IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-6, Issue-5, May 2018 E-ISSN: 2347-2693

A Novel Hybrid Digital Image Encryption Technique

Vikas Thada[1*], Utpal Shrivastava[2]

[1] Amity Institute of computer science and Engineering,Amity University, Haryana, India
[2] Amity Institute of computer science and Engineering,Amity University, Haryana, India

[*]*Corresponding Author: vthada@ggn.amity.edu, Tel.: 9958324522*

Available online at: www.ijcseonline.org

Accepted: 17May/2018, Published: 31/May/2018

***Abstract*—**In this growing era of information technology and the Internet, everybody is using interactive media in communication directly or indirectly. Images may have high confidential data.So these images need high security when they are stored somewhere, and when there is a need to send over any insecure communication network, then it is required to provide complete protection from tampering, accessing by illegal party that is not intended receiver. In this research work the problem is to design a novel scheme for 2D image encryption and decryption using an affine cipher, circular rotation of image matrix and the XOR operation. Father the security is enhanced by the fact that main secret key is broken into 3 sub keys and same sub keys are used for encrypting the three different panels of an RGB image. The use of circular shift is also performed by applying a secret operation on a secret key. A special secret key was also generated to be applied during the XOR operation after affine transformation is performed on the original. The cumulative effect of all the above steps results in secure encryption of the image. The encryption process is written in such a manner so that it can be easily reversed and decryption can be achieved by simply running the encryption algorithm in reverse order. This proposed encryption scheme can efficiently be utilized for securing the digital images.

Keywords*— *affine, encryption, decryption, key, image, xor

I. INTRODUCTION

Numeric representation (normally binary) of a 2-D image is a digital image. Pixels are used to make a digital image. Each pixel in the image is a representation of color as a single dot in the image, so another definition of pixel is that "it's a small color point of any color". The digital image contains multiple number of rows and columns of pixels. These pixels collectively represent some information. In this growing era of information technology and the Internet, everybody is using interactive media in communication directly or indirectly. Digital images cover a wide portion of multimedia data. Images play a very important role in network communication, for example in social networking sites, in commercial use, medical, military, national security agencies and diplomatic affairs etc.

It is a common fact that images play a critical role in military and in national security related task. Images may have high confidential data .So these images need high security when they are stored somewhere, and when there is a need to transfer over insecure network, then it becomes more necessary to provide complete protection from tempering, accessing by illegal party that is not intended receiver.

Cryptography is a technique to provide security in images. It is a process which transforms an image into a secrete image using a key, in the result that is difficult to understand the cipher image. On the basis of key as parameter there are two types of cryptography technique: Symmetric and Asymmetric

Secret key cryptography also known as shared key cryptography in which just one key is used for performing encryption and decryption. The same key is used by both the parties/person (sender and receiver) to encrypt and decrypt the data. This cryptography technique is also known as symmetric key cryptography as the key is same for encryption and decryption. The only problem with this technique is that how to securely distribute the key to both the parties/person.

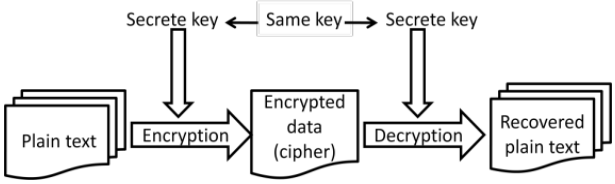


Fig 1: Secret or symmetric key cryptography

Public key cryptography makes use of two different keys to make a secure communication. Since a pair of keys (both different) is used so this technique is also known as asymmetric key cryptography. In this technique each party/person is in possession of a private key and a public key. The public key is used to encrypt data while the private key is used for decrypting the data. For example, if user A wants to send an encrypted message to B using this scheme then A will make use of B's public key to encrypt message and on receiving the same message user B will decrypt the message using its own private key.

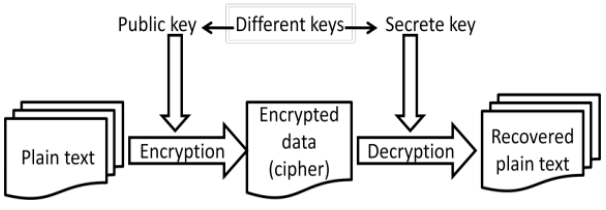


Fig2: Public or asymmetric key cryptography

However, there are distinct data encryption algorithms, for example, DES, IDEA, AES and RSA etc. and these techniques are powerful enough to provide protection to data, but these approaches are deficient to encrypt image data. Since images are different from text data in many aspects such as, images have bulky data, high redundancy, and strong correlation between adjacent pixels. Besides these attributes, images are less sensitive compares to text data, so if someone makes a little change in an image then it is hard to detect.

The rest of the paper is organized as follows: In section 2 a brief summary of various literary work done in the similar area is analyzed. Section 3 presents a brief overview of the proposed research work. Material and methods covering affine cipher, extended Euclid, Euclid and circular rotation is discussed in section 4. Section 5 presents the enciphering and deciphering algorithm used in this research work which is followed by section 5 which discusses experimental analysis and discussion of results. The paper ends with conclusions and references.

II. RELATED WORK

(Nag et al.,2011) have imparted a method, which applies 64 bits key in the encryption. The method operates using affine transformation and four sub keys of 8 bits. The authors decomposed the image into 2*2 pixel block size, and XOR with keys as discussed earlier to get new pixels. The disadvantage of this method was short key and no adequate security. (L.Bao et al, 2012) suggested a chaotic system that constitute 3 distinct one- dimensional chaotic maps. Authors used methods Logistic map as a role of controller to make decision in between Tent map or a Sine map for the generation of random sequences (L.Bao et al, 2012). The proposed approach provides a good security for the exhaustive key search and extreme key sensitivity and chaotic behavior. In this paper (Q.Sun et al., 2012) have proposed a one-dimensional random scrambling based method. In this a 2-D image is transformed into 1-D vector followed by random shuffling (Q.Sun et al., 2012). To produce encipher image an anti-transformation was done on to the resultant vector. Because of the only scrambling process the highly confidential images cannot be enciphered using this technique. In this paper, (Aminesh and Nidhi ,2012)an effective system is proposed which decomposes the original image into n*n block size. The technique use a transformation algorithm to minimize the correlation .The results of simulation validate that the propounded system generates a robust cipher image with the help of displacement in RGB values. In this treatise, (S.Joshi et al., 2012) have proposed a method , which scans an image pixel by pixel followed by substitution and permutation. For decryption ANN was used. The beauty of this method is that key exchange was not required and encryption was done on sender side only.The only problem was that decryption process was slow. In this paper, (Mohammed Abbas and Fadhil Al-Husainy, 2012) have contrived an approach that works on the bit level permutation by utilizing XOR and rotation of bits . The cryptographic method was symmetric. In this paper, (Anchal and Navin,2012) proposed a CNN technique that works on the diffusion and substitution. The permutation was achieved in initial layer and next layer does the substitution. In decryption this is reversed. The proposed technique has proven to be effective against the exhaustive key search and the plaintext or chosen plaintext attack. In this script, (Nidhi and Deepika,2012) have provided an encryption technique, which takes advantage of logistic mapping to encipher and compress an image. The Logistic based mode satisfies the confusion and diffusion properties in the cipher picture. Results show that the suggested strategy can offer feasible protection. In this paper, (Somdeep,2012) has proposed a combined technique. The propounded approach relies on the three methods of cryptography: (1) Extended Hill Cipher, (2) Bits rotation and reversal (3) Modified MSA Randomization [9]. The results corroborate that SD-AEI encoding procedure is better than the SD-EI due to additional randomization. In this exposition, (V.Chalam et al.,2012) The proposed method uses an artificial neural network to fulfil three tasks compression, authentication and security. The proposed method uses the universal approximation for the compression. The feed forward neural network for compression is used ; in which, the hidden layer has the least number of neurons as compared to the input layer. In this treatise, (Piya Singh & Karamjeet,2013) the proposed method is based on the blowfish algorithm. There are two processes; a key expansion, and then a data encryption. The aftermaths corroborate that blowfish technique is fast and secure. In this script, (R.U. Ginting, 2013) have propounded an algorithm which works on the RC4 Stream Cipher and Chaotic Logistic map. The results of this encryption algorithm validate that the decryption process is the highly key sensitive. In this article, (Gurpreet and Amandeep,2013)an advance version of the SD-IES technique by adding a new permutation block in the SD-IES technique. The results show that the GS-IES algorithm is better than previous SD-IES because of the inclusion of permutation block in the last stage.

III. PROPOSED WORK

Based on the review of literature (Nag et al.,2011;L.Bao et al, 2012;Q.Sun et al., 2012)The proposed research work try to overcome the limitations of the earlier research work in the same field by designing a novel scheme for 2D image encryption and decryption using an affine cipher, circular rotation of image matrix and the XOR operation. The hypothesis is: proposed encryption scheme using an affine cipher, circular rotation and xor operation successfully encrypts and decrypts the 2D digital image.

The scope of the work is providing a secure scheme for image encryption and decryption that involves symmetric key cryptography and some existing encryption technique for text encryption and decryption to be applied to digital images. This proposed encryption scheme can efficiently be utilized for securing the digital images.

IV. MATERIALS & METHODS

In this section various tools and methods used for carrying out this research work has been discussed. The main methods like affine cipher, Euclid algorithm, extended Euclid algorithms, Matlab, circular rotation etc are discussed.

4.1 Affine cipher

Affine cipher is an encryption scheme or type of substitution cipher, in which each English alphabet is represented by its numeric values starting from 0 for A, 2 for B upto 25 for Z. Then using an encryption method which is nothing but a mathematical formula (discussed shortly) every alphabet is converted to some other alphabet. During the decryption process reverse formula is applied and original text is recovered from encrypted text.

The encryption scheme is written in the following form:

$$\boldsymbol{E(x) = (px + r) mod\ 26}$$

Here E(x) is the affine encryption function where x is the integer value of English alphabet as discussed earlier to this function and p and r are (appropriately chosen) integers that work as constants and serve as key for this affine cipher.Changing different values of p and r results in

different versions of the affine scheme. Taking mod by 26 is to confining the numerical value E(x) within 0 and 25.

4.1.1 Encryption Using Affine Cipher

The affine cipher is a type of substitution cipher in the category of mono alphabetic cipher where each letter encrypts to one other letter, and back again following the rules of standard substitution cipher.

Considering the numerical values for the alphabets as given below:

A	*B*	*C*	*D*	*E*	*F*	*G*	*H*	*I*	*J*	*K*	*L*	*M*
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**

N	*O*	*P*	*Q*	*R*	*S*	*T*	*U*	*V*	*W*	*X*	*Y*	*Z*
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
13	**14**	**15**	**16**	**17**	**18**	**19**	**20**	**21**	**22**	**23**	**24**	**25**

Following the mathematical formula as shown above first the letters of an alphabet of size M (26 in this case) are converted to their numerical equivalent integers. After these using concepts of modular arithmetic same alphabet is transformed into an integer that is the corresponding cipher text for the plain text under consideration. The encryption formula for each alphabet is

$$E(x) = (px + r) \bmod M$$

Where M is total number of possible alphabets in the set (26 in English) , known as the size of the alphabet and p and r are the key of the affine cipher. The value p must be chosen such that p and M are co prime i.e. GCD (a, M) =1.

4.1.2 Decryption Using Affine Cipher

If we take y = E(x) = (px + r) mod 26, then we can solve the formula in terms of y for the value of x and can easily find out E−1(y) known as inverse that is, if y = (px + r) (mod 26), then y − r = px (mod 26)

By dividing both sides by mod 26 we get

$$px = (y - r) \bmod 26$$

Multiplying both sides by p^{-1} mod 26 we get then

$$x = p^{-1}(y - r) \bmod 26$$

So the formula for affine decryption becomes

$$E^{-1}(y) = p^{-1}(y - r) \bmod 26$$

Where p^{-1} is known as MMI (modular multiplicative inverse) of a modulo M. I. The MMI satisfies the following equation

$$1 = p.p^{-1} \bmod M$$

The MMI of a number pcan only exists when GCD (p, M) = 1. This is the requirement for the affine decryption.

4.2 Algorithm of Euclid

For finding greatest common divisor (GCD) or highest common factor(hcf) algorithm of Euclid is used. The algorithm is based on the following two observations:

If y|x then GCD (x, y) = y Where y|x means y divides x. The basis of Euclid's algorithm is division theorem.

If x = yt + r, for integers t and r, then GCD(x, y) = GCD(y, r). Here t is quotient and r is remainder.

Indeed, every common divisor of x and y also divides r. Thus GCD(x, y) divides r.

4.3 The Extended Euclidean Algorithm

The basis of Extended Euclidean algorithm is Euclid Algorithm. The algorithm is extended form of Euclid algorithm to find two values x and y such that

d=gcd(a,b)=ax+by (1)

From the equation (1) two more equations can be written provided d=gcd(a,b)=1

$ax \equiv d \bmod b \Rightarrow ax \equiv 1 \bmod b \Rightarrow x \equiv a^{-1} \bmod b$ (2)

$by \equiv d \bmod a \Rightarrow by \equiv 1 \bmod a \Rightarrow y \equiv b^{-1} \bmod a$ (3)

where x and y are known as modular multiplicative inverse of *a mod b* and *b mod a* respectively.

The algorithm is given below:

```
EXTENDED_EUCLID(a,b)
1 if b == 0
2     return (a,1,0)
3 else  (d1, x1,y1)=EXTENDED_EUCLID(b,a mod b)
4       (d,x,y)=(d1,y1,x1- (a/b)*y1)
5 return (d,x,y)
Note: (a/b) in line no 4 is integer division
```


The algorithm make use of Euclid algorithm in line number 3 and then using back substitution finds the value of x and y. The example will simply increase the length of the paper so reader is advised to search net for an illustrative example.

3.4 Circular Shifting Matrix in MATLAB

MATLAB is an acronym for Matrix Laboratory. It is known as language of technical computing. The software is developed by Mathworks Company of USA. MATLAB is a complete IDE for high-level language and for scientific computing.For circularly shifting matrix in Matlab there is a function by the name circshift. The syntax of this method is given as:

$$\boldsymbol{B = circshift(A, SS)}$$

The method shown above circularly shifts the values in the matrix A, by `SS` elements. `SS` is a vector / matrix of integer scalars written as a matrix of either 1 x 1 or 1 x 2. First element performs shifting in the first dimension i.e. in row of A and second dimension performs shifting for second dimensions i.e. column of A. For positive elements in SS contents of A are shifted down (or to the right). For negative elements in SS contents of `A` are shifted up (or to the left). As an example consider the following matrix:

$$\boldsymbol{A} = \begin{bmatrix} \mathbf{1} & \mathbf{2} & \mathbf{3} & \mathbf{4} \\ \mathbf{5} & \mathbf{6} & \mathbf{7} & \mathbf{8} \\ \mathbf{9} & \mathbf{10} & \mathbf{11} & \mathbf{12} \end{bmatrix}$$

Applying

circshift(A,[1]) operation on the above matrix gives following output:

$$\boldsymbol{A} = \begin{bmatrix} \mathbf{9} & \mathbf{10} & \mathbf{11} & \mathbf{12} \\ \mathbf{1} & \mathbf{2} & \mathbf{3} & \mathbf{4} \\ \mathbf{5} & \mathbf{6} & \mathbf{7} & \mathbf{8} \end{bmatrix}$$

It can be checked above operation results in circularly shifting of first dimension values of array A down by 1. Consider one more example of **circshift(A, [1, -1])**

$$\boldsymbol{A} = \begin{bmatrix} \mathbf{10} & \mathbf{11} & \mathbf{12} & \mathbf{9} \\ \mathbf{2} & \mathbf{3} & \mathbf{4} & \mathbf{1} \\ \mathbf{6} & \mathbf{7} & \mathbf{8} & \mathbf{5} \end{bmatrix}$$

It can be observed clearly that above operation results in circularly shifting first dimension values of Adown by 1 and second dimension values of A to the left by 1.

V. EXPERIMENT

In this section the experimentation process carried out in the research work is discussed. The algorithms for encryption and decryption along with implementation details are discussed. The implementation was done on MATLAB 7.1 by writing the code for both encryption and decryption.

5.1 Encryption Algorithm

The main concept behind developing this image encryption algorithm is generating of three separate keys for encrypting different planes of 2D image: Red, Green and Blue. Details of the process is presented in the algorithm.

Algorithm: AffineImageCipher

Input: Image IMG and Key secret. The image IMG can be any standard jpg/png colored or b/w image and key secret is any 6 digit integer value .

1. Calculate size of image IMG into m, n, and p; rows(height) are stored in m, columns(width) in n and number of color channels (3 for RGB) are represented by p.
2. Generate new key key2 which is a vector of length m*n using random generation method.
3. Reshape key2 vector into matrix FKey of size m by n.
4. Apply **SubKey** process to key secret and get six subkeys as key1(1) to key1(6) each of two digit.
5. Split the image IMG into 2-D matrices to get Red, Green and Blue components. Lets call them matrices R, G and B respectively.
6. Apply the affine cipher transformation on each pixels values of R, G and B matrices as:
   - 6.1 Use affine cipher for matrix R with a=key1(1) and b=key1(4)
   - 6.2 Use affine cipher for matrix G with a=key1(2) and b=key1(5)
   - 6.3 Use affine cipher for matrix R with a=key1(3) and b=key1(6)
7. Apply simple transformation on vector key1 and generate new subkeys k1, k2 and k3 using the concept of circular shifting the rows of matrices R, G and B. Use subkeys k1 for matrix R, k2 for matrix G and k3 for matrix B. Same keys with slight modification are used in decryption process.
8. Using Fkey with each of the matrix R, G and B apply XOR logical operation on each pixel on matrices R, G and B.
9. Combine R, G and B to get encrypted image EIMG.

The crux of the algorithm in subkey generation and its use in encrypting different planes of RGB image. Let's assume input key key1 is 985643. First we divide the input 6 digit number into 98, 56 and 43 and then reverse of this to get 89, 67 and 34. Now GCD of each of the number is calculated with 256. The GCD of each of preceding numbers must be 1 in case they are not then the number is incremented by 1. In this case it will be: Key1 = [99 57 43 89 65 35]

The general formula for the affine cipher is E(x) = (A * x + B) mod 26 where x is any input alphabet and A and B are constants. This formula we want to use for pixel transformation so instead of 26 value used is 256 as for class type uint8 the range of pixel values can be in between 0 and 255 i.e total 256 values. The value of x will be every pixel value from the Red , Green and Blue matrix. Though these matrices will be very big in size like 256 by 256 but for illustration purpose we have matrices of just 4 by 4 size.

Modified Affine Cipher for Image Processing will be:

(i) R(i,j)=(key1(1) * R(i,j) + key1(4)) mod 256
(ii) G(i,j)=(key1(2) * G(i,j) + key1(5)) mod 256
(iii) B(i,j)=(key1(3) * B(i,j) + key1(6)) mod 256

Next we get vector k1=[key1(1) –key1(4], k2=[key1(2) –key1(5)], k3=[key1(5), -key1(6)] and perform circular shift as:

(i) For matrix R
R(:,:)=circshift(R(:,:),k1);
R(:,:)=circshift(R(:,:),[99,-89]);

The above code means shifting the rows from bottom rows to top rows circularly 99 times and then shifting the columns from left side to right side 89 times. Similar transformation is applied to matrix G and B.

In the next step we make use of step 2 and 3 of the algorithm for the generation of FKey of size m by n using random generation method. Using this FKey and matrices R, G and B we apply bitxor operation onto the three matrices. Lets apply bitxor of FKey with R, G and B matrices. The bitxor simply performs bit by bit xor operation onto the bits of

(i) R(i,j)=bitxor(R(i,j), FKey(i,j))
(ii) G(i,j)=bitxor(G(i,j), FKey(i,j))
(iii) B(i,j)=bitxor(B(i,j), FKey(i,j))

Finally at the end the 3 2-D matrices combined to get a 2D image of size m by n by p.

II. Decryption Algorithm

The decryption algorithm is just the reverse of encryption algorithm. The steps applied in encryption process are simply reversed along with modular inverse operation as affine cipher decryption make use of modular inverse.

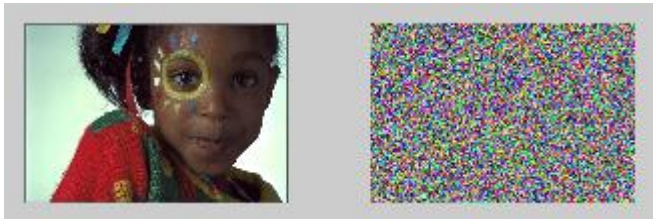
Algorithm: AffineImageDeCipher

Input: Image EIMG and Key secret. The image EIMG must be encrypted jpg/png colored or b/w image using the encryption algorithm and secret key of any 6 digit integer value .

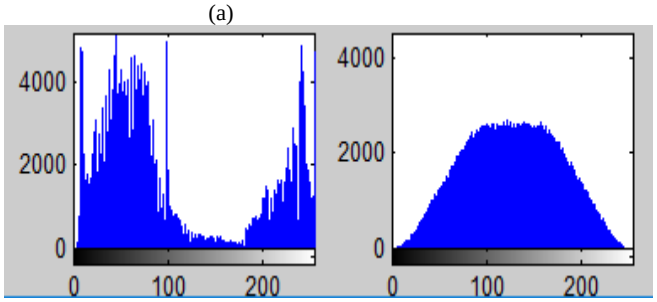
1. Calculate size of image EIMG into m, n, and p; rows(height) are stored in m, columns(width) in n and number of color channels (3 for RGB) are represented by p.
2. Split the image EIMG into 2-D matrices to get Red, Green and Blue components. Lets call them matrices R, G and B respectively.
3. Generate new key key2 which is a vector of length m*n using random generation method.
4. Reshape key2 vector into matrix FKey of size m by n.
5. Using Fkey with each of the matrix R, G and B apply XOR logical operation on each pixel on matrices R, G and B.
6. Apply **SubKey** process to key secret and get six subkeys as key1(1) to key1(6) each of two digit.
7. Using key1(1), key1(2) and key1(3), modular inverses mod 256 of these preceding keys are calculated using extended euclid algorithm and stored in variables inv1, inv2 and inv3.
8. Apply simple transformation (reverse of encryption) on vector key1 and generate new subkeys k1, k2 and k3. Use these keys in circular shifting the rows and columns of matrices R, G and B. Use subkeys k1 for matrix R, k2 for matrix G and k3 for matrix B.
9. Apply the affine cipher decryption transformation using the formula : $E^{-1}(y)=a^{-1}(y-b) \bmod 256$ on each pixels values of R, G and B matrices as:
   9.1 Use affine decipher for matrix R with a^{-1}=inv1 and b=key1(4)
   9.2 Use affine decipher for matrix G with a^{-1}=inv2 and b=key1(5)
   9.3 Use affine decipher for matrix B with a^{-1}=inv3 and b=key1(6)
10. Combine R, G and B to get decrypted image DIMG.

VI. RESULTS & DISCUSSION

The algorithm discussed in the previous section was implemented in MATLAB 7. Total 10 ".png" images were considered for this research work. The images were obtained from [X]. Here we are showing only 4 images along with their histograms though the experiment was conducted for all 10 images. This is just not to increase the length of the research paper.



(a)



(b)

Fig 3: (a) Original(girl.png) & Encrypted Image (b)Histogram of original & encrypted image

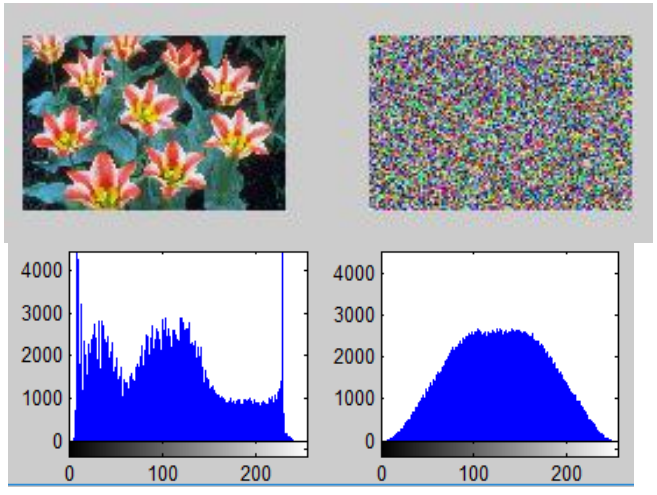


Fig 4: (a) Original(tulips.png) & Encrypted Image (b)Histogram of original & encrypted image

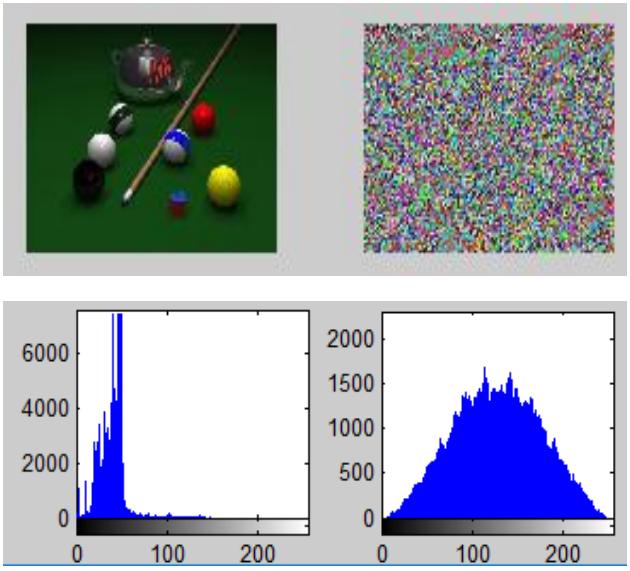


Fig 5: (a) Original(pool.png) & Encrypted Image (b)Histogram of original & encrypted image

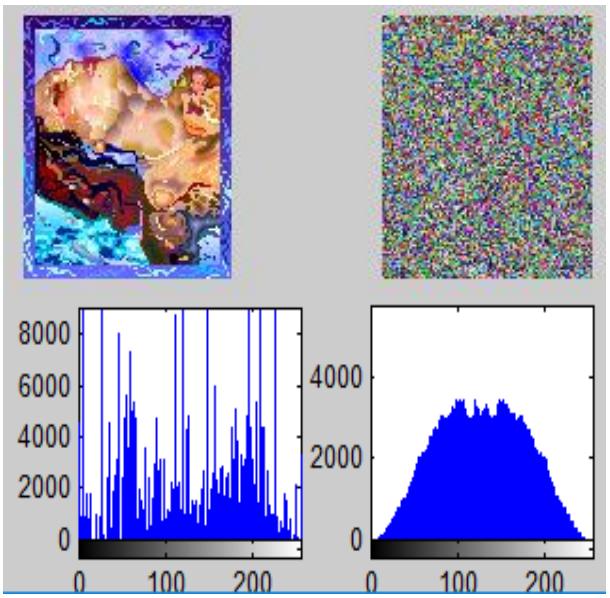


Fig 6: (a) Original(serrano.png) & Encrypted Image (b)Histogram of original & encrypted image

Looking at all four figures (b) part it is clear that histogram of encrypted image is sort of uniformly distributed edge to edge, not up the sides as compared to original image. This type of histogram is ideal for the image security as it does not give any clue about the original image. Further looking at the encrypted image also it is extremely difficult to decipher the image without the use of key used for encryption.

Table 1: Various image quality parameters calculated in research work

	airplane.png	girl.png	watch.png	tulips.png	pool.png	monarch.png	frymire.png	peppers.png	590errano.png	sails.png
Image Size(KB)	439	608	680	663	182	599	246	526	104	787
MSE	170.887	96.7602	61.8465	91.2084	26.7473	93.3529	99.3094	100.7726	125.9713	104.2463
RMSE	13.0724	9.8367	7.8643	9.5503	5.1718	9.6619	9.9654	10.0386	11.2237	10.2101
PSNR	25.8402	28.3284	30.2634	28.5801	34.6817	28.6653	28.1979	28.4145	27.1851	28.0268
Entropy	7.9998	7.9998	7.9999	7.9998	7.9997	7.9998	7.9999	7.9997	7.9999	7.9999
Corr	-0.0025	-0.0005	-0.0006	-0.0003	0.0008	-0.0003	0.0005	-0.0013	0.0004	-0.001
MAE	206.1524	107.8527	41.0916	89.6975	15.6267	80.4463	124.1952	98.1384	147.4216	89.2804
Etime	1.715826	2.565544	5.132536	2.591361	1.266444	2.58568	8.361211	1.730276	3.458236	2.588638
Dtime	1.721422	2.602107	5.177072	2.619358	1.285156	2.630956	8.396961	1.739099	3.38319	2.593517

Various image quality parameters like Mean Square Error(MSE), Root Mean Square Error(RMSE),Peak Signal to Noise Ratio(PSNR),Mean Absolute Error(MAE), Correlation Coefficient and Entropy was calculated for all images. Here values for all the above quality parameters for image are tabulated in table 1.

The correlation coefficient(cc) parameter has an indication of how much two images are correlated. The value of cc lies in the range between -1 and +1. Co-relation means change in the value of one image will predict a change in the same direction in the second image. Negative value of cc means change in the opposite direction. Looking at the values in the table clearly indicates that there is no chance of any positive correlation between original and encrypted image. MSE,MAE, PSNR has to be high for image security which is clearly visible in the table 1. Further for 8-bit image having max value as 256 entropy has to be near about 8 and same is obtained of encrypted image.
The encryption and decryption time is also in within 1-10 seconds. The research work has not considered big size images as Matlab does not treat them well and they are not loaded fully in memory.

The research work has also analyzed the size of encrypted image from original and also recovered image from encrypted image. The analysis is shown in the table 2 and 3given below:

Table 2: Comparison of plain and encrypted image size

Sr.No	Image Name	Original Size(KB)	Decrypted Size(Kb)	% Loss /Gain in size
1	Airplane.png	439	415	0.05
2	Girl.png	608	603	0.008
3	Watch.png	680	694	-0.02
4	Tulips.png	663	666	-0.004
5	Pool.png	182	176	0.03
6	Monarch.png	599	604	-0.008
7	Frymire.png	246	379	-0.54
8	Peppers.png	526	495	0.05
9	Serrano.png	104	154	-0.48
10	Sails.png	787	791	-0.005

Table 3: Comparison of decrypted and original image size

Sr.No	Image Name	Original Size(KB)	Encrypted Size(Kb)	%Increase in Size
1	Airplane.png	439	769	75
2	Girl.png	608	1154	90
3	Watch.png	680	2308	239
4	Tulips.png	663	1154	74
5	Pool.png	182	573	215
6	Monarch.png	599	1154	93
7	Frymire.png	246	3621	1372
8	Peppers.png	526	769	46
9	Serrano.png	104	1466	131
10	Sails.png	787	1154	47

Looking at the table 2 it is easily analyzed that proposed encryption method is increasing the size of the encrypted file by a factor between 0.75 to 3 except two images number 7 and 9 where encrypted size increased to whopping 13 times. The test have been conducted for images <1 MB so the encryption and decryption time cannot be considered as high but for big size images say between 5-10 MB encrypted size. One single image of size 5.04 MB was tested and it took around 119 seconds for encryption and size of encrypted image was approximately 10 times of the original image.

The table 3 analyzed the size of recovered image after performing decryption on the encrypted image. Looking at the table 3 and column 4 and 5 it was observed that decrypted file size was either more or less in size than original file size. In case of size greater than original result is shown in table 3 with –ve sign. If you look at all entries in the column 5 then you will notice that loss is negligible andno noticeable difference were observed from naked eyes for all the images. Thus decryption process has successfully recovered the original file.

VII. CONCLUSION

The research work has performed encryption and decryption of 2D digital images using affine cipher, circular shift of matrix and XOR operation in the MATLAB environment. Experimentation results on various images of varying sizes and extensions have shown that this new proposed scheme for image encryption and decryption has turned out to be secure considering the fact that secret key is to be kept secure. Further the security is enhanced by the fact that main secret key is broken into 3 sub keys and same sub keys are used for encrypting the three different panel of an RGB image. Use of circular shift is also performed by applying secret operation on secret key. Shift elements for circular shift is also derived from the original secret keys. A special secret key was also generated to be applied during the XOR operation after affine transformation is performed on the original. The cumulative effect of all the above steps result in secure encryption of the image. The encryption process is written in such a manner so that it can be easily reversed and decryption can be achieved by simply running the encryption algorithm in reverse order. Thus the hypothesis stated in proposed work have turned out to be true. The research work carried out is complete in all respect but with some limitations. It has still a lot of future scope for increasing the performance of encryption and decryption. First improvement that can be seen as future work is making the implementation as graphical based. Second the length of key can be increased from just 48 bits to some other big size such as 56, 72, 128,256, 512 bits etc. Further complexity of the encryption and decryption can be increased by adding some more randomness in selecting the keys and performing circular rotation onto the submatrices of input image. Third improvement can be to performing the encryption and decryption on almost any image type. The research work has not used tiff images in the experiment process.

ACKNOWLEDGMENT

The authors would like to thank many researchers and authors whose work have helped us in understanding the research matter well. Special thanks to Google and our colleagues who directly and indirectly helped us in carrying out this research work.

REFERENCES

[1] Nag, Jyoti Prakash Singh, Srabani Khan, Sushanta Biswas, D. Sarkar, ParthaPratim Sarkar "Image Encryption Using Affine Transform and XOR Operation" 2011 International Conference on Signal Processing, Communication, Computing and Networking Technologies (ICSCCN 2011), 21-22 July 2011, pages : 309-312.

[2] Long Bao, Yicong Zhou, C. L. Philip Chen, Hongli Liu "A New Chaotic System for Image Encryption" 2012 International Conference on System Science and Engineering, June 30-July 2, 2012, pages: 69-73 .

[3] Qiudong Sun, Ping Guan, YongpingQiu, YunfengXue "A Novel Digital Image Encryption Method Based on One-dimensional Random Scrambling" 2012 9th International Conference on Fuzzy Systems and Knowledge Discovery, 29-31 May 2012, page: 1669-1672.

[4] AmneshGoel, Nidhi Chandra "A Technique for Image Encryption Based On Explosive n*n Block displacement Followed By Inter-Pixel Displacement of RGB Attribute of A Pixel" 2012 International

Conference on Communication Systems and Network Technologies, 11-13 May 2012, page: 884-888.
[5] Saraswati D. Joshi, Dr. V.R. Udupi, Dr. D.R. Joshi, "A Novel Neural Network Approach for Digital Image Data Encryption/Decryption", Power, Signals, Controls and Computation (EPSCICON), 2012 International Conference on 3-6 Jan. 2012, pages: 1-4.
[6] Mohammed Abbas Fadhil Al-Husainy, "A Novel Encryption Method for Image Security", International Journal of Security and Its Applications, vol.6, no.1, January 2012, pages: 1-8.
[7] Anchal Jain, NavinRajpal, "A Two Layer Chaotic Network Based Image Encryption Technique", Computing and Communication Systems (NCCCS), 2012 National Conference on 21-22 Nov.2012, pages: 1-5.
[8] NidhiSethi, Deepika Sharma, "A New Cryptographic Approach for Image Encryption", Parallel, Distributed and Grid Computing (PDGC), 2012 2nd IEEE International Conference on 6-8 Dec. 2012, pages: 905-908.
[9] SomdipDey, "SD-AEI: An Advanced Encryption Technique for Images", Digital Information Processing and Communications (ICDIPC), 2012 Second International Conference on 10-12 July 2012, pages: 68-73.
[10] Hazem Mohammad Al-Najjar, "Digital Image Encryption Algorithm Based on Multi-Dimensional Chaotic System and Pixels Location", International Journal of Computer Theory and Engineering, Vol. 4, No. 3, June 2012, pages: 354-357.
[11] Dattatherya, S. VenkataChalam&Manoj Kumar Singh, "Unified Approach with Neural Network for Authentication, Security and Compression of Image: UNICAP", International Journal of Image Processing (IJIP), Volume (6), Issue (1), 25 Feb 2012, pages: 13-25.
[12] Pia Singh, Karamjeet Singh, "Image Encryption and Decryption Using Blowfish Algorithm in MATLAB", International Journal of Scientific & Engineering Research, Volume 4, Issue 7, July-2013, pages: 150-154.
[13] RiahUkurGinting, Rocky YefrencesDillak, "Digital Color Image Encryption Using RC4 Stream Cipher and Chaotic Logistic Map", Information Technology and Electrical Engineering (ICITEE), 2013 International Conference on 7-8 Oct. 2013, pages: 101-105.
[14] Gurpreet Singh, Amandeep Kaur, "GS-IES: An Advanced Image Encryption Scheme" International Journal of Engineering Research & Technology, Vol. 2 Issue 9, September – 2013, pages: 465-468.
[15] D. R.Stinson, Cryptography, Theory and Practice. Third edition: Chapman & Hall/CRC, 2006.
[16] William Stallings, Cryptography and Network Security, Principles and Practice. Fifth edition.
[17] ShujiangXu, Yinglong Wang, Jizhi Wang, YucuiGuo, "A Fast Image Encryption Scheme Based on a Nonlinear Chaotic Map", 2010 2nd International Conference on Signal Processing Systems (ICSPS), 5-7 July 2010, pages: v2-326-v2-330.
[18] Linhua Zhang, Xiaofeng Liao, Xuebing Wang, "An image encryption approach based on chaotic maps", Chaos, Solitons & Fractals. Volume 24, Issue 3, May 2005, Pages 759–765.
[19] http://en.wikipedia.org/wiki/Histogram
[20] Karl Pearson (1895), "Contributions to the Mathematical Theory of Evolution II, Skew Variation in Homogeneous Material". Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences 186: 343–414.
[21] XuShujiang Wang Yinglong, GuoYucui Wang Cong, "A Novel Chaos-based Image Encryption Scheme", International Conference on Information Engineering and Computer Science (ICIECS) 2009, 19-20 Dec. 2009, pages: 1- 4.
[22] http://www.waset.org/journals/waset/v3/v3-7.pdf Analysis and Comparison of Image Encryption Algorithms by IsmetÖztürk and Ibrahim Soukpinar.
[23] Abhinav Srivastava, "A survey report on Different Techniques of Image Encryption", International Journal of Emerging Technology and Advanced Engineering, Volume 2, Issue 6, June 2012, pages: 163-167.
[24] Khaled Loukhaoukha, Jean-Yves Chouinard, and AbdellahBerdai, "A Secure Image Encryption Algorithm Based on Rubik's Cube Principle", Journal of Electrical and Computer Engineering, Volume 2012 (2012), Article ID 173931, 13 pages.
[25] J. Bangarraju, V. Rajagopal, and B. Nithin, "Mitigation of supply disturbances using three-leg VSC based DVR from Single Phase P-Q Control Strategy," in 2015 International Conference on Electrical, Electronics, Signals, Communication and Optimization (EESCO), 2015, pp. 1–6.
[26] P. K. Naskar, A. Chaudhuri, and A. Chaudhuri, "A Secure Symmetric Image Encryption Based on Linear Geometry," in Ieee, 2014, pp. 67–74.
[27] Nurhayati and S. S. Ahmad, "Steganography for inserting message on digital image using least significant bit and AES cryptographic algorithm," in 2016 4th International Conference on Cyber and IT Service Management, 2016, pp. 1–6.
[28] N. Saikumar, R. B. Krishnan, S. Meganathan, and N. R. Raajan, "An encryption approach for security enhancement in images using key based partitioning technologies (ICCPCT), 2016, pp.-1-4.
[29] K. Sivaranjani and P. B. Prabahar, "Mended algorithm for image encryption based on random shuffling technique," in 2013 IEEE International Conference on Computational Intelligence and Computing Research, 2013, pp. 1–4.
[30] C. Torres-Huitzil, "Hardware realization of a lightweight 2D cellular automata-based cipher for image encryption," in 2013 IEEE 4th Latin American Symposium on Circuits and Systems (LASCAS), 2013, pp. 1–4.
[31] J. Vreugdenhil, K. Iverson, and R. S. Katti, "Image encyption using dynamic shuffling and XORing processes," in 2009 IEEE International Symposium on Circuits and Systems, 2009, no. 2, pp. 734–737.
[32] M. Bin Younas and J. Ahmad, "Comparative analysis of chaotic and non-chaotic image encryption schemes," in Proceedings - 2014 International Conference on Emerging Technologies, ICET 2014, 2014, pp. 81–86.

Authors Profile

Dr. Vikas Thada has doctoral and Master's degree in Computer Science & Engineering. He is currently serving as Associate Professor in the Department of Computer Science & Engineering. He has more than 17 years of teaching experience with around 7 years of research experience. He has many publications in international journals and is author of number of books on programming, data structures etc. His research interests genetic algorithm, cryptography, machine learning and deep learning.

Mr Utpal Shrivastava has Master's degree in Computer Science & Engineering and pursuing Ph.D in the area of machine learning. He is currently serving as Assistant Professor in the Department of Computer Science & Engineering. He has more than 10 years of teaching experience with around 4 years of research experience. He has many publications in national and international journals. His research interests genetic algorithm, networking, computer graphics and machine learning .

