International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 05 | May 2019 www.irjet.net p-ISSN: 2395-0072

Image Encryption based on Non-Subsampled Contourlet Transform with Differential Evolution

S.Thaslim banu[1]M.E, Dr.Rahila bilal [2] M.E., Ph.D.,,

[1]M.E Applied electronics, Thanthai periyar govt. inst. of technology, Vellore, India, thaslimsubhan@gmail.com
[2]Professor, department of ECE, Thanthai periyar govt. inst. of technology, Vellore, India, bilalrahila@gmail.com

---

Abstract - *The main challenges of image encryption are robustness against attacks, key space, key sensitivity, and diffusion. In this proposed technique, two concepts are utilized to encrypt the images in an efficient manner. The first one is Arnold transform, which is utilized to permute the pixels position of an input image to generate a scrambled image and the keys also confused using this transform. The second one is generalized logistic equation to generate a secrete key. Those keys are diffused in permuted pixels after taking Non-subsampled contourlet transform. Differential evolution is used for fine tuning of key space. Different test analysis like correlation, PSNR, MSE and histogram analysis is done for verification of the performance of the algorithm.*

Key Words: Arnold transform (AT), permutation, diffusion, generalized logistic equation, non-subsampled contourlet transform, differential evolution (DE).

1. INTRODUCTION

Due to the innovation in multimedia tools and Internet, media such as images, video, audio, etc. have become large day by day. Images are the prime source of information in various fields such as military communication, medical imaging, remote sensing, personal photographs, private video conferences, telemedicine system, etc. Hence, images require protection while storage and transmission over the Internet from eavesdropping, unauthorized access, and manipulations. To deal with these issues, image encryption techniques have been developed by researchers in past few decades to protect confidential images.

As long as a communication network exists in world, there would be hacking and stealing up of data. Apart from commercial loss due to such hacks, it would result in collapse of the database. Also, it is seen commonly in cyberspace that a popular website is hacked and data are stolen or spoiled. This would result in high degree of uncertainty in security of the data. It should be noted that there is a tremendous increase in the no of users on internet day by day which eventually increases the amount of text data and multimedia data to be handled and hence storage capacity is proportionally increased as well.

This is an abnormal scenario that exists at present, is being compensated through available methods of encryption and compression standards. There exists a large gap between the expected image encryption standards and available methods. This has highly motivated to conduct the research in a new orientation to a better extent and improve the metrics of the existing encryption standards and methods. Choosing chaotic based encryption domain has many valid reasons as presented below. By the term chaos, it is understood that a system, which behaves, based on the initial conditions but appear to be random. All the natural systems such as planetary motions, weather conditions, rain fall seasons, chemical processes have chaotic behaviour. It means that, the system output is predictable at an instant in any dimension provided, the initial conditions are known to us. In image encryption systems, just shuffling the pixel positions would not result in better encryption.

Hence, additional keys are included into the system, which are under chaos. These chaotic systems appear to be random is the main advantage to be used in encryption process. The tasks in image security are just not only to encrypt it but also to discourage the intruders and fool the hackers while they try to decrypt the image. In chaotic based systems, usually logistic maps are used and the lattice values are modified through several iterations and finally forms a spatio-temporal system. Since linear coupling of lattices results in easy guessing of pixels, non-linear coupling is getting popular among chaotic based encryption systems.

1.1 CHAOTIC SYSTEM

Chaotic maps are widely used in image encryption techniques to develop the secret keys. The reason behind this is that the properties of the chaotic map comprise dynamic behavior, ergodicity, sensitive towards initial conditions, and non-linear deterministic nature. Generalized logistic equation is one of the chaotic map. Therefore, it map provides good confusion and diffusion in encryption techniques. These can be used in both spatial and transform domains. Therefore, image encryption techniques are broadly classified into two categories such as spatial-domain and transform-domain based image encryption techniques. Image encryption is the process of encrypting the image with the help of some algorithm. Encryption has long been used by militaries and governments to facilitate secret communication. It is now commonly used in protecting information within many kinds of civilian systems.

In recent years there have been numerous reports of confidential data such as customers' personal records being exposed through loss or theft of laptops or backup drives. Encrypting such files at rest helps protect them should physical security measures fail. Digital rights management systems which prevent unauthorized use or reproduction of copyrighted material and protect software against reverse engineering are another somewhat different example of using encryption on data at rest.

2. PROPOSED SYSTEM

The proposed technique consists of two main phases. They are encryption phase and decryption phase.

Arnold Transform used to scramble the input image as well as to confuse (shuffle) the keys also. Generalized logistic equation is used to generate the secrete keys. NSCT is used to change the pixel values. Differential evolution is used for fine tuning of key parameter.

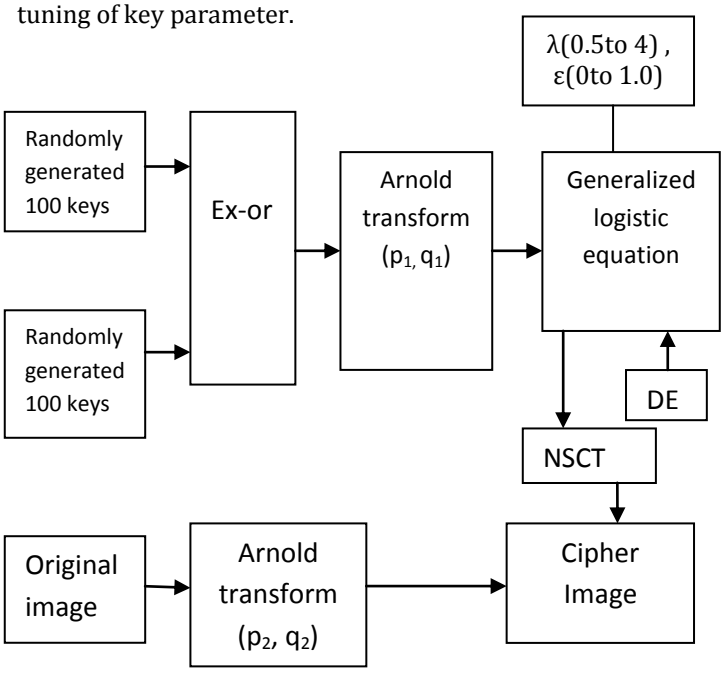

Fig-1: Block diagram of proposed system

a) **Encryption process:**

•Input RGB image is separated into three layers
•For each layer of input, the image is first permutated to vary its locations based on Arnold transform.
•Set of 200 randomly generated keys are ex-or to get 100 keys
•These keys are separated as 10×10 keys further locations are changed using Arnold transform
•Further the map is then coupled with generalized logistic map, with the iterations varying from 10 to 1000.
•Differential evolution (DE) algorithm is used for fine tuning of key space.
•Each iteration the pixel value is varied in both its location and its value using NSCT
•After adding generated secrete keys in a image inverse NSCT is taken to convert the frequency domain image in spatial domain image finally cipher image is created.

b) **Decryption process:**

•The encrypted image is decomposed using NSCT.
•The secret key is developed by applying optimistic parameters provided by differential evolution to the generalized logistic equation.
•The inverse NSCT is applied on the decrypted sub-bands to obtain an intermediate decrypted image.
•The original image can be recovered by applying the inverse of AT on D_m' g with the same number of iterations
•Finally values are permutated and hence the original image is retrieved. The key can never be predicted, as it takes several years for a processor to find it out.

A. Arnold transform

AT is a permutation method which changes the pixel positions of an image without manipulating the pixels values Apply AT on Image to generate a scrambled image (Img ′), this process is repeated for a specified number of iterations, and the number of iterations depends upon the size of an input image.

Where p_1 =12, q_1 =7 and L=100 during the diffusion phase. The determinant value of the matrix using p_1 and q_1 is found to be 1. Hence, these values are suitable to use in chaotic systems. While assuming the 100 initial lattice values in key space each of 40 bit length, it could be doubled by using the following XOR method. Hence, from the user point of view the key space consists of 200 lattices. Further, the diffusion phase is realized as follows. K_i = 1, 2…100 is initially shuffled using Arnold transform. To reach this, 100 values in a row vector is reshaped to a 2D matrix consisting of 10 rows and 10 columns then these keys is also shuffled.

$$\begin{bmatrix} j \\ k \end{bmatrix} = \begin{bmatrix} 1 & p \\ q & pq+1 \end{bmatrix} \begin{bmatrix} i \\ i \end{bmatrix} (mod\ L)$$

B. Generalized logistic equation

The generalized logistic equation is used with multiple iterations of Arnold cat map in diffusion phase in order to reduce the mutual information among the lattices. The proposed system consists of a key space of λ= 0.5 to 4 with 0.001 resolution, ε=0.0 to 1.0, p_1 =12, q_1 =7, initial lattice values K_i =1,2,…100, each of 40 bit length and K_j =1,2,…100 and additionally p_2 =12, q_2 =7 and p_3 =12, q_3 =7.

Generalized logistic equation generate secrete key x_{n+1}.

$$x_{n+1} = \frac{4\lambda^2 x_n(1-x_n)}{1+4x_n(1-z_n)(\lambda^2-1)}$$

Diffusion process is carried out by using this following equation to combine the generated keys from generalized logistic equation and shuffled keys from Arnold transform with permuted pixels to get cipher image.

$$c[i] = \left(p[i] + c[i-1] + floor\left(x_{300+i}\left(floor\left(\frac{s[m-1]}{4}+\right)\right)10^{12}\right)\right) mod256$$

C. Non-subsampled contourlet transform

NSCT is an extension of the well-known contourlet transform (CT) that has shift-invariant feature. The multiscale decomposition feature of CT is achieved by using Laplacian Pyramids. Directional filter banks (DFBs) are used to generate the directional decomposition of CT.

Non-subsampled pyramid (NSP): NSP guarantees the multiscale characteristic of NSCT. NSP depends upon two-channel non-subsampled 2D filter banks. The three-stage decomposition of NSP is described in Fig. 2

$$H0(z)G0(z) + H1(z)G1(z) = 1$$

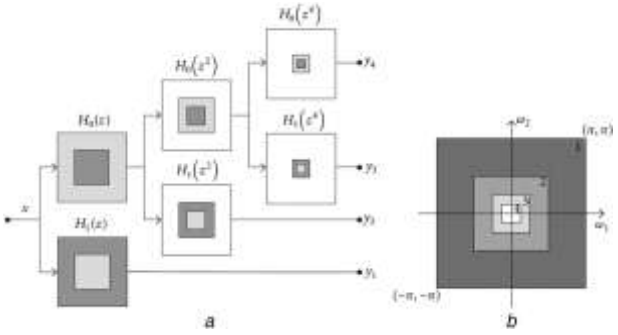

Fig-2: *Non-subsampled pyramid*

(a) Three-stage pyramid decomposition, ***(b)*** Frequency divisions of a non-subsampled pyramid

D. Differential evolution

Differential evolution is a well-known evolution-based optimisation technique. It elegantly combines the mutation and crossover operators of GA. Therefore, it has better convergence speed than standard GA [39]. It consists of five main steps. These are population initialization, mutation, recombination, selection, and stopping criteria to find optimal solutions. The steps of differential evolution are described below:

i. Population initialization: Initially, random solutions are generated whose values lie between lower and upper bound. Normal distribution is mostly used to develop the random solutions. where $f(S)$ represents the fitness of image

$$f(S) = -\sum (P(s_i) \times \log_2 P(s_i))$$

ii. Mutation: It expands the search space. In this, three distinct solutions are randomly selected for a target solution. A donor solution is generated by adding the difference of two solutions to the third solution, b_{sol_i} represents the best solution and b_{sol_i} is a target solution b_{sol_i}, mutant solution M_i is generated according to

$$M_i = b_{sol}r1 + F(b_{sol}r2 - b_{sol}r3), \qquad r1 \neq r2 \neq r3 \neq i$$

iii. Recombination: It is used to combine the successful solutions from the previous generation. It generates a trial solution from the elements of the target solution and donor solution of the mutation step. Secondly, the target solution (b_{sol_i}) is mixed with the mutated solution (M_i) to yield the trial solution (new (j)).

iv. Selection: To select the best solution, the fitness value of target solution is compared with a trial solution. The fitness value of solutions depends upon the objective function. In case of the maximization problem, if the fitness of the trial solution is more than the target solution, then it is survived for the next generation. The best known solution will be replaced with a new solution.

v. Stopping criteria: If the termination criterion is satisfied, the algorithm stops. Otherwise, steps (ii–iv) will be repeated.

1) Security analysis

i) Histogram Analysis:

Histogram analysis is one of the security analyses which tell us the statistical properties of the ciphered image. Histogram of a ciphered image tells us how pixels in an image are distributed. It is done by plotting the number of pixels against the color intensity levels. In order to have a perfect ciphered image in terms of histogram, the histogram of the image must have uniform distribution of pixels against the colour intensity value. In our proposed scheme, we see that our method leads to this uniform distribution. Thus, our scheme does not provide any room for the statistical attacks.

ii) Correlation Coefficient Analysis:

To analyse the correlation between two horizontally, vertically and diagonally adjacent pixels in the original Lena image and its various encrypted images. For the original image the adjacent pixels have high correlation (horizontally, vertically, and diagonally).

iii) Mean absolute error (MAE):

MAE measures the mean absolute difference between input and decrypted images.

$$MSE = \frac{1}{MN}\sum_{Y=1}^{M}\sum_{X=1}^{N}[I(X,Y) - I'(X,Y)]^2$$

iv)The Peak Signal to Noise Ratio (PSNR):

PSNR usually calculated in the logarithmic scale is used to evaluate the quality image. The higher value of PSNR indicates that the given image has good visual quality.

$$PSNR = 20\ log_{10}\frac{255}{\sqrt{MSE}}$$

3. SIMULATION & RESULT

The image is encrypted and decrypted using MATLAB below table shows the PSNR and MSE value for various images and figure 4 represents the cipher image.

Table -1: PSNR and MSE taken for various images having 512×512 pixel size

Image name	PSNR (Db)	MSE
Lena	134.8406	0.0906
Peppers	134.7572	0.0913
Barbara	135.9002	0.0815
Butterfly	154.4878	0.0127

Table -2: NPCR and UACI obtained in proposed method

Encryption criteria (to get 2 ciphered images)	*UACI* (%)	*NPCR* (%)
λ=3.870 and 3.871 (common K_i) (Case 1)	33.5270	99.6541
Last bit change in K_{100} (common λ) (Case 2)	33.4391	99.7402
One pixel changed (Common key) (Case 3)	33.4572	99.6114

figures

Fig -3: original image of peppers

Fig -4: Encrypted image of peppers

Fig -5: Decrypted image of peppers

4. CONCLUSION

The proposed system has a total key space of 28000. The major advantage of the proposed system stands on the reduction of mutual information of all 100% lattices. Using the generalized equation, the periodic windows are also reduced. The KS entropy density and KS entropy generality plots shows that the proposed system is well suited to be used in cloud environment. Turbulence in space- time and space-amplitude plots ensure the wide range of changes in lattice values over time and amplitude. When compared to the conventional methods, this proposal is highly robust for attacks. Moreover, the correlation values among the pixels in the encrypted image will never help the intruders to guess the original pixel values using the correlation values. The time consumed to break the key would take several years in a personal computer with memory of 4GB RAM. In order to ensure the image quality of the decrypted image, PSNR and Figure of Merit (FOM) has been calculated and found to be ∞ and 100% respectively when correct key is supplied. Hence, this method is highly suitable to store and preserve the medical images in cloud databases. Any research work naturally means an endless operation. Of course, the results obtained in any technical work could yield a nearest optimum and not global full optimum results.

REFERENCES

[1] Rim Zahmoul, Ridha Ejbali, Mourad Zaied, "Image encryption based on new Beta chaotic maps," Optics and Lasers in Engineering 96 pp.39–49, Jan. 2017

[2] Huiqing Huang, Shouzhi Yang, "Colour image encryption based on logistic mapping and double random-phase encoding," IET Image Processing, Vol. 11 Iss. 4, pp. 211-216., Jan. 2017
[3] M.Sivagami, Mr.R.Premkumar and Dr.S.Anand, "An efficient method based on crossover operator for image encryption," International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS), 2017
[4] Brindha Murugan , Ammasai Gounden Nanjappa Gounder, "Image encryption scheme based on blockbased confusion and multiple levels of diffusion,"IET Computer Vision, Vol. 10 Iss. 6, pp. 593-602, April 2016
[5] Yannick Abanda, Alain Tiedeu, "Image encryption by chaos mixing," IET Image Processing, doi: 10.1049/iet-ipr.2015.0244., may 2016
[6] MARTÍN DEL REY, G. RODRÍGUEZ S´ANCHEZ and A. DE LA VILLA CUENC, "A protocol to encrypt digital images using chaotic maps and memory cellular automata," IEEE trans. Vol. 23 No. 3, march 2015
[7] Xiaoqiang ZHANG, xuesong WANG, and yuhu CHENG, "Image encryption based on genetic algorithm and chaotic system," IEICE TRANS.COMMUN., Vol.E98-B, no.5, may 2015
[8] Prerna Dureja, Bhawna Kochhar, "Image Encryption Using Arnold's Cat Map and Logistic Map for Secure Transmission," IJCSMC, Vol. 4, Issue. 6, pg.194 – 199, June 2015
[9] Qiong Zhang, Minfen Shen, Bin Li, Ruoyu Fang, "Chaos-based Color Image Encryption Scheme in the Wavelet Domain," IEEE 7th International Congress on Image and Signal Processing, 2014
[10] A. K. Qin, V. L. Huang, and P. N. Suganthan, "Differential Evolution Algorithm With Strategy Adaptation for Global Numerical Optimization," IEEE Transactions on evolutionary computation, VOL. 13, NO. 2, April 2009.