposed encryption method of Modified AES with image compression using RLE encoder.

The overall block diagram explains the structure of the proposed method. The key is first extracted from the given input image by summing all the even values of each row and converting into binary, the last 8-bit is extracted and converted back to decimal to obtain the key. The key is used as stating position for modified AES shuffling. From that starting point, check diagonal values of image and arrange that diagonal values as array data stream and this was continue to left side upto end of matrix. And then continue this to right side from starting point of matrix from key upto end of matrix. This can be described as in figure 6.

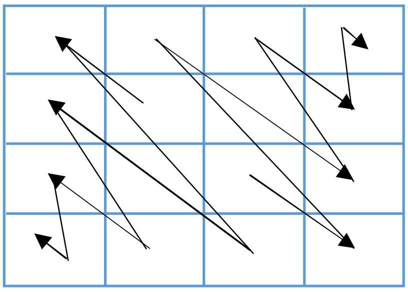


Fig. 3 Proposed AES shifting

Algorithm 4 and 5 describes step-by-step procedure for proposed encryption and decryption of shifting method of Modified AES.

Algorithm – 4: Proposed AES shifting (Encryption)

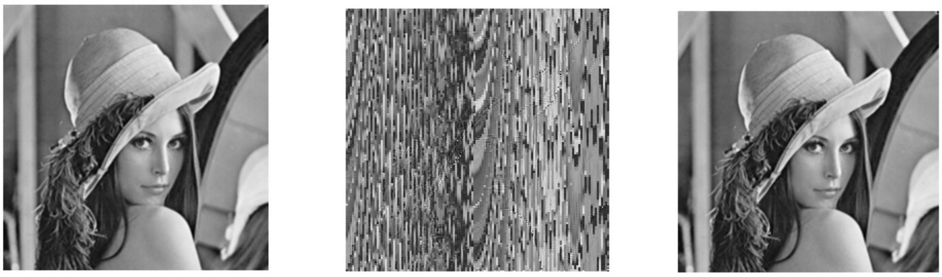
```
Inputs: I – Input image, K – Key
        N – Size of image at LL band.
1. I = Input Image
2. For i =1 to N
3. I_enc(i) = I (Diagonals from 1 to K);
4. End loop;
5. For i = N+1 to N*N
6. I_enc(i) = I_LL(Diagonal from K to end);
7. End loop;
8. Embed Key bit stream to LSM of encrypted image.
9. Apply RLE encoding
```

Algorithm – 5: Proposed AES shifting (Decryption)

```
Inputs: I_enc– Encrypted Input image, K – Key
        N – Size of image at LL band.
1. Decode RLE data
2. Extract LSM bit stream and find key, 'K'
3. For i =1 to N
4. I_dec(i) = I(Diagonals from 1 to K);
5. End loop;
6. For i = N+1 to N*N
7. I_dec(i) = I(Diagonal from K to end);
8. End loop..
```

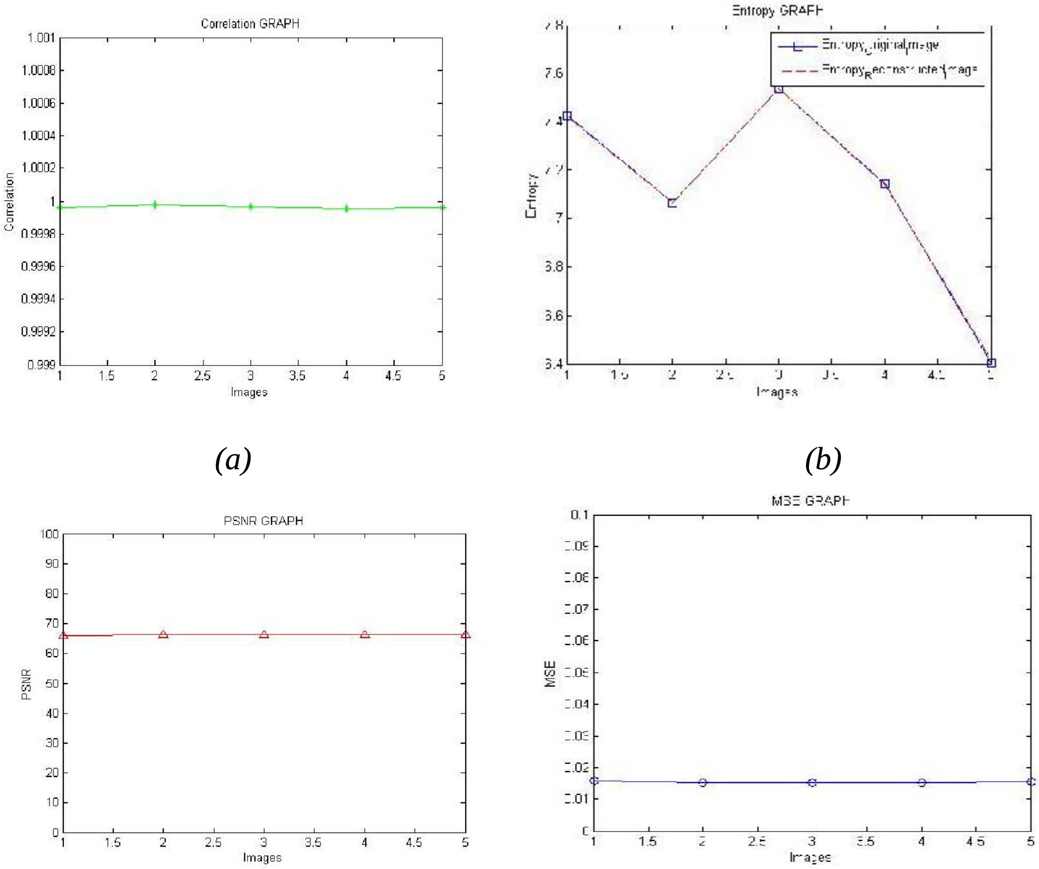
V. EXPERIMENTAL RESULTS

The image encryption steps of Lena input image using modified AES method is highlighted in figure 6. The input of Lena image is applied with modified AES to shuffle the image pixel with initialized key value. The total image is shuffled and compressed using RLE encoder. At decryption stage, decode the compressed data and extract key value which embedded in the encrypted image and apply Inverse AES respectively to get the original image.These step by step procedures are explained in below figures.



(a) (b) (c)

Fig. 4 Proposed Encryption Process: (a) Original Input image, (c) Modified AES Shifting, (c) Image Decryption



(a) *(b)*

(c) *(d)*

Fig. 5 Performance Chart of proposed algorithm (a)Correlation, (b) Entropy, (c) PSNR (d) MSE value.

Images	MSE	Correlation	PSNR	Entropy Original Image	Entropy Decrypted Image
Lena	0.0162	0.9997	66.0288	7.4272	7.4246

CONCLUSION

The proposed work of this paper defines a new image encryption of modified AES algorithm with Arithmetic Encoding which risesdifficulty of the image security. Compared to other image encryption algorithm, the proposed research attains better result.This algorithm has achieved well efficiency than existing image encryption and compression algorithms. The proposed system grades in an efficient structure in both image security and image storage capacity. The assessment of the proposed work with the traditional image encryption technique shows a better concert in the constraints of PSNR and MSE.Further, a better Correlation and entropy values are achieved through this proposed algorithm.

REFERENCES

[1]G. Chen, Y. Mao, and C. K. Chui, \A symmetric image encryption scheme based on 3D chaotic cat maps,"Chaos, Solitons& Fractals, vol. 21, no. 3, pp. 749 -761, 2004.

[2] Y.-L. Lee and W.-H. Tsai, \A new secure image transmission technique via secret-fragment-visible mosaic imagesby nearly reversible color transformations," IEEE Transactions on Circuits and Systems for Video Technology,vol. 24, no. 4, pp. 695 -703, 2014.

[3] J. Li, X. Li, B. Yang, and X. Sun, \Segmentation-based image copy-move forgery detection scheme," IEEETransactions on Information Forensics and Security, DOI:10.1109/TIFS.2014.2381872, 2015.

[4]ZHANG, Y., D. XIAO (2014)An image encryption scheme based on rotation matrix bit-level permutation and block diffusion. Communications in Nonlinear Science and Numerical Simulation, 19: 74-82.

[5] MASMOUDI, A., MASMOUDI, A. (2013) A new arithmetic coding model for ablock-based lossless image compression based on exploitinginter-block correlation. Signal, Image and Video Processing, pp. 1–7

[6] Miao Zhang, Xiaojun Tong, "A new chaotic map based image encryption schemes for severalimage formats, 2014" *The Journal of Systems and Software,Elsevier,*vol. 98, pp. 140-154,.

[7] P. Refregier and B. Javidi, \Optical-image encryption based on input plane and fourier plane random encoding,"Optics Letters, vol. 20, no. 7, pp. 767 - 769, 1995.

[8] B. Hennelly and J. Sheridan, \Optical image encryption by random shifting in fractional fourier domains,"Optics Letters, vol. 28, no. 4, pp. 269 -271, 2003.

[9] M. R. Abuturab, \Security enhancement of color image cryptosystem by optical interference principle and spiralphase encoding," Applied Optics, vol. 52, no. 8, pp. 1555 -1563, 2013.

[10] H. S. SharathKumar,H. T. Panduranga,S. K. Naveen Kumar,2013,"A Two Stage Combinational Approach for Image Encryption," *Advances in Intelligent Systems and Computing, Springer,*vol. 177, pp. 843-849.

[11] Parameshachari B.D.,K. M. S. Soyjaudah, 2012,"Analysis and Comparison of Fully Layered Image Encryption Techniques and Partial Image Encryption Techniques," *Journal of Engineering Research and Applications,* vol. 292, pp. 599-604.