Original Article

IJCIH
Converging Healthcare & Technology

International Journal of Convergence in Healthcare

Published by
IJCIH & Pratyaksh Medicare LLP

www.ijcih.com

An Optimized Image Encryption Scheme, Leveraging the Arnold Transform and Chaotic Map

Bhavana Sharma[1], Hukm Singh[2], Mehak Khurana[3]

[1]PhD Scholar, Department of Computer Science and Engineering, The NorthCap University, Gurugram, India, [2]Professor, Department of Applied Sciences, The NorthCap University, Gurugram, India, [3]Assistant Professor, Department of Computer Science and Engineering, The NorthCap University, Gurugram, India

Abstract

The traditional approach to image encryption faces significant challenges and issues, including inadequate safety, image degradation, low latency, low-key sensitivity, diffusion, and strong correlation. To address these shortcomings, a new image encryption algorithm is proposed in this work. The algorithm uses a combination of Discrete Cosine Transform (DCT) and Arnold transform along with chaotic scrambling to enhance the image security. The two-level encryption approach performs transformations in the position of each pixel without changing their values or statistical features. The proposed algorithm is evaluated and shown to offer several advantages, including robust performance, statistical efficacy, high key sensitivity, picture security, and real-time performance. Overall, the proposed algorithm represents a significant improvement over the traditional approach to image encryption.

Keywords: *Discrete cosine transform, Chaotic Map, Arnold Transform.*

Introduction

Communication and transmission of multimedia are encouraged by the rapid growth of networks. As one of the most important data carriers, multimedia contains a tremendous amount of visually rich content. Since multimedia is important in many situations and has many applications, it is vulnerable to being intercepted and changed while being transmitted via public information networks. Therefore, despite numerous attacks on security and privacy, the assurance of security and privacy in a picture is of the utmost importance in today's digital world. Afterward, it is noted through a review of the literature that image encryption is a process through which digital images can be securely protected using several methods. To prevent the real image data from being instantly deciphered, image encryption employs a hidden key and encryption feature, encrypted image is and then decryption is performed to reveal the original image. The conventional methods of picture encryption like DES, AES, and IDEA have been replaced by countless more ways that have since been developed. The encryption of digital image is based on the combination of the two properties pixel scrambling and transformation matrices. Image scrambling only modifies a pixel's position, having no effect over the pixel value or numerical characteristics[1] ·Because just using grey picture prevents the smallest change in cipher-text pixel from having an impact on all cipher-text pixels, multiple rounds of encryption are required to scramble the grey image in the image

Corresponding Author:
Bhavana Sharma
Department of Computer Science and Engineering, The NorthCap University Gurugram, India
e-mail: bhavanasharma@ncuindia.edu

encryption technique [2]. Some of the related literature work have been discussed here, An Improved Image Encryption Algorithm Using DCT and Arnold Transform by N. Niu et al. (2019): The authors proposed an image encryption scheme that uses a combination of DCT, Arnold transform, and logistic map key. The algorithm is designed to provide high security, fast encryption, and low computational cost. The results of the experiments demonstrated that the suggested algorithm performed better than other existing algorithms in terms of encryption speed and security [3]. An Effective Image Encryption Scheme Using DCT and Arnold Transform by S. Kumar et al. (2020): In this paper, the authors presented an image encryption scheme based on the DCT and Arnold transform along with logistic map key. The proposed algorithm offers high security, low computational cost, and robustness against various attacks[4]. A secure image encryption approach using DCT and Arnold Transform by S. Islam et al. (2018): The authors proposed an image encryption algorithm that uses the DCT and Arnold transform along with a chaotic map-based key generation scheme. The proposed algorithm provides high security and fast encryption speed. The experimental findings demonstrated that, in comparison to other current algorithms, the suggested method is more resistant to a variety of attacks[5]. A novel approach of DCT using chaotic map scrambling by K. Ahmad et al. (2019): The authors described a method for encrypting images that relies on the logistic map key, the DCT, and the Arnold transform. The suggested approach provides good security at a cheap cost of computation. The experimental findings demonstrated that, in comparison to other current algorithms, the suggested method is more resistant to a variety of attacks[6] . Image Encryption Using DCT and Arnold Transform with Logistic Map Key by S. S. Gade and S. R. Wagh (2018): The authors proposed an image encryption scheme that uses the DCT and Arnold transform along with a logistic map key. The suggested technique offers strong security at a cheap cost of computation. The experimental findings demonstrated that, in comparison to other current algorithms, the suggested method is more resistant to a variety of attacks [7]. In conclusion, DCT and Arnold transform along with logistic map key have been widely used in the literature for image encryption. These algorithms offer high security, fast encryption speed, and low computational cost. In terms of encryption speed and security, the experimental findings demonstrated that the suggested algorithms perform better than other current methods[8].

Related Work

Arnold Transform: A technique that scrambles digital images is frequently employed to address image security concerns[9]. To secure an image from outside influences, it is necessary to scramble the pixels in the original image in this transition, although quick and easy, results in a great number of textural features in the image. This type of scrambling is used to produce row-by-row visual sequences. Despite good randomization, the textural qualities are barely discernible. Instead, iterating through numerous rounds of scrambling algorithms is costly and time-consuming. One of the scrambling methods is Arnold Transform, it is a mathematical transform that preserves the area of a two-dimensional plane while mapping it onto itself [10]. Four parameters that affect the behavior of the map are used in a set of equations that specify the transformation. It is one among the most widely used algorithms for scrambling that combines control parameters with the Arnold function, that strengthens the scrambling algorithm[11]. The equation (1) shows the mathematical representation of Arnold transform.

$$\binom{a'}{b'} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \binom{a}{b} \bmod 1. \tag{1}$$

Where a and b are the scrambling equation's control parameters. The picture pixel position is (x, y). N is the order of digital image matrix.

$$\binom{a'}{b'} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \binom{a}{b} \bmod N \tag{2}$$

Discrete Cosine Transform: The Discrete Cosine Transform (DCT) is a mathematical technique used in signal processing, image compression, and other applications to transform a signal or image from the spatial domain to the frequency domain[12]. The formula for the DCT is shown in equation (3)

$$X_k = \sqrt{\frac{2}{N}} C_k \sum_{n=0}^{n-1} X_n \cos\left(\frac{\Pi}{n}\left(n + \frac{1}{2}\right) k\right) \tag{3}$$

where X_k is the DCT coefficient at frequency index k, x_n is the original signal or image sample at time or spatial index n, and n is the length of signal or image. C_k is a scaling factor given by equation (4).

$$C_{k=} \begin{cases} \frac{1}{2} & \frac{k=0}{k>0} \\ 1 & \end{cases} \tag{4}$$

The DCT formula calculates the cosine transform of a finite sequence of N real-valued numbers, producing a sequence of N real-valued DCT coefficients. The DCT can be envisioned as a means to aggregate cosine functions with various frequencies and amplitudes in order to represent the original signal or image[13].There are several variants of the DCT, with the most common being the DCT-II (used in JPEG compression) and the DCT-IV (used in MPEG compression)[12].

Logistic Map: A computer model called the logistic map is used to analyze population increase in environments with constrained resources. It is a nonlinear difference equation that, depending on the parameter values, displays chaotic behavior [14]. The formula for the logistic map is stated in equation (5).

$$x_{n+1} = rx_n(1 - x_n) \tag{5}$$

where Xn represents the population size at time n and r controls the rate of population growth. The logistic map equation is recursive, therefore the value of x+1 depends on the value of X_n from the previous step [15].The discrete-time dynamical system known as the logistic map exhibits a variety of behaviours depending on the value of the r parameter. The population size reaches a stable equilibrium value for low values of r. The population of the system oscillates between two values as r rises, resulting in a period-doubling cascade. When r reaches a certain critical value, the system transitions into chaos, and the population size changes in an unpredictable and seemingly random way. The logistic map is a crucial model in the study of nonlinear dynamics and chaos theory, and it has practical uses in physics, population ecology, and economics[15]. The Figure 1 depicts the progression of different initial conditions as a function of r.

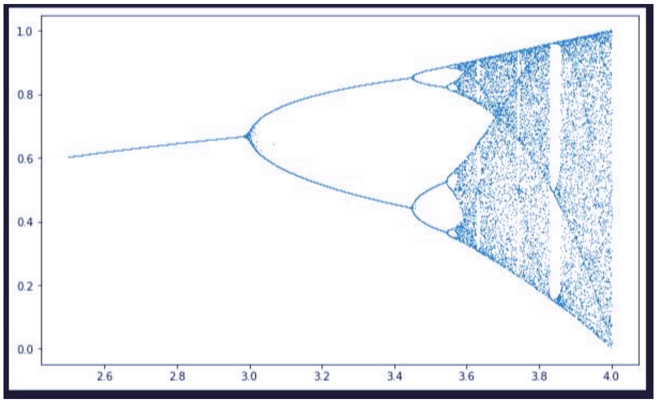


Fig. 1. Logistic Map

The Proposed Cryptosystem: The encryption process of the proposed algorithm is divided into three parts. Firstly, the input image is multiplied with random phase mask, followed by DCT transform along with Arnold transform is applied and then key generation using Logistic map of chaotic maps [16].

3.1 Encryption and Decryption Steps

The process of encryption is discussed below:

Step 1: The input image $I_{x,y}$ first multiplied with the random phase mask as shown in equation 6.

$$I_1 = I \otimes RPM_1 \tag{6}$$

where RPM1 = exp ($2\pi i$ * v(x, y)) and v(x, y) is any random matrix having size as that of the input image

Step 2: The DCT transform is performed on I_1, followed by Arnold transform as shown in equation 7.

$$I_2 = AT[DCT[I_1]] \tag{7}$$

Step 3: In this step, the chaotic logistic map is iterated for (v* r+S) times to generate a random sequence of X and Y having (v*r)/2+S elements in each I2 is multiplied with the logistic key (LK) of chaotic maps as shown in equation 8.

$$I_3 = I_2 \otimes LK \tag{8}$$

Step 4: Apply IDCT on I_3 and result is stored as I_4 Mathematically Step 4 is described in equation (9).

$$I_4 = IDCT[I_3] \tag{9}$$

Step 5: I_4 is the final cipher text image.

The decryption process of proposed algorithm is discussed as follow:

Step 1: The cipher text image I_4 obtained during the encryption process is bonded with the inverse private key (LK) generated using the process of logistic key mapping explained above, mathematical results are stored in equation 10, as shown below

$$D_1 = [I_4 \otimes ILK] \tag{10}$$

Step 2: Now the DCT is performed on $D_{1,}$ and results are stored in D_2 as shown in equation (11).

$$D_2 = DCT[D_1] \tag{11}$$

Step 3: In this step, we perform inverse of Arnold transform on D_2 and store the results in image D_3 as shown in equation 12.

$$D_3 = IAT[D_2] \tag{12}$$

Step 4: Obtained result is the retrieved image D_3, the complete steps of decryption process are diagrammatically shown in figure 2.

$$D_{4\,=}\,D_3 \otimes RPM^* \tag{13}$$

Step 5: The output obtained in equation 13 is propagated through inverse discrete cosine transform to get the final decrypted image, mathematical results shown in equation 14.

$$D_5 = IDCT[D_4] \tag{14}$$

Figure 2(a), 2(b) shows the flow chart of the proposed encryption and decryption schemes.

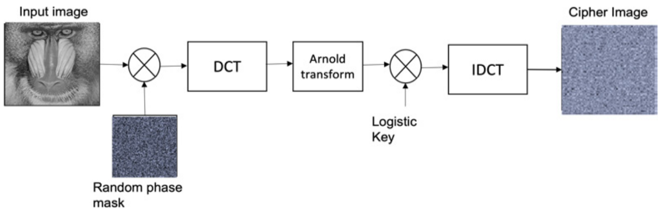


Fig. 2(a) Proposed encryption algorithm

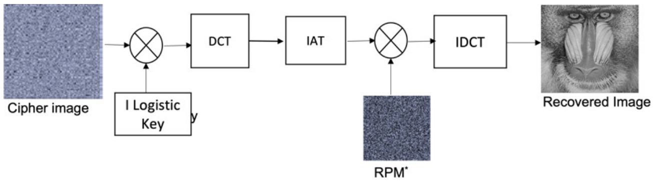


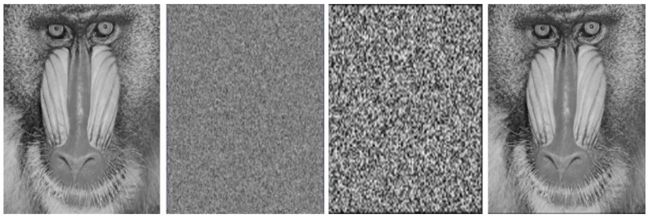
Fig. 2(b) Proposed decryption algorithm

Performance Analysis and Result

The input greyscale images with parameters as shown in table 1 are used to evaluate the algorithm's efficacy. Two quality evaluation metrics were utilized to compare the original image with the encrypted image as can be seen in table 2, the low MSSIM score and high PSNR score point to a significant degree of dissimilarity between the two images. As the PSNR increase, the performance of the encryption algorithm improves. It is clearly displayed in the Table 2, the PSNR, MSSIM, MSE, Entropy of different images.

Table 1. Showing the Details of Input Images Used in the experiment along with results.

Sno.	Image	Type	Dimensions
1.	Baboon	tiff	256x256
2	Cameraman	tiff	256x256
3	Lena	tiff	259x194
4	Onion	tiff	300x168
5	Barbara	tiff	250x250



PSNR: The peak signal to noise ratio (PSNR) serves as a barometer for similarity in visual perception. The more similar the image is to the decrypted image, the higher its PSNR value[16].The formula of PSNR is shown in equation (15)

$$PSNR = 10log10\left(\frac{255\times255}{MSE}\right) \tag{15}$$

MSE: Measuring the average squared difference between anticipated and actual values in a dataset is done using the metric known as MSE or mean squared error[17.] The formula of MSE is shown in equation 16.

$$MSE = \frac{1}{M\times N}\sum_{i=0}^{m}\sum_{j=0}^{n}\left(I\,(i,j) - I\,(i,j)\right)^2 \tag{16}$$

SSIM: An indicator of the similarity of visual perception is the image similarity index (SSIM). The more similar the SSIM image is to the decoded image, the higher its value[18]. The formula of SSIM is stated in equation 17.

$$SSIM_{(x,y)} = \frac{(2\mu_x\mu_y+c_1)(2\sigma_{xy}+c_2)}{(\mu_x^2+\mu_y^2+c_1)(\sigma_x^2+\sigma_y^2+c_2)} \tag{17}$$

ENTROPY: Entropy refers to the average of the information and generally refers to the measure of unpredictability of a system[19]. Table 2 shows the entropy of the encrypted data using the previously given reference to the measure of unpredictability of a system. Table 2 shows the entropy of the encrypted data using the previously given formula in equation 18.

$$H(s) = -\sum_{i=1}^{N} P(s_i)\log_2 P(s_i) \tag{18}$$

Where P(Si) is the probability of S_i and H(s) is the entropy.

Table 2. Showing PSNR, MSE, SSIM, Entropy of the images.

Lena, Onion, Cameraman, Baboon, Barbara

Sno	Image	PSN(Db)	MSE	SSIM	Entropy
1.	Lena	53.7881	0.2718	0.99999642	7.4462
2	Onion	55.2607	0.1934	0.99999267	7.6245
3	Cameraman	53.7132	0. 2765	0.99999647	7.0097
4	Baboon	53.5687	0.2858	0.99999597	7.3583
5	Barbara	54.0180	0.2577	0.99999549	7.6321

Histogram Analysis: The histogram for comparison of the original image with the encrypted image is also presented in Fig. 4 for Barbara similarly for other images Lena, Onion, Baboon, Cameraman respectively. It can be observed that the histogram for all the input images (a-h), the pixels are unevenly distributed whereas in the histogram of encrypted images (e-h), the pixels are uniformly distributed, so it cannot reveal the original image[20,21].

Conclusion

In this paper a superior encryption approach is proposed that is focused on scrambling and employs the Arnold transform along with the logistic map, and the DCT transformation phenomenon. These encryption techniques are offered to address the issue of the weak functioning of the scrambling encryption method in the space phenomena. Image encryption techniques usually combine many rounds of encryption with image scrambling and encryption to boost image security.

Since real-time efficacy is high and encryption time is short, it can meet the demand for real-time secure encryption and decryption and withstand a variety of attacks because the association between neighboring pixel points is weak and the pixel grey distribution is consistent.

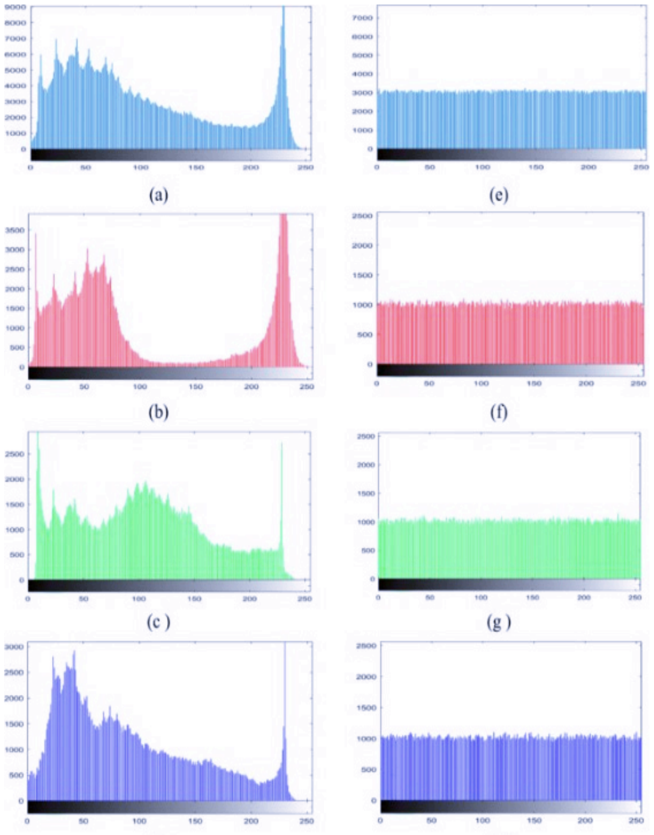
Conflicts of Interest: The authors report no conflicts of interest. The authors alone are responsible for the content and writing of this article.

Funding Statement: This manuscript does not receive any financial support.

Data Availablity Staement: Data sharing is not available for this manuscript unless requested by the editor or reviewers.

Ethical Clearance

1. This material is the authors' own original work, which has not been previously published elsewhere.
2. The paper is not currently being considered for publication elsewhere.



(a) (e)

(b) (f)

(c) (g)

Fig. 4 Histogram plots of a-d input image, d-h cipher image of Lena, Onion, Baboon and Cameraman respectively

References

1. Assad SE, Farajallah M. A new chaos-based

image encryption system. Signal Processing Image Communication. 2016; 41:144–57.

2. Chai X, Chen Y, Broyde L. A novel chaos-based image encryption algorithm using DNA sequence operations. Opt Lasers Eng [Internet]. 2017; 88:197–213. Available from: http://dx.doi.org/10.1016/j.optlaseng.2016.08.009
3. Niu N, Li Y, Liu X, Tian Y, Guo Y, Wei X. "An Improved Image Encryption Algorithm Using DCT and Arnold Transform," IEEE Access. 2019; 7:25065–76.
4. Kumar S, Singh SK, Bedi SS. An Efficient Image Encryption Scheme Using DCT and Arnold Transform. International Journal of Advanced Science and Technology. 2020;29(6):785–98.
5. Islam S, Ali M, Karim MA. A Novel Image Encryption Scheme Using DCT and Arnold Transform. Journal of Ambient Intelligence and Humanized Computing. 2018;9(4):1257–65.
6. K. Ahmad, M. Ahmad, F. Tariq, and M. Alghathbar, "A Secure Image Encryption Algorithm Using DCT and Arnold Transform," Journal of Ambient Intelligence and Humanized Computing, vol. 10, no. 10, pp. 4353-4363, 2019.
7. R. S. Gade, S S Wagh. Image Encryption Using DCT and Arnold Transform with Logistic Map Key. International Journal of Advanced Research in Computer Science. 2018;9(3):61–7
8. Chang C-C, Hwang M-S, Chen T-S. A new encryption algorithm for image cryptosystems. J Syst Softw [Internet]. 2001;58(2):83–91. Available from: http://dx.doi.org/10.1016/s0164-1212(01)00029-2
9. C.Fu C, Wen Z kao, Zhu Z liang, Yu H. A security improved image encryption scheme based on chaotic Baker map and hyperchaotic Lorenz system. International Journal of Computational Science and Engineering. 2016;12(2/3):113.
10. Khurana M, Singh H. Asymmetric image cryptosystem based on chaotic zone plate phase mask and Arnold transform. In: Lecture Notes on Data Engineering and Communications Technologies. Singapore: Springer Singapore; 2022. p. 45–51.
11. Dey S, Ghosh R. A review of cryptographic properties of S-boxes with generation and analysis of crypto secure S-boxes. [Internet]. PeerJ; 2018 Jan [cited 2023 May 2]. Available from: http://dx.doi.org/10.7287/peerj.preprints.26452v1
12. Khurana, M., Singh, H. Two level phase retrieval in fractional Hartley domain for secure image encryption and authentication using digital signatures. Multimed Tools Appl 79, 13967–13986 (2020). https://doi.org/10.1007/s11042-020-08658-3.
13. Zhang Q, Yang LT, Liu X, Chen Z, Li P. A Tucker Deep Computation Model for Mobile Multimedia Feature Learning. ACM Transactions on Multimedia Computing, Communications, and Applications. 2017 Aug 10;13(3s):1–18.
14. Rahim R, Hariyanto E. Arnold's Cat Map Algorithm in Digital Image Encryption. International Journal of Science and Research (IJSR). 2016 Oct 5;5(10):1363–5.
15. Li-Chin, Huang, Min-Shiang, Hwang, Lin-Yu, Tseng. Reversible Data Hiding for Medical Images in Cloud Computing Environments Based on Chaotic Hénon Map. In: Journal of Electronic Science and Technology, vol 11, no 2, pp 2013. 2013. p. 230–6.
16. Yin S, Liu J, Li H, Teng L. A density-based clustering method for K-anonymity privacy protection. Journal of Information Hiding and Multimedia Signal Processing. 2017 Jan;8:12–8.
17. L. Liu and Z. Cao, "Analysis of two con dentiality-preserving image search schemes based on additive homomorphic encryption," *Interna- tional Journal of Electronics and Information Engineering*, vol. 5, no. 1, pp. 1–5, 2016.
18. Rajendran S, Doraipandian M. Chaotic map based random image steganography using LSB technique. International Journal of Network Security. 2017 Jul;19:593–8.
19. Ye G, Huang X. An efficient symmetric image encryption algorithm based on an intertwining logistic map. Neurocomputing. 2017 Apr 14;251:45–53.
20. Li HY, Li HF, Wei KB, Yin SL, Zhao C. A multi-keyword search algorithm based on polynomial function and safety inner-product method in secure cloud environment. Journal of Information Hiding and Multimedia Signal Processing. 2017 Jan;8(2):413–22.
21. Sharma H, Khatri N. An Image Encryption Scheme Using Chaotic Sequence for Pixel Scrambling and DFrFT. In: Proceedings of First International

Conference on Smart System, Innovations and Computing [Internet]. Singapore: Springer Singapore; 2018 [cited 2023 May 2]. p. 487–93. Available from: http://dx.doi.org/10.1007/978-981-10-5828-8_46

22. Ye G, Huang X. An efficient symmetric image encryption algorithm based on an intertwining logistic map. Neurocomputing. 2017 Apr 14;251:45–53.

23. Yin S, Liu J. A K-means approach for map-reduce model and social network privacy protection. Journal of Information Hiding and Multimedia Signal Processing. 2016 Nov;7:1215–21.

24. Zhang Q, Yang LT, Liu X, Chen Z, Li P. A Tucker Deep Computation Model for Mobile Multimedia Feature Learning. ACM Transactions on Multimedia Computing, Communications, and Applications. 2017 Aug 10;13(3s):1–18.