International Journal of Advance Research in Science and Engineering
Volume No. 12, Issue No. 05, May 2023
www.ijarse.com
IJARSE
ISSN 2319 - 8354

Image Encryption Based on 3D Chaotic Map

SHRAVAN S[1], SHREYA[2], SHWETHA PRABHU[3], SINCHANA[4],

Mr. ARUN UPADHYAYA[5]

Department of Electronics and Communication,

Shri Madhwa Vadiraja Institute of Technology and Management,

Vishwothama Nagara, Bantakal, Udupi-574115 India

[1]iamshravanshettigar@gmail.com, [2]shreyakarunakar07@gmail.com, [3]prabhushwetha07@gmail.com,

[4]sinchana9402r@gmail.com, [5]arun_upadhyaya.ec@sode-edu.in

Abstract

Secure transmission of images over networks is a challenging issue in communication technology. Encryption can be used to convert original images into a cipher image that cannot be understood or unscrambled by unauthorized access. Image security through the combination of chaotic theory and cryptography is an important field, with numerous image encryption algorithms relying on chaotic maps. However, some of these algorithms can be complex and time-consuming, with limited key space. To address this, we have developed an encryption technique using 3D chaos sequences for image pixel position permutation and pixel value transformation. Our proposed method is statistically resistant and performs well in comparison to similar image encryption methods.

1. INTRODUCTION

The tremendous spreading out of the communication networks has evoked increased dependency on digitized information in our society. As a result, information is more vulnerable to abuse. Today the web is going towards multimedia data due to the development of network and multimedia technology. Multimedia data consist of image, audio, video, text, etc. The digital images have become one of the most important information carriers which are helpful in many applications.

In the past ten years, chaos-based cryptography has become popular because it uses noise-like signals that prevent unauthorized access. These signals have properties similar to those of effective ciphers, like confusion and diffusion. Researchers have proposed many image encryption algorithms based on chaotic systems, some of which rely on chaotic maps. Algorithms that use higher dimensional chaos functions are typically more secure against attacks.

Due to various inherent features of chaotic systems, a significant number of image encryption schemes based on chaos have been proposed. In the field of information security, numerous image encryption algorithms have been proposed which are based on chaotic systems. The two types of encryption processes are known as position permutations and value transformation. Position permutation technique involves the permutation of image positions without changing pixel values; whereas, in value transformation technique, pixel values are replaced by

another pixel value without changing their position. Among the value transformation techniques, XOR operation is one of the most popular ones which is used to achieve linear independence between two or more variables. To enhance the security performance of encryption algorithm, the concept of shuffling the positions of pixels in the plain image and then modifying the grey values of the shuffled image pixels are used.

Cryptography secures multimedia data such as digital images. A hybrid encryption technique utilizing pixel rotation and XOR-based encryption, aided by 3D chaos, enhances secure multimedia communication.

2. LITERATURE SURVEY

This encryption scheme works for 2D and 3D images. The iteration length of the chaotic system depends on the image size and its position index determines the diffusion sequence. The design uses the full capabilities of the 3D chaotic system and is resistant to brute force attacks due to strong key-sensitivity. The security performance is checked through various analyses, such as histogram, correlation, entropy, and differential attack measurement, all of which demonstrate the algorithm's statistical ability [1]. A method for encrypting colour images while maintaining scale invariance is proposed. The technique involves using 3D substitution and permutation for image diffusion and confusion. In substitution, XOR and circular shift are applied to sub image pixel values using suitable keys. Position of pixels is changed using 3D chaos mapping in permutation. Multiple analyses were performed to assess security performance, such as histogram, correlation, entropy, and key image sensitivity measurement. The values obtained for NPCR and UACI were 99.62 and 33.51, respectively, and the entropy was measured at 7.9994 [2]. Chaotic maps are utilized for confusion and diffusion in generating random numbers. They possess particular properties necessary for encrypting and decrypting images, including sensitivity to initial conditions. Security of the image encryption system is guaranteed when both substitution and permutation keys used for image pixels are random and dependent on the plain image. The paper discusses nine distinct methods for image encryption using chaotic maps [3]. The Bulban chaotic map is the basis of a new image encryption method, which is fast and efficient. The processing unit has been increased from pixel to row/column level, further enhancing the speed. Security is maintained through the use of a substitution-permutation network, which disrupts the correlation between adjacent pixels by circularly shifting rows and columns. The XOR operation is combined with the Modulo function to prevent information leakage by masking pixel values. Tests and simulations have verified that the scheme is very secure and highly suitable for real-time image processing at 80 fps. The NPCR and UACI values for the proposed scheme are 99.6186% and 33.4444%. The entropy of the scheme is 7.9032 [4]. The proposed technique achieves an NPCR value of 99.64 and a UACI value of 30.66, while maintaining an entropy of 7.998. The encryption process involves 3D logistic maps, serving as the initial safeguard. The method is highly efficient and produces a uniformly distributed image when its histogram is analysed [5]. The paper presents a new color image encryption algorithm that uses a combination of two low-dimensional chaotic maps to efficiently couple the chaotic system. Shuffling and diffusion are applied to rearrange the pixels and substitute them with a series generated from a chaotic map. The plain image is initially shuffled using 3D-PHM and then diffused to increase complexity. The cipher is tested for key sensitivity, histogram analysis, correlation, and difference measurement to assess its security performance. The results show high values for NPCR and UACI (99.62 and 33.41, respectively) and entropy of 7.9983. This cipher offers advantages such as efficiency, flexibility,

and resistance to attacks [6]. A method that utilizes chaos to encrypt images has been employed. This method involves permutation and diffusion operations. Information security is paramount in cryptography, especially in regard to confidentiality, integrity, and availability. The process included the use of Galois Field, matrix manipulation, and chaotic maps. The experiment was simulated using MATLAB software on a standard computer. Results yielded NPCR and UACI values of 99.62 and 33.51, respectively, and an entropy of 7.9994 [7]. A new image encryption system has been proposed that is both secure and fast. It addresses the issue of traditional encryption schemes where permutation and diffusion are separate processes, making them easier to crack. The proposed scheme generates key streams and indexes that are linked to the plaintext, making it more sensitive to the content being encrypted. Additionally, the encryption process handles pixel values by rows and columns. The scheme has almost ideal values for NPCR and UACI. The use of two chaotic maps also increases the randomness of the cipher text, leading to high information entropy [8].

3. METHODOLOGY

There are five stages to complete the overall encryption process. They are:

a) 3D Chaos Generation
b) Chaos Histogram Equalization
c) Row Rotation
d) Column Rotation
e) XOR Operation

Fig. 1. represents the overall encryption process where x (0), y (0), z (0), a, b, c, N1, N2, N3, N4, N5, N6 are the key.

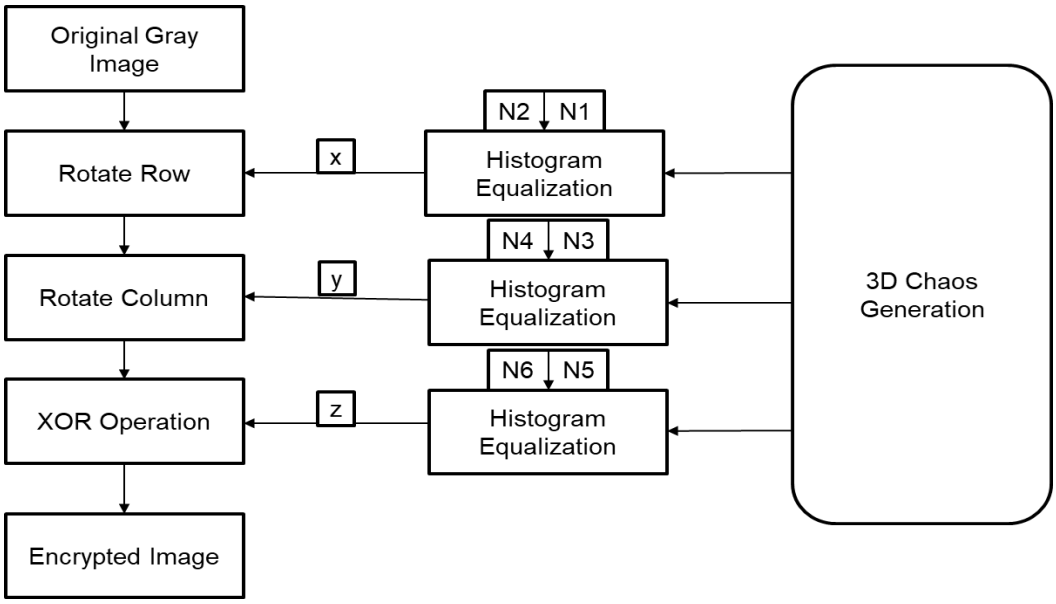

Fig. 1. Encryption technique using 3D Chaos.

A. 3D Chaos Generation

The logistic map is the simplest way of chaos generation given by an equation:

International Journal of Advance Research in Science and Engineering
Volume No. 12, Issue No. 05, May 2023
www.ijarse.com
IJARSE
ISSN 2319 - 8354

$$X_{n+1} = \mu X_n(1 - X_n) \quad (1)$$

For 0< X_n <1 and μ = 4 is the condition to make this equation chaotic. The 3D version of this logistic map is given by:

$$x_{n+1} = \gamma x_n(1 - x_n) + \beta y_n^2 x_n + \alpha z_n^3 \quad (2)$$

$$y_{n+1} = \gamma y_n(1 - y_n) + \beta z_n^2 y_n + \alpha z_n^3 \quad (3)$$

$$z_{n+1} = \gamma z_n(1 - zn) + \beta x_n^2 x_n + \alpha y_n^3 \quad (4)$$

Here the above equations exhibit the chaotic behaviour for 3.53<γ<3.81, 0<β<0.022, 0<α<0.015 and the initial value of x, y, z any value in-between 0 and 1. Presence of cubic, quadratic coupling and 3 constant terms make the 3D logistic map even more complicated and secure. Fig. 2 (a), (b), (c) shows the generated chaos sequences using the equation 2, 3, 4 and initial value of x(1)=0.2350; y(1)=0.3500; z(1)=0.7350; α=0.0125; β=0.0157; γ=3.7700.

B. Chaos Histogram Equalization

In Fig. 2 (d), (e) and (f) it is clear that histogram of x, y and z has non-uniform distribution. For higher security we need to equalize histogram. If a grey image with M×N dimension where M is the number of row pixels and N is the number of column pixels, then equalizes histogram by following formula

$$x = (integer(x \times N2)) mod\ N \quad (5)$$

$$y = (integer(y \times N4)) mod\ M \quad (6)$$

$$z = (integer(z \times N6)) mod\ 256 \quad (7)$$

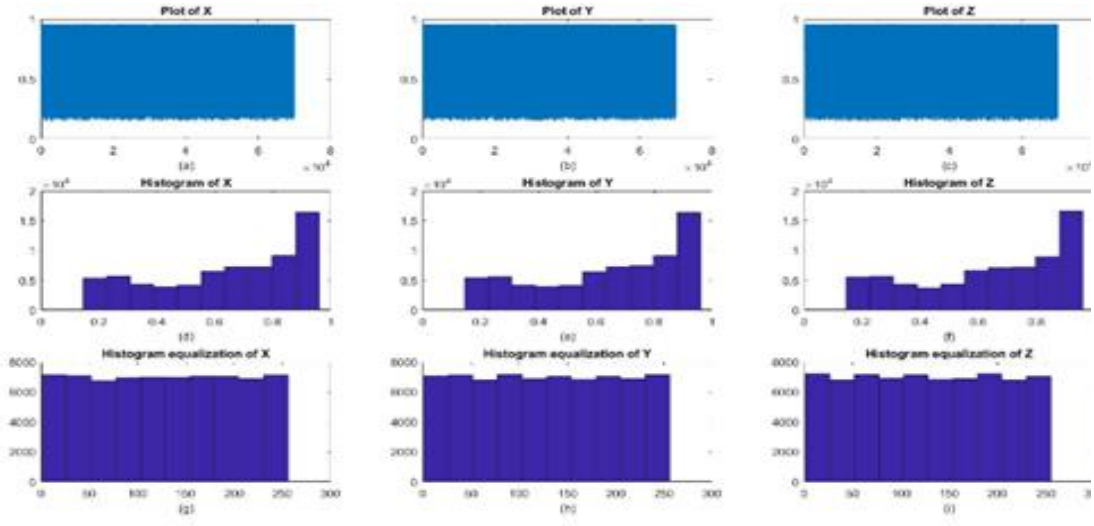

Fig. 2. Histogram Equalization of 3D Chaos.

Where, N2, N4, N6 are a large random number generally greater than 10000. For the simplicity we also can consider N2, N4 and N6 are equal. Figure. 2 (g), (h) and (i) shows the equalized histogram by using N2=N4=N6= 100000, M=256, N=256.

C. Row Rotation

Our new image pixel permutation approach involves rotating rows and columns in a manner similar to a combination lock on a briefcase. To rotate the rows of a gray image with dimensions MxN, we randomly select M chaos sequences starting from a large random number N1. The rows are then rotated based on the value of chaos 'x' from equation 5, with right rotation used for even chaos values and left rotation for odd values, thus enhancing security.

D. Column Rotation

Column rotation is just as similar as row rotation when it comes to gray image. To execute row rotation on an M×N dimension gray image, we have to choose N chaotic sequences. Firstly, we generate a large random number, N3, followed by selecting N chaotic sequences starting from index N3. We then rotate the row depending on the value of the y chaos from Eq.6. For better security, we rotate upwards when the chaos value is even and downwards when the value is odd. After the row and column rotation, the image becomes encrypted, but there is still a problem with unchanged histograms, which can cause a histogram attack. To prevent this attack, we need to add another step that changes the pixel value of the image.

E. XOR Operation

The encryption process ends with an XOR operation that transforms the pixel values into new values which cannot be reversed without knowing the chaotic key. To begin, we create a large random number (N5) and convert the M×N image into a 1×MN image. Then, we XOR the chaos (starting from index N5) with the row-column shifted image, resulting in the encrypted image.

DECRYPTION

For decryption process, these steps are performed in the reverse order. Hence we will get the original image as the decrypted image.

4. SIMULATION RESULT

For simulation purpose we use Peppers(P1), Deblur(P2) and Flower(P3) image and we will resize all the images to a size 256 x 256 in our experimental analysi

A. Encryption Example

In order to confirm the algorithm's validity, the experiment has been taken. The initial keys are taken as: (1)=0.2350; y(1)=0.3500; z(1)=0.7350; α=0.0125; β=0.0157; γ=3.7700, N2=N4=N6=100000, N1=5000, N3=6000, N4=7000.

International Journal of Advance Research in Science and Engineering
Volume No. 12, Issue No. 05, May 2023
www.ijarse.com
IJARSE
ISSN 2319 - 8354

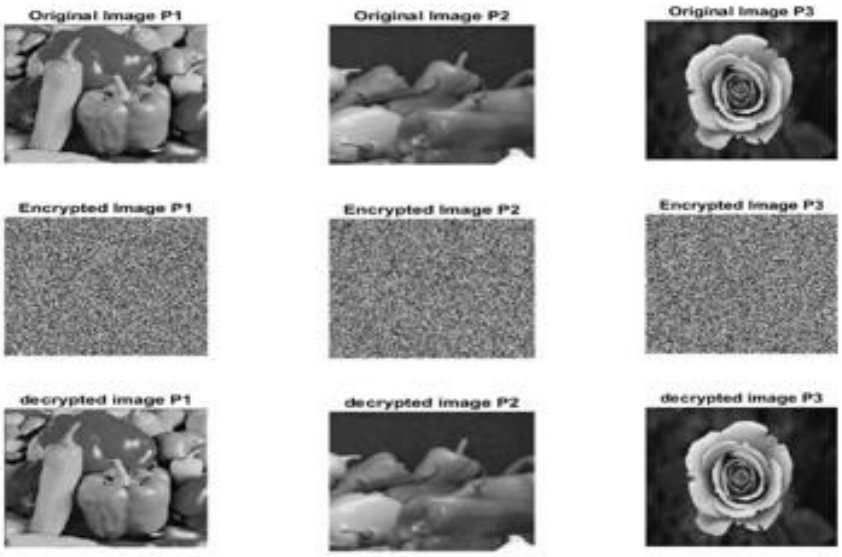

Fig.3. Encryption and Decryption for image P1, P2, P3

In Fig.3 shows the encryption and decryption image for all the taken images. From the figure we can see that pixels are diffused properly and completely different from original image.

B. Entropy Analysis

The entropy H of a symbol source S can be calculated by following equation

$$H(S) = -\sum N - 1\, P(Si) log 2\, P(Si)$$

The probability of a symbol Si is represented by where P(Si), and the resulting entropy is measured in bits. If the source S emits 28 symbols with equal probability, H(S) is 8. This indicates a truly random source, which is an ideal value for the entropy of message source S. A uniform distribution of gray value results in higher information entropy. If the encrypted image has a significantly lower information entropy than 8, it becomes predictable and is vulnerable to security breaches. However, our proposed algorithm produces encryption with information entropy values very close to the ideal value of 8. See Table I for the entropy values of the encrypted images.

Table I. Information Entropy of Encrypted images for various images

Entropy Analysis of Image					
Peppers(P1)		**Deblur(P2)**		**Flower(P3)**	
Plain Image	Cipher Image	Plain Image	Cipher Image	Plain Image	Cipher Image
7.5553	7.9886	7.2636	7.9891	7.0204	7.9888

C. Plain-text Sensitivity Analysis

Information about the underlying encryption algorithm.

The sensitivity of plain-text attacks is determined by assessing the NPCR and UACI of the encrypted image.

The NPCR (Number of Pixel Change Rate) is the percentage of varying pixels between two cipher images,

while the UACI (Unified Average Changing Intensity) is the average intensity of the differences between the two cipher images of size M×N.

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

$$UACI = \frac{1}{M \times N}[\sum_{i,j}[\frac{[I(i,j) - K(i,j)]}{255}]] \times 100\%$$

Table II. NPCR and UACI values of Encrypted images for various image

	Peppers(P1)	**Deblur(P2)**	**Flower(P3)**
NPCR	99.5819	99.2844	99.6902
UACI	33.3027	34.8025	34.7675

D. Statistical Analysis

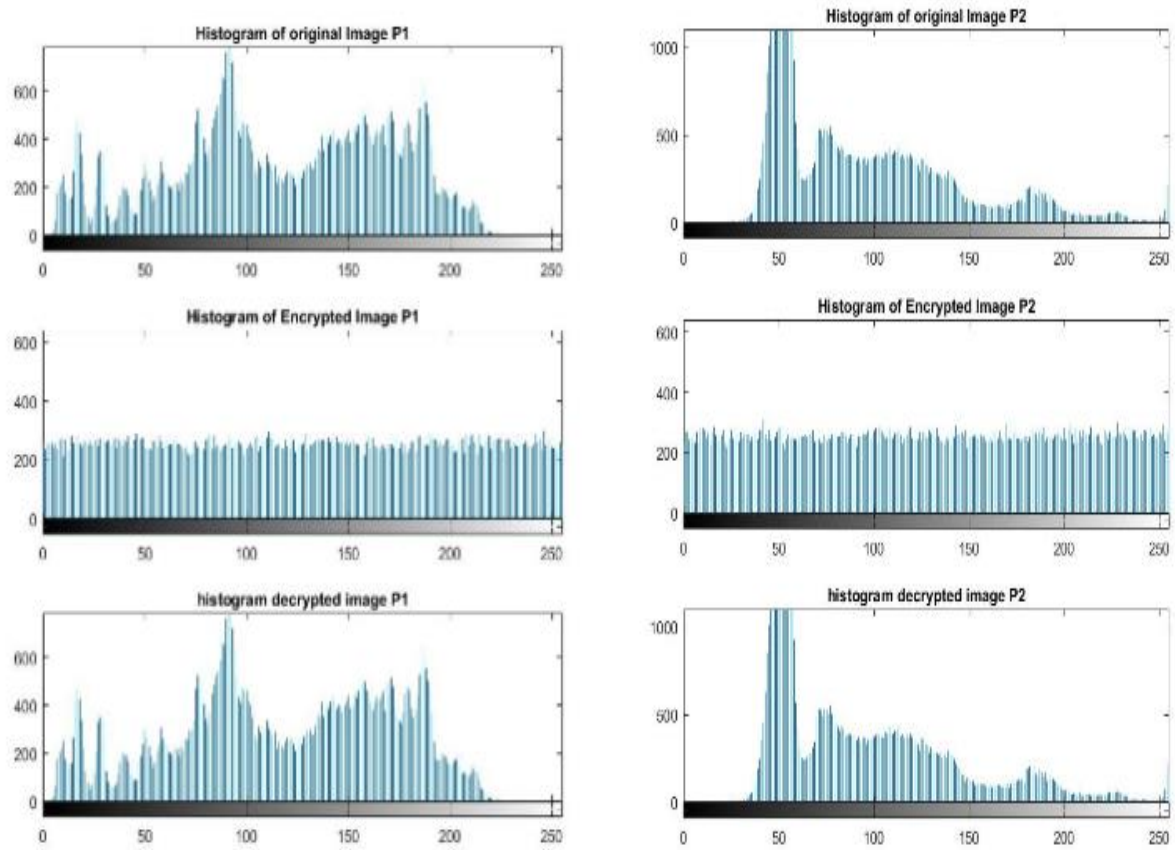

Fig.4. Histogram of original, encrypted and decrypted Peppers(P1) and Deblur(P2) images

The correlation between adjacent pixels in images can lead to serious security threats for image encryption. Statistical analysis is a powerful tool to demonstrate the strong resistance to such attacks provided by the confuse and diffuse properties of encryption. In Figure 4, the histogram of the original, encrypted, and decrypted images are shown. The histogram of the encrypted image shows that the pixel values are uniformly distributed, with no information that could be accessed by an intruder.

E. Correlation Coefficient Analysis

In order to evaluate the encryption quality of the proposed encryption algorithm, the correlation coefficient is used calculate the correlation coefficients between two vertically, horizontally adjacent pixels of an encrypted image.

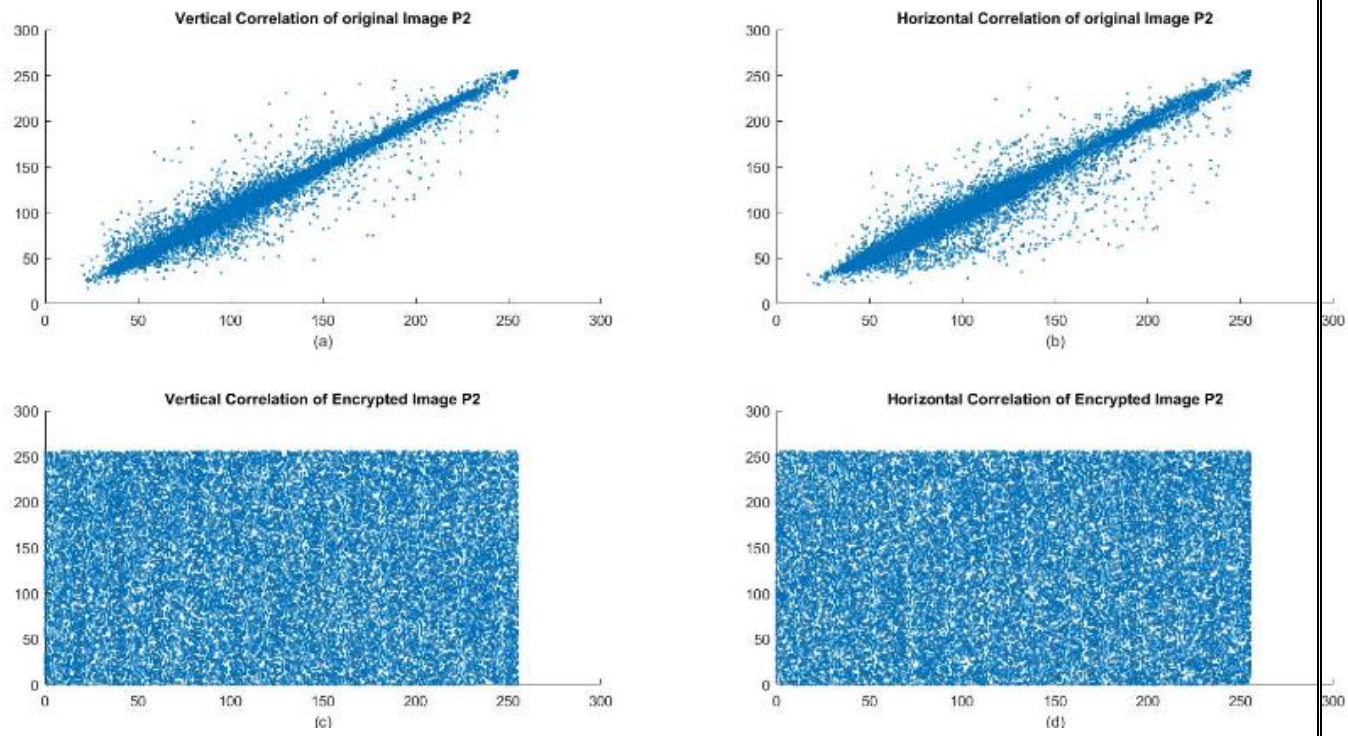

Fig.5 Correlation of original and encrypted Deblur (P2) image.

In Fig.5 shows the correlation for 256×256 Deblur image. Among them (a) Vertical correlation (b) Horizontal correlation of the original image and (c) (d) stands for encrypted image. From Fig.5 we can see that though the original image is highly correlated to the adjacent pixels and values are distributed near the center but after encryption pixel values are uniformly distributed as a result lower the correlation level.

5. CONCLUSION

In this article, we suggest a 3D encryption algorithm that uses Chaos theory, along with pixel position permutation and pixel value transformation techniques. The level of security offered by the algorithm can be adjusted for low, medium or high security needs. The article presents a comprehensive statistical analysis of both the stream generation system and the encryption scheme. Moreover, we have performed various tests like entropy analysis,

statistical analysis and plain-text sensitivity to evaluate the proposed algorithm's security against different attacks. The results demonstrate that the algorithm provides high security level and outperforms existing schemes. In addition, the algorithm has high throughput and can be used for real-time encryption applications. The proposed algorithm is suitable for secure multimedia information transmission over the internet. This paper's algorithm encrypts and decrypts images, but it can also be used in other areas of information security.

ACKNOWLEDGEMENT

We would like to express our sincere gratitude to the Management and Principal, Shri Madhwa Vadiraja Institute of Technology and Management Bantakal for the facilities provided and their support. Also, we would like to thank the Head of department Electronics and Communication and faculties for their encouragement and support.

REFERENCES

[1]. Gao, Xinyu, Miao Miao, and Xiaoyang Chen. "Multi-image encryption algorithm for 2D and 3D images based on chaotic systems." Frontiers in Physics (2022): 498.

[2]. Asl, Ali Momeni, Ali Broumandnia, and Seyed Javad Mirabedini. "Scale invariant digital color image encryption using a 3D modular chaotic map." IEEE Access 9 (2021): 102433-102449.

[3]. Veena, G., and M. Ramakrishna. "A survey on image encryption using chaos-based techniques." International Journal of Advanced Computer Science and Applications 12.1 (2021).

[4]. Talhaoui, Mohamed Zakariya, Xingyuan Wang, and Mohamed Amine Midoun. "Fast image encryption algorithm with high security level using the Bülban chaotic map." Journal of Real-Time Image Processing 18.1 (2021): 85-98.

[5]. Allawi, Salah T., and May M. Abbas. "A New method for image encryption based on 2D-3D Chaotic Maps." International Journal of Computer Science and Information Security (IJCSIS) 18.11 (2020).

[6]. Liu, Chunyuan, and Qun Ding. "A color image encryption scheme based on a novel 3d chaotic mapping." Complexity 2020 (2020).

[7]. Broumandnia, Ali. "Image encryption algorithm based on the finite fields in chaotic maps." Journal of Information Security and Applications 54 (2020): 102553.

[8]. Liu Lidong, Donghua Jiang, Xingyuan Wang, Linlin Zhang, Xianwei Rong, "A Dynamic Triple-Image Encryption Scheme Based on Chaos, S-Box and Image Compressing", IEEE Access, vol.8, pp.210382-210399, 2020.

[9]. Ye, Guodong, Kaixin Jiao, Chen Pan, and Xiaoling Huang. "An effective framework for chaotic image encryption based on 3D logistic map." Security and Communication Networks 2018 (2018).

[10]. Pan, Hailan, Yongmei Lei, and Chen Jian. "Research on digital image encryption algorithms based on double logistic chaotic maps." EURASIP Journal on Image and Video Processing 2018.1 (2018): 1-10.

[11]. Chaudhary, Nirmal, Tej Bahadur Shahi, and Arjun Neupane. "Secure Image Encryption Using Chaotic, Hybrid Chaotic and Block Cipher Approach." Journal of Imaging 8, no. 6 (2022): 167.

[12]. Tanveer, Muhammad, Tariq Shah, Amjad Rehman, Asif Ali, Ghazanfar Farooq Siddiqui, Tanzila Saba, and Usman Tariq. "Multi-images encryption scheme based on 3D chaotic map and substitution box." IEEE Access 9 (2021): 73924-73937.

[13]. Huang, Wei, Donghua Jiang, Yisheng An, Lidong Liu, and Xingyuan Wang. "A novel double-image encryption algorithm based on the Rossler hyperchaotic system and compressive sensing." IEEE Access 9 (2021): 41704-41716.

[14]. Lidong, Liu, Donghua Jiang, Xingyuan Wang, Linlin Zhang, and Xianwei Rong. "A dynamic triple-image encryption scheme based on chaos, S-box and image compressing." IEEE Access 8 (2020): 210382-210399.

[15]. Patro, K. Abhimanyu Kumar, Ayushi Soni, Pradeep Kumar Netam, and Bibhudendra Acharya. "Multiple grayscale image encryption using cross-coupled chaotic maps." Journal of Information Security and Applications 52 (2020): 102470.

[16]. Li, Hao, Lianbing Deng, and Zhaoquan Gu. "A robust image encryption algorithm based on a 32-bit chaotic system." IEEE Access 8 (2020):pp. 30127-30151.

[17]. Li, Chunhu, Guangchun Luo, and Chunbao Li. "An Image Encryption Scheme Based on The Three-dimensional Chaotic Logistic Map." Int. J. Netw. Secur. 21.1 (2019): 22-29.

[18]. Preishuber, Mario, Thomas Hütter, Stefan Katzenbeisser, and Andreas Uhl. "Depreciating motivation and empirical security analysis of chaos-based image and video encryption." IEEE Transactions on Information Forensics and Security 13, no. 9 (2018): 2137-2150.