KEYLESS IMAGE ENCRYPTION APPROACH FOR SECURED TRANSMISSION OF IMAGES

[1]Chetana Singh, [2]Binay Kumar Pandey, [3]Dr. H.L.Mandoria, Ashok Kumar
[1]M.Tech Student, [2]Assistant Professor, [3]Head and Professor, Assistant Professor
[1]Information Technology, G.B.Pant University of Agriculture and Technology, India
[2]Information Technology, G.B.Pant University of Agriculture and Technology, India
[3]Information Technology, G.B.Pant University of Agriculture and Technology, India

Abstract : In current years, the chaos based totally cryptographic algorithms have recommended some new and effective approaches to ameliorate impervious image encryption methods. In this communication, we introduced a advance image encryption strategy, which is totally based on modified cat map using 802.11 a/g in WSN. For impenetrable transmission of image, image is metamorphose in the coded form using encryption of images. Because image send over public domain is invulnerable is major concern. In this introduced encryption procedure, firstly image is encrypted through the modified cat map, then it is metamorphose into linear array, after that image information modulated and demodulated using OQPSK then using decryption it back again into its authentic format. The outcomes of several experimental, statistical analysis, histogram examination show that this proposed image encryption scheme offers an efficient and secure way for real -time image encryption and transmission.

***Keyword* - Chaotic Map, Chaos Theory, Cat map**

I. INTRODUCTION

With the fast enhancement of computer network technology, a lot of delicate records are given to the public domain. Data protection becomes greater and greater importance. Information about image devolution has accelerated hastily and encryption of image method has drawn greater attention [1]. Encryption of image is distinctive from the encryption of text due to some inherent aspect such as bulk information ability and excessive correlation amongst pixels. Therefore, traditional cryptographic techniques such as DES, IDES, and RSA are no longer appropriate for encryption of image. The competence of the chaotic maps such as sensibility to preliminary prerequisites and random-like behavior have interested the attention to increase algorithms of image encryption. Method of Image encryption group into three instructions they are: Transformation of values, Permutation of position, and transformation of visual. In our proposed work main concern is to transmit image information into the invulnerable network. So for invulnerable information transmission, improvised Arnold's cat map using 802.11a/g is proposed having PSNR value between 94 and MSE between the input image and encrypted image is 0.0866.

II. **Arnold's Cat Map (ACM)**

Arnold's cat map is a chaotic mapping, discovered by a Russian mathematician "Vladimir I. Arnold". He discovered this algorithm using image of cat. According to Arnold's transformation, an image is hit with the transformation which is used to change the pixel position of image without the removal of any information from that image. However, if iterated several times, finally original image recurs. Number of iterations required are known as Arnold's period. The period depends on size of image i.e., for dissimilarimages in size, Arnold's period will be different[2].Following is Arnold's Cat Map equation:

$$\begin{bmatrix}x_{n+1}\\ y_{n+1}\end{bmatrix} = A\begin{bmatrix}x_n\\ y_n\end{bmatrix}(mod\ N) = \begin{bmatrix}1 & p\\ q & pq+1\end{bmatrix}\begin{bmatrix}x_n\\ y_n\end{bmatrix}(mod\ N)$$

Where N = Size of image,p and q = Positive integers,det (A) = 1 ,(x_n, y_n) = Position of pixels in image,(x_{n+1}, y_{n+1}) = Transformed position.

III. RELATED WORK

Several image encryption and decryption algorithm introduced for invulnerable information transmission in network. Some of them are: *Wang et al.* [2] have proposed 3-D cat map. In this approach firstly shuffled the image and afterward ,diffuse that image by proposed method. parameter of Sensitivity is firstly analyzed by *Lian et al.* [3] for a typical chaotic map, and there after typical chaotic transformation is compared with cat map and baker map. Logistic map and a permutation of the position are used for decryption of image by in this method. *Wang et al.* [4] combine perception model with Lorenz map. For color image encryption, it uses logistic transformation. Drawback of *Wang's* algorithm is that if one bit change in the input image the ciphered image is also changed by one bit. Using Baker Map *Alvarez et al.* [5] have proposed basic guidelines for protection of information. By swapping pixel values Chen et al. have proposed 3D map for confusion and diffusion. It overcomes the weakness of chosen or known plaintext image. Combination of Chen map and Arnold cat map is proposed by Guan et al. [6].

In this paper rest of the work described in section III, Section IV and Section V. Section III describes algorithm of proposed work .Simulation and result of this paper shows in Section IV and conclusion in Section V.

IV. PROPOSED ALGORITHM

Steps of Proposed System

A) Encryption algorithm

```
Step 1: Read the input image
Step 2: Convert the RGB image to gray scale
Step 3: loop through rows
Step 4: loop through columns
Step 5: pixelvalues ←  image(i,j)
Step 6: newpixelvalue ←  (pixelvalue + i^ columns)/256
Step 7: tImage(I,j) ←  newpixelvalue
Step 8: end row loop
Step 9: end column loop
Step 10: Convert image to linear form
Step 11: Modulate image data using OQPSK
Step 12: Transmit packet
```

B) Decryption algorithm:

```
Step 1: Convert packet into one.
Step 2: Demodulate the data.
Step 3: Reconstruct the image.
Step 4: Retrieve image reversing step 4 to step 10 of encryption.
```

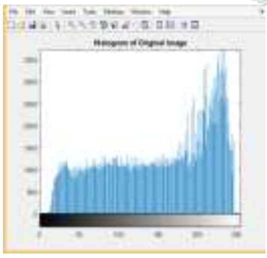
4.1 STATISTICAL ANALYSIS

It is properly identified that many ciphers have been correctly analyzed with the help of statistical evaluation and numerous statistical attacks have been devised on them. Therefore, an perfect cipher should be robust against any statistical attack. To demonstrate the robustness of the proposed image encryption procedure, we have performed statistical analysis by calculating the histograms of the input image, encrypted image and acquired image.

4.1.1. HISTOGRAM ANALYSIS

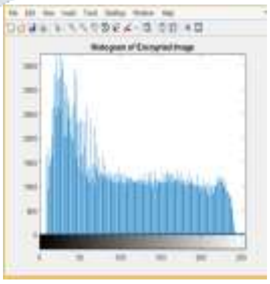
An image-histogram illustrates how pixels in an image are disbursed by way of graphing the number of pixels at each color intensity level. We have calculated and analyzed the histograms of the numerous encrypted as well as its original colored images that have widely different content. One example of such histogram analysis is shown in Fig. 1. As we can see, the pixel distribution of the cipher images is fairly uniform, which can greatly reduce the correlation between the pixel.

(a)

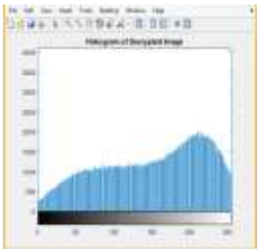


(b)

(c)



(d)



(e)

Figure 1:(a) original image,(b)Histogram of original image,(c)Cipher image by proposed algorithm,(d)Histogram of cipher image,(e)histogram of decrypt image

4.1.2 SENSITIVITY ANALYSIS

A good encryption algorithm should be sensitive to the plain image.

4.1.2.1 Plain image sensitivity

For calculation of the number of pixel change rate(NPCR)and unified average changing intensity(UACI),let us assume two cipher images C1 and C2 whose corresponding plain images have only one pixel difference. NPCR and UACI are defined through the following formula as:

$$NPCR = \frac{\sum_{i=1}^{M} \sum_{j=1}^{N} D(i,j)}{T} \times 100\%$$

$$UACI = \left[\sum_{i} \sum_{j} \frac{|Ior(i,j) - Ienc(i,j)}{L.T} \right] \times 100\%$$

The symbols T and L denote the number of pixels in the cipher image and the largest allowed pixel intensity, respectively. D(i,j) is defined as:

$$D(i,j) = \begin{cases} 0 & Ior(i,j) = Ienc(i,j) \\ 1 & Ior(i,j) \neq Ienc(i,j) \end{cases}$$

Table 1 shows the real values of NPCR and UACI of cipher images by changing a pixel of plain image.

Table 1: Comparison of NPCR and UACI of cipher image by changing a pixel of plain image

Image	Method	NPCR%	UACI%
Aisle	Proposed system Hua et al.	98.433380 94.623107	33.463541 31.463145
Building	Proposed system Hua et al.	98.430480 93.622414	33.463541 31.472513
Cars	Proposed system Hua et al.	98.442687 93.60	33.463541 31.48

V. CONCLUSION

In this paper, we proposed a new encryption algorithm based on cat map. The experimental results showed that the proposed approach yields a better encryption performance compared to existing algorithm. These comparisons were based on histogram, NPCR,UACI.

For future works we can study in detail the strength of the cat map matrix genration and check its effort on the final results in encryption and decryption.

REFERENCES

[1] A. J. Paul, P. Mythili, and K. Paulose Jacob, “Matrix based cryptographic procedure for efficient image encryption,” in Proceedings of the IEEE Recent Advances in Intelligent Computational Systems (RAICS ’11), pp. 173–177, 2011.

[2] K. Wang, W. Pei, L. Zou, A. Song, and Z. He, “On the security of 3D Cat map based symmetric image encryption scheme,” Physics Letters A, vol. 343, no. 6, pp. 432–439, 2005.

[3] Lian S, Sun J, and Wang Z. " A block cipher based on a suitable use of the chaotic standard map. Chaos, Solitons & Fractals.", vol.26(1), pp.117–29,2005.

[4] Wang X, Teng L, and Qin X. "A novel colour image encryption algorithm based on chaos. Signal Processing." Vol.92(4), pp.1101–8, 2012

[5] Alvarez G, and Li S. "Breaking an encryption scheme based on chaotic baker map. Physics Letters A.,vol352(1),pp.78–82. 2006

[6] Guan Z-H, Huang F, and Guan W. "Chaos-based image encryption algorithm" Physics Letters A., vol.346(1), pp.153–7, 2005

[7] Xiao D, Liao X, Wei P." Analysis and improvement of a chaos-based image encryption algorithm" Chaos, Solitons & Fractals.vol. 40(5),pp.2191–9, 2009.

[8] Fu C, Lin B-B, Miao Y-S, Liu X, Chen J-J. A novel chaos-based bit-level permutation scheme for digital image encryption. Opt Commun. vol.284(23),pp.5415–23, 2011.

[9] Wu Y, Agaian S, Noonan JP. A new family of generalized 3D cat maps. ArXiv preprint. ArXiv: 12053208. 2012.

[10] P. Meenakshi,* and D. Manivannan, "An Efficient Three Layer Image Security Scheme using 3D Arnold Cat Map and Sudoku Matrix:

[11] P. Tian-Gong and L. Da-Yong, "A novel image encryption using arnold cat," International Journal of Security and Its Applications, vol. 7, no. 5, pp. 377–386, 2013.

[12] V. Patidar, N. K. Pareek, G. Purohit, and K. K. Sud, "A robust and secure chaotic standard map based pseudorandom permutation-substitution scheme for image encryption," Optics Communications, vol. 284, no. 19, pp. 4331–4339, 2011.

[13] H. S. Kwok and W. K. S. Tang, "A fast image encryption system based on chaotic maps with finite precision representation," Chaos, Solitons & Fractals, vol. 32, no. 4, pp. 1518–1529, 2007.

[14] V. K. Kushwaha and K. Anusudha, "Based double encryption approach for secure transaction of medical images," International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, vol. 2, no. 4, pp. 1418–1423, 2013.

[15] M. Ahmad and T. Ahmad, "A framework to protect patient digital medical imagery for secure tele diagnosis," Procedia Engineering, vol. 38, pp. 1055–1066, 2012.

[16] A. Al-Haj, G. Abandah, and N. Hussein, "Crypto based algorithms for secured medical image transmission," IET Information Security, vol. 9, no. 6, article 365, 2015.

[17] F. Cao, H. K. Huang, and X. Q. Zhou, "Medical image security in a HIPAA mandated PACS environment," Computerized Medical Imaging and Graphics, vol. 27, no. 2-3, pp. 185–196, 2003.