IJNRD.ORG ISSN : 2456-4184

INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG

An International Open Access, Peer-reviewed, Refereed Journal

EXPEDITION OF CHAOS DRIVEN FACSIMILE USING DYNAMIC APPROACH

[1]Asst. Prof A. Radha, [2]P. Anusha, [3]K. Harish, [4]B. Yuva Kishore, [5]M. Hemasundhar

[1]Assistant Professor, [2, 3, 4, 5] Scholar

Department of Electronics and Communication Engineering

[1, 2, 3, 4, 5] UCEN JNTUK, AP, India

Abstract : The protection of data is a major concern in recent times. Many image encryption techniques have been prevailing in recent times. Among them, the most efficient is the chaotic maps technique which resembles the diffusion and perplexity properties. The Logistic Maps in chaos system is a high-speed technique and the best against brute force attacks. In this method, the logistic mathematical equation with a dynamic key is used for encrypting the Image. Image encryption can be built efficiently by logistic mapping with serial XOR operation as uncertain and random features of the chaos method increase the confidentiality of the information. Also, comparisons have been made between Logistic maps and Arnold cat map, for both standard and real-time images based on various parameters such as Number of Pixels Change Rate, Unified Average Change in Intensity, Information Entropy, Structural Similarity Index Measure, Naturalness Image Quality Evaluator. The memory utilization and execution time have been decreased compared to the other chaotic maps.

***IndexTerms* - Chaos logistic maps, Correlation.**

I. Introduction

Numerous ways for encryption of data have been discovered as time ticks away, starting with basic ideas of altering the places of letters throughout to very high and intricate mathematical calculations to lay out the element of protection to our important data. There has been tremendous interest in learning the behavior of chaotic systems. They are identified by the sensitive dependence on the initial conditions.

As the complexity increases automatically the cryptosystem becomes highly resistant to different attacks. Chaos-based cryptography has drawn the attention of researchers as the pseudorandom sequences produced by such nonlinear chaotic systems are hard to understand and anticipate because of their structural complexity.

Web 2.0 plays a crucial role in transferring bulk amounts of data in abundant fields. Some data transmitted through channels from sender to receiver many remain insecure. Private and public sectors use distinct techniques and methods to secure important data from external attacks. Cryptography sails as the best and most prominent technique to provide safety to data from external attacks using two main processes: Encryption and Decryption. Encryption is the process of encoding data to prevent external attackers from reading the original data easily. This stage can convert the user data into a random format known as Cipher text.

The next process to be done by the user is Decryption. Decryption is a contrasting element to encryption. It is the process to convert cipher text into plain text without missing any words in the original text. To perform this process cryptography relies on mathematical calculations along with some substitutions and permutations with or without a key. Modern cryptography provides confidentiality, integrity, nonrepudiation, and authentication.

II. Literature review

"An image encryption method based on chaos system and AES algorithm" [1], this paper introduces a novel algorithm for encrypting images, which utilizes a combination of a chaos sequence and a modified AES algorithm. In this method, the encryption key is generated by the Arnold chaos sequence. Then, the original image is encrypted using the modified AES algorithm and by implementing the round keys produced by the chaos system. The proposed approach reduces the time complexity of the algorithm and also adds the diffusion ability to the proposed algorithm, which makes the encrypted images by the proposed algorithm resistant to differential attacks. The proposed method possesses a key space that is sufficiently large to withstand brute-force attacks. This method is so sensitive to the initial values and input image that small changes in these values can lead to significant changes in the encrypted image. Using statistical analyses, we show that this approach can protect the image against statistical attacks. The entropy test results illustrate that the entropy values are close to the ideal, and hence, the proposed algorithm is secure against entropy attacks.

"A simple, sensitive and secure image encryption algorithm based on a hyper-chaotic system with only one round diffusion process" [2], the advantages of this proposed approach are that it can be realized easily in one round diffusion process and is computationally very simple while attaining high-security level, high key sensitivity, high plaintext sensitivity, and other properties simultaneously. The key stream generated by the hyper-chaotic system is related to the original image. Moreover, to encrypt each pixel, we use the sum of the pixels which is located after that pixel. The algorithm uses different summations when encrypting different input images (even with the same sequence based on a hyper-chaotic system). This, in turn, will considerably enhance the cryptosystem resistance against known/chosen plaintext and differential attacks. The change rate of the number of pixels in the cipher-image when only one pixel of the original image is modified (NPCR) and the Unified Average Changing Intensity (UACI) is already very high (NPCR > 99.80233 % and UACI > 33.55484 %).

"A chaotic block cipher algorithm for image cryptosystems" [3], in this paper, a new chaotic block cipher scheme for image cryptosystems that encrypt a block of bits rather than a block of pixels is introduced. It encrypts 256 bits of the plain image to 256 bits of the cipher image within eight 32-bit registers. The scheme employs the cryptographic primitive operations and a non-linear transformation function within encryption operation and adopts round keys for encryption using a chaotic system. The new scheme can encrypt large size of images with superior performance speed than other schemes.

"A novel algorithm for image encryption based on a mixture of chaotic maps" [4], in this paper, an implementation of a digital image encryption scheme based on the mixture of chaotic systems is reported. The chaotic cryptography technique used in this paper is symmetric key cryptography. In this algorithm, a typically coupled map was mixed with a one-dimensional chaotic map and used for high-degree security image encryption while its speed is acceptable. The proposed algorithm is described in detail, along with its security analysis and implementation. The effectiveness of the proposed method and the implementation of the algorithm has been verified through experimental results using a combination of chaotic maps. This mixture application of chaotic maps shows the advantages of large key space and high-level security

"A symmetric image encryption scheme based on 3D chaotic cat maps" [5] in the paper, the authors have proposed a novel real-time secure symmetric encryption scheme that is based on 3D chaotic cat maps. They have extended the previously used 2D chaotic cat map to 3D and utilized it to shuffle the positions and grey values of image pixels. Additionally, they have incorporated another chaotic map to disrupt the relationship between the cipher image and the plain image, thereby enhancing the protection against statistical and differential attacks. Thorough experimental tests are carried out with detailed analysis, demonstrating the high security and fast encryption speed of the new scheme.

"A new image encryption scheme based on a chaotic function" [6], a new scheme for encrypting images has been introduced, which involves the combination of a chaotic function and XOR operator. The key benefits of this approach include the ability to generate a vast key space to withstand brute-force attacks, as well as to securely encrypt images with varying entropy structures, ensuring that the corresponding cipher images have indistinguishability, confusion, and diffusion properties. The results of several statistical analyses of randomness, sensitivity, and correlation of the cipher images show that the proposed cryptosystem is efficient and secure enough to be used for image encryption and transmission.

"An image encryption scheme based on new spatiotemporal chaos" [7], in this paper, a new chaotic system in the spatiotemporal domain has been introduced by defining the local nonlinear map in the CML using the nonlinear chaotic algorithm (NCA) chaotic map. Furthermore, an image encryption scheme has been proposed utilizing these chaotic maps with the permutation-diffusion mechanism. The encryption algorithm involves the use of the bitwise XOR operation between the pixels of the plain image, followed by the permutation of the resulting image using the chaotic sequence generated by the NCA map. Finally, the shuffled image is further diffused using the constructed spatiotemporal chaotic sequence. The experimental results indicate that the proposed encryption scheme is highly sensitive to the key and provides a large key space. Additionally, it has been shown to be secure against various types of attacks, including brute-force attacks, entropy attacks, differential attacks, chosen-plaintext attacks, known-plaintext attacks, and statistical attacks.

"A novel image encryption scheme based on improved hyperchaotic sequences" [8], this paper proposes a novel image encryption scheme based on the improved hyperchaotic sequences. Firstly, the hyperchaotic sequences are modified to generate chaotic key stream that is more suitable for image encryption. Secondly, the final encryption key stream is generated by correlating the chaotic key stream and plaintext which result in both key sensitivity and plaintext sensitivity. The scheme can achieve high key sensitivity and high plaintext sensitivity through only two rounds of diffusion operation. The performance test and security analysis have been performed using the histograms, correlation coefficient, information entropy, peak signal-to-noise ratio, key sensitivity analysis, differential analysis, key space analysis, decryption quality, and speed analysis.

III. Chaos logistic mapping

Chaos logistic mapping is a mathematical model that exhibits chaotic behavior, meaning that its output appears random and unpredictable, even though it is generated by a deterministic algorithm. The chaotic behavior of the logistic map can be utilized in cryptography for generating a secure key

The Logistic Mapping The logistic map is a simple mathematical formula that describes the population growth of a species under ideal conditions. The formula is:

$X_{n+1} = rX_n(1-X_n)$

Here, X_n represents the initial value at nth, and r is a constant between 0 and 4 that determines the rate of growth. The formula calculates the X_{n+1} at n+1 based on the X_n at n.

Key Generation using the Logistic Mapping to generate a key using the logistic mapping, we first choose a value of r between 3.57 and 4. We also choose a random initial value for X0 between 0 and 1.

We then apply the logistic map formula repeatedly to generate a sequence of numbers:

$X_1 = rX_0(1-X_0)$
$X_2 = rX_1(1-X_1)$
$X_3 = rX_2(1-X_2)$
...
$X_n = rX_{n-1}(1-X_{n-1})$

This sequence of numbers is our key. We can use the key to encrypt and decrypt messages using a symmetric key algorithm, such as the Advanced Encryption Standard (AES).

To ensure the security of the key, we must keep the value of r and the initial value of X_0 secret. Anyone who knows these values can generate the same sequence of numbers and decrypt our messages. We must also generate a new key for each message to prevent an attacker from decrypting multiple messages with the same key.

A bifurcation diagram is a graphical representation of the behavior of a dynamic system as a parameter is varied. In the case of the chaos logistic map, the bifurcation diagram is a plot of the values of the logistic map output as the value of the growth rate parameter (r) is increased.

In the context of key generation using chaos logistic maps, the bifurcation diagram is important because it helps to identify the values of r that produce chaotic behavior. The chaotic behavior of the logistic map is desirable for a key generation because it produces a sequence of numbers that appear random and unpredictable, which is essential for security.

The bifurcation diagram of the chaos logistic map shows the values of X_n for each value of r. The X-axis represents the values of r, and the Y-axis represents the values of X_n. As r is increased, the logistic map output exhibits a sequence of bifurcations, where the output transitions from a stable value to an unstable value, and then to chaos. These bifurcations occur at specific values of r known as the bifurcation points.

For r<3, the x remains constant with one value. For r=3, the graph gets bifurcated and we get 2 values for x. Similarly, at 3.5 the graph bifurcated again. This process continues and so on.

We can continue applying the logistic map formula to generate a sequence of numbers. The output of the logistic map appears random and unpredictable, even though it is generated by a deterministic algorithm. This property makes the logistic map useful in cryptography for generating a secure key.

IV. PROPOSED METHOD

4.1 Encryption

In the encryption process, first, the given input image of size m*n is transformed into an image array of m*n size. Here the input image can be color or black and white and of different sizes. At the same time, the hexadecimal key of 64-bit size is taken. This is first converted into ASCII format and later into binary format. The binary key is divided into 16 sets each containing 4 bits. These sets are stored as 'elements' in the list. The list is of k size.

Now each element taken from the list k is XORed with the image matrix and the XOR output is converted into decimal value. This decimal value is used as the initial input X_n. Chaotic logistic map operation is done by taking X_n as input. 'r-value or the controlling factor is taken as 4. The basic equation used in the chaos logistic mapping operation is

$X_{n+1}=r*X_n*(1-X_n)$

The second set of elements is taken from the list is taken and XORed with the image matrix. This is again converted into decimal values and sent to the logistic operation block. This process continues for all the 16 sets in the list k. The 16 image outputs which are obtained undergo an image fusion process to form a final encrypted image.

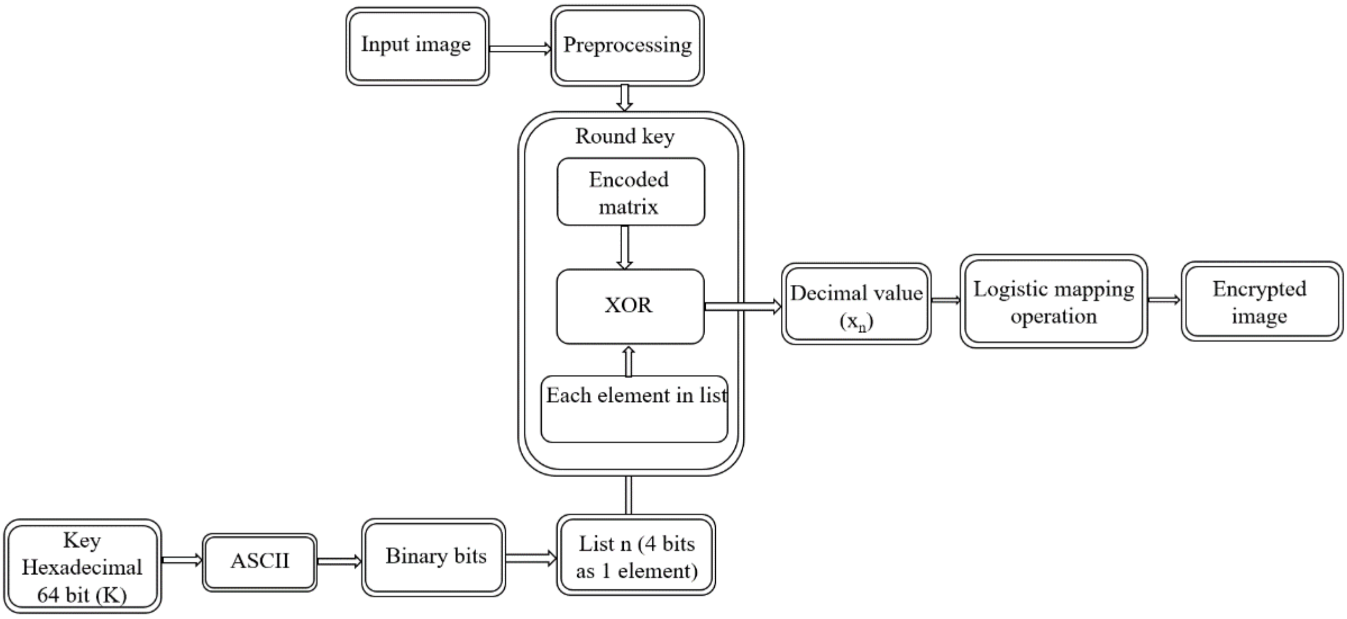


Figure 4.1: Encryption Block Diagram

4.2 Decryption

The decryption process is a reverse process of encryption. The decrypted image first undergoes a reverse image fusion process to recover the 16 images. Each image is preprocessed to get an image matrix. This is taken as input for the logistic mapping operation block. The ‘r-value or the controlling factor is taken as 4. The output matrix from this stage is converted into binary format and sent to the round key block.

Simultaneously, the hexadecimal key of 64-bit size is taken as input. One should note that this must be the same key that is given on the encryption side. Similar to the encryption side, this is first converted into ASCII format and later into binary format. The binary key is divided into 16 sets each containing 4 bits. These sets are stored as ‘elements’ in the list. The list is of k size.

Both the binary matrix and element 1 from the list k undergo XOR operation to get the encoded matrix. This matrix undergoes preprocessing to get the decrypted image.

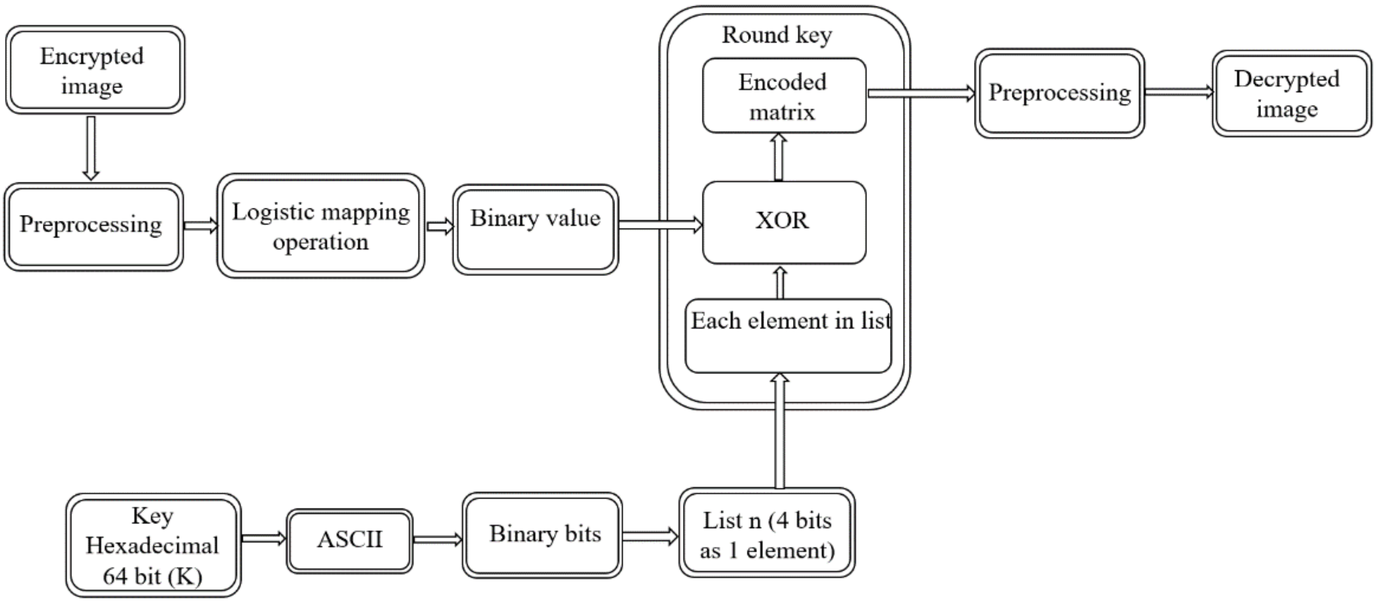


Figure 4.2: Decryption Block diagram

IV. RESULTS AND DISCUSSION

4.1 Results of parameters

	Runtime (sec)		NPCR (%)		IE		UACI	
Images	CCAES [1]	Logistic map	CCAES [1]	Logistic map	CCAES [1]	Logistic map	CCAES [1]	Logistic map
Lena	2.88	2.349	99.5368	99.626	7.9434	7.973	33.4724	33.463
Camera man	2.9	2.247	99.5697	99.603	7.9571	7.972	33.4767	33.411
F16	2.9	2.262	99.5712	99.602	7.9373	7.972	33.3877	33.358
Pepper	2.9	2.246	99.5414	99.613	7.9579	7.972	33.5864	33.394

Table 5.1: Comparison between CCAES and Logistic map results

Images	PSNR (dB)	SSIM		NIQE	
		Encrypted	Decrypted	Initial Image	Decrypted image
Lena	27.33	0.0095	0.9907	4.5214	4.5210
Cameraman	27.88	0.0087	0.9899	3.7980	3.7895
UCEN	27.89	0.0143	0.9960	5.4718	5.4713
UCEN Campus	27.90	0.0193	0.9981	1.8990	1.8970
Building	27.89	0.0176	0.9959	5.4718	5.4715

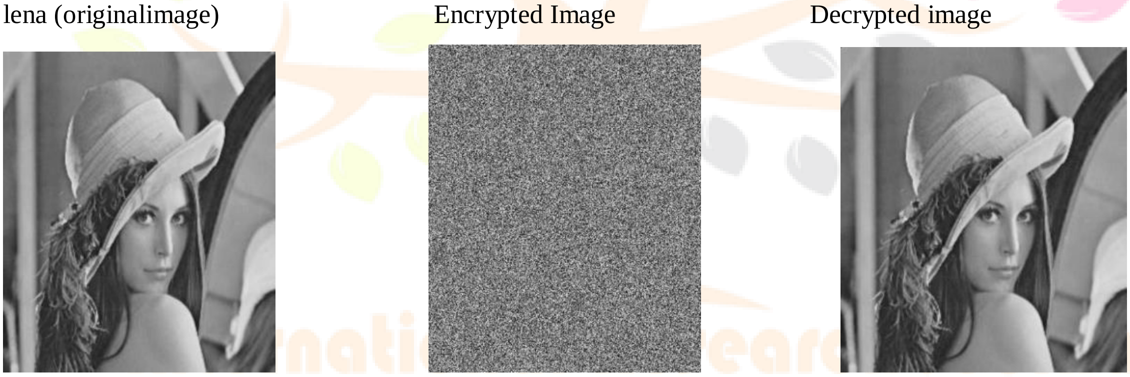
Table 5.2: PSNR, SSIM, NIQE of Chaos logistic maps

S.no	Images	Vertical	Diagonal	Horizontal
1	Lena	-0.00013	-0.00028	-0.00302
2	Cameraman	-0.00298	0.00136	-0.00476
3	F16	0.00091	0.00164	-0.00315
4	Pepper	-0.00135	0.00226	-0.00539
5	UCEN	0.01315	-0.00418	0.00368
6	UCEN Campus	0.01550	-0.00327	0.00325
7	Buildings	0.01896	-0.00167	0.00402

Table 5.3: Correlation between adjacent pixels

The comparison table shows that the proposed method shows better results when compared to the Chaotic Arnold Cat map using AES in different parameters like runtime, NPCR, UACI, and IE. The PSNR, SSIM, NIQE, and correlation between adjacent pixels are done for different standard images and also real-time images. The code and the results are performed on the google collab platform in Python language.

4.2 Encryption and decryption results of Standard images

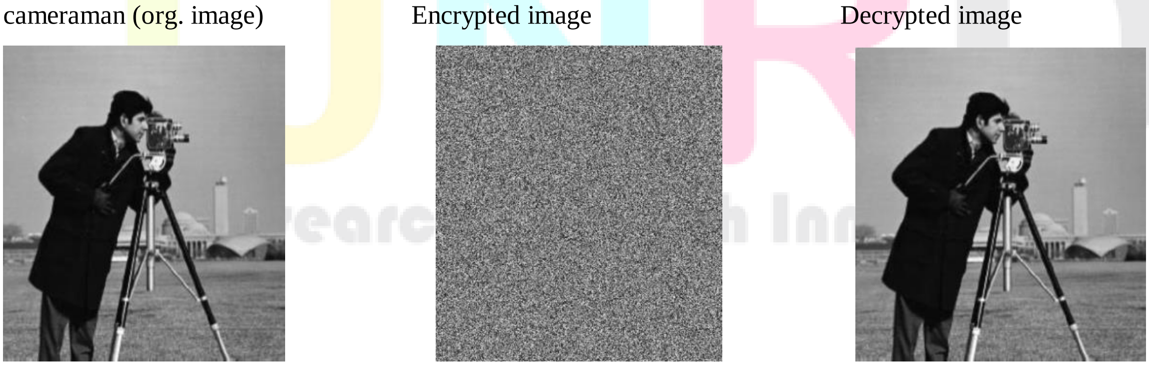


lena (originalimage)

Encrypted Image

Decrypted image

Figure 5.1: Encryption and Decryption results for Lena image



cameraman (org. image)

Encrypted image

Decrypted image

Figure 5.2: Encryption and Decryption results for Cameraman image

F16 jet (org. image)

Encrypted image

Deccrypted image

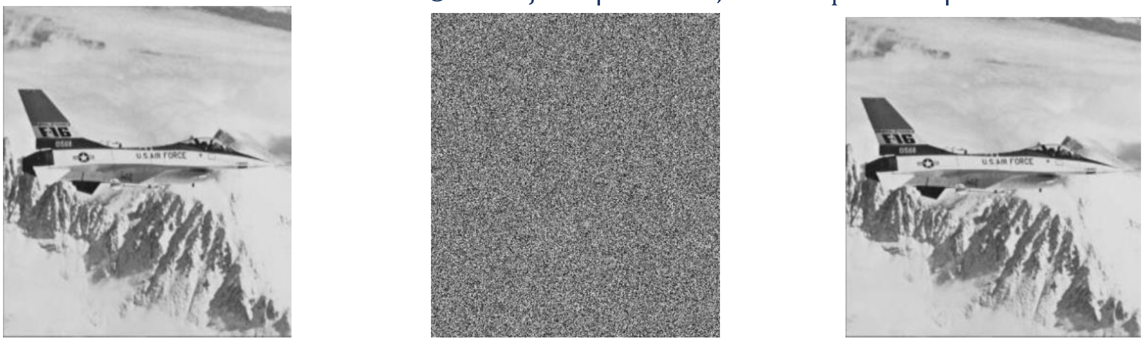
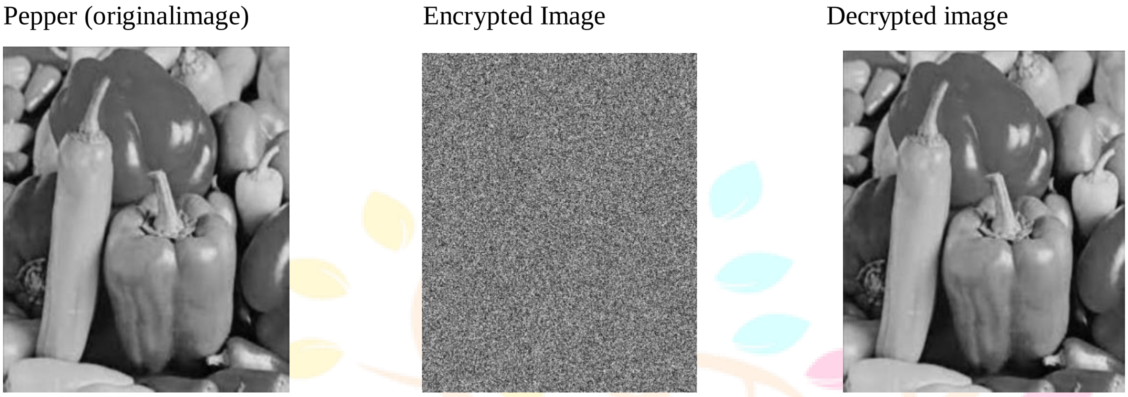


Figure 5.3: Encryption and Decryption results for F16 jet image



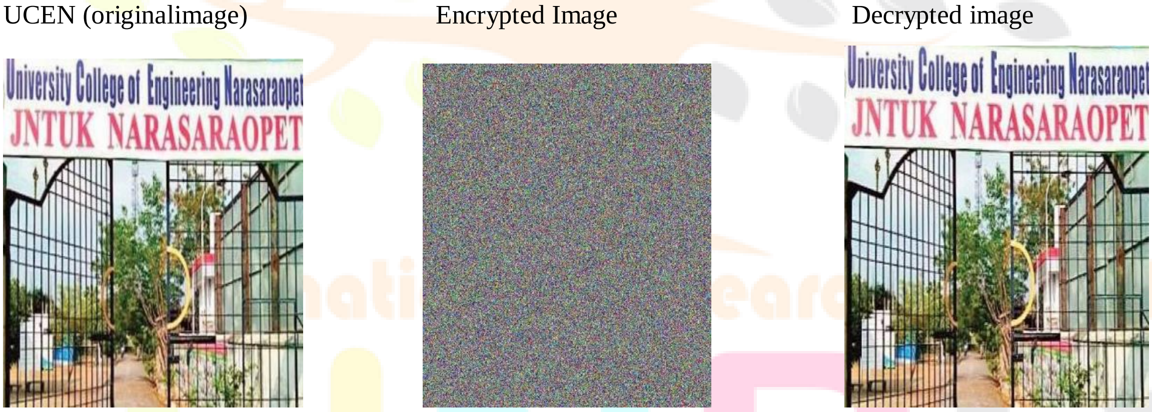
Pepper (originalimage)

Encrypted Image

Decrypted image

Figure 5.4: Encryption and Decryption results for Pepper image

4.3 Encryption and decryption results of Real-time images

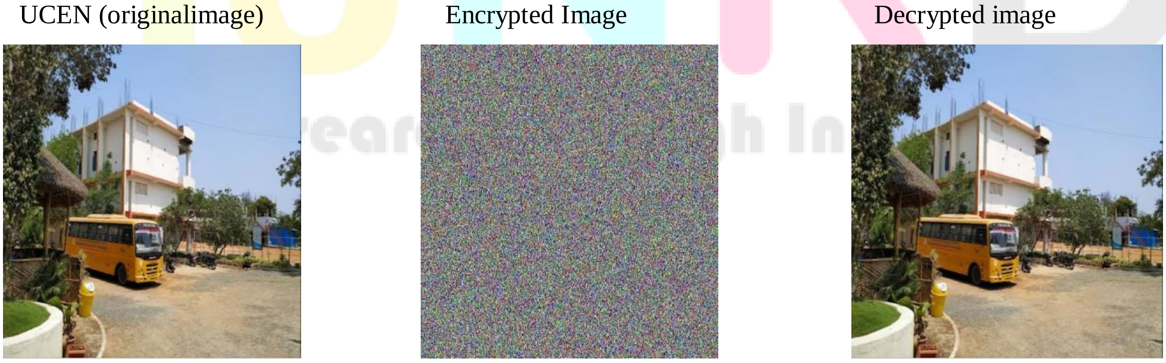


UCEN (originalimage)

Encrypted Image

Decrypted image

Figure 5.5: Encryption and Decryption results for UCEN image



UCEN (originalimage)

Encrypted Image

Decrypted image

Figure 5.6: Encryption and Decryption results for UCEN image

Buildings (originalimage) Encrypted Image Decrypted image

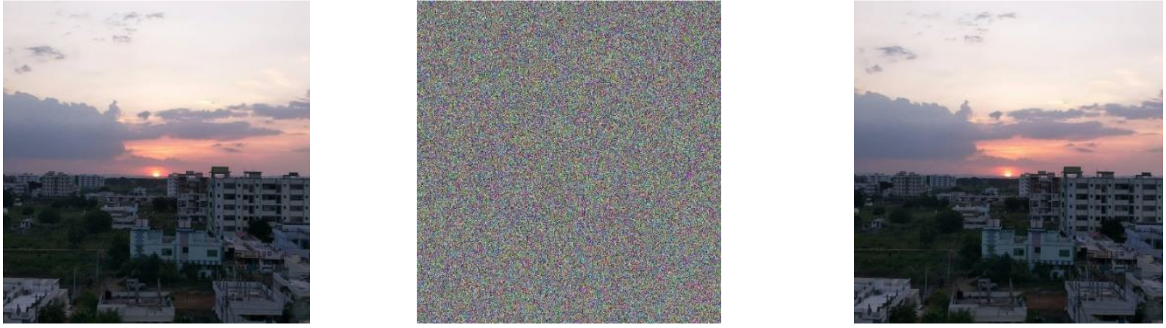


Figure 5.7: Encryption and Decryption results for Buildings image

4.4. Discussion

We successfully developed a more secure image encryption algorithm using the chaos logistic method and XOR operation. We also compared the NPCR, UACI, IE, and runtime with the Chaotic Arnold Cat map using the AES method (CCAES) and also evaluated different parameters like PSNR, SSIM, and NIQE with standard and real-time images.

References

[1] *Alireza Arab, Mohammad Javad Rostami, Behnam Ghavami1* ***(2019)*** *An image encryption method based on chaos system and AES algorithm.* The Journal of Supercomputing (2019) 75:6663–6682.

[2] *Norouzi B et al* ***(2014)*** *A simple, sensitive, and secure image encryption algorithm based on hyperchaotic system with only one round diffusion process. Multimed Tools Appl 71(3)* ***(****1469–1497)*

[3] Mohamed Amin , Osama S. Faragallah , Ahmed A. Abd El-Latif A chaotic block cipher algorithm for image cryptosystems. Communications in Nonlinear Science and Numerical Simulation ***(*****2010),** Pages 3484-3497

[4] S. Behnia , A. Akhshani, H. Mahmodi, A. Akhavan A novel algorithm for image encryption based on mixture of chaotic maps. Chaos, Solitons & Fractals *(***2008)**, Pages 408-419

[5] Guanrong Chen, Yaobin Mao , Charles K. Chui A symmetric image encryption scheme based on 3D chaotic cat maps. Chaos, Solitons & Fractals Volume 21, **(2004)**, Pages 749-761

[6] M. François, T. Grosges , D. Barchiesi , R. Erra A new image encryption scheme based on a chaotic function Signal Processing: Image CommunicationVolume 27, **(2012)**, Pages 249-259

[7] Song C-Y, Qiao Y-L, Zhang X-Z (2013) An image encryption scheme based on new spatiotemporal chaos. Opt Int J Light Electron Opt 124(18):3329–3334

[8] Zhu C (2012) A novel image encryption scheme based on improved hyperchaotic sequences. Opt Commun 285(1):29–37