International Journal of Multidisciplinary Innovative Research.
ISSN: 2583-0228 Volume 1, Number 1 (Jul' 2021) pp. 34-43

https://www.ciir.in

A New Technique of Image Encryption using Modified AES Algorithm

Abhinav Gupta[1] and Aayush Gupta[2]

[1] *Researcher, Sri Satya Sai University of Technology & Medical Sciences, Sehore, Madhya Pradesh*

[2] *Research Associate, Council of Industrial Innovation and Research, Noida*

Email: abhinavgupta7806@gmail.com

ABSTRACT: ***The privacy of the pictures is a huge challenge and demands more attention to resolve the existing issues related to image security. To provide an effective and fast way to protect the data or information stored in various images, the confidentiality and privacy of the images are becoming an enormous challenge. Several methods and algorithms have been investigated to provide the desired solution to existing problems, but these methods and algorithms are not ideal for multiple image formats of different dimensions within current communication systems. A novel picture encryption algorithm has been investigated in this research paper which is rooted in the enhanced AES algorithm. This investigated approach offers numerous advantages over existing picture encryption algorithms such as less computational complexity and lower image encryption time which is high in demand across the globe for efficient and fast transmission of the pictures over communication channels. The proposed algorithm is more protected and fast as well as maintain the confidentiality of the images against various noise attacks by multiple strikers over communication channel during picture transmission for multifarious purposes.***

KEYWORDS: ***Communication Channel, Data, Image Encryption, NPCR, UACI, Privacy.***

INTRODUCTION

Due to many current problems and image transmission through the internet communication platform, the protection of digital images is becoming difficult and challenging around the globe. During the transmission, the security of the images is the fundamental and primary concern and various methods have been explored to protect the transmitted data through the communication channels [1]. The security and authentication of information are the immense challenges facing different individuals around the world. In order to reduce the chances of data leakage, it is important to investigate and validate some novel methods to protect confidential data during communication channel transmission [2]. The techniques and algorithms of image encryption play a crucial role in sensitive data or information protection as it is transmitted over wireless communication channels [3]. Various methods have been studied by different researchers to secure data, such as cryptography, which is a useful technique to secure private data to decrease the probability of unauthorized access during the broadcast of information [4]. One of the most critical areas of communication that require more effort to secure private data is data or information protection.

The security of the images is more complicated when snaps are transmitted over wireless networks [5]. The pictures information is very different from other data forms, such as text, audio, video, etc. When important and rational information is transmitted from one end to another when individuals send the data in the form of images or text, safe methods are needed [6]. Now a few days for diverse purposes, the data or information in the form of pictures is growing more and more and the management of these gigantic records is crucial during the broadcast to provide the needed safety during the broadcast [7].

LITERATURE REVIEW

Setyaningsih *et al*. discussed another paper on the compression of the pictures and encryption methods. The secrecy of the images that contain a huge amount of essential and confidential data or information has become a primary concern during the last decade due to the dramatic increment in multimedia applications. There have been investigated multifarious new techniques and algorithms to provide the required secrecy to various picture formats. In this research article, a novel picture encryption method has been explored via a joint grouping of cryptographic as well as the compression method for security and privacy perspectives of the pictures. These compression and encryption methods jointly provide improved picture encryption time over conventional methods [8]**.**

Panda *et al*. investigated another picture encryption method and evaluated various performance parameters to validate the results. The privacy and secrecy of the digital data in a form of images is a huge problem and challenge across the globe and numerous method has been exploring to overcome this threat. The encryption of the pictures is a pragmatic method that has been adopted by various researchers to validate and test numerous image formats to secure confidential picture data. The image encryption methods play a crucial role to maintain the privacy of the images during the transmission over the communication channels. There are various pragmatic image encryption algorithms such as DES, RSA, Blowfish and many more that provide the enhanced security as required but in the modern world, these algorithms have certain limitations [9]**.**

Rajinder *et al*. studied another paper on the techniques and algorithms of picture encryptions. The secrecy and privacy of the pictures is a huge challenge worldwide due to the increment in multimedia applications day by day. Picture encryption is one of the most pragmatic techniques to provide the required secrecy to the pictures during the transmission over the communication media. The encryption methods are utilized where highly secure digital image transmission is required such as in the medicinal or military sector. Over the last decade, various picture encryption algorithms have been explored to offer the required secrecy of pictures from various strikers. This comprehensive study provides information about recent trends in the arena of image encryption [10].

METHODOLOGY

3.1 Design:

From the viewpoint of confidentiality, the encryption of snaps has become very vital in the contemporary world. To avoid the strikers' sensitive data, several methods for image guard have been examined. A novel way for picture encryption using the modified AES algorithm has been explored in this paper. Figure 1 portrays a flow map of the modified AES algorithm for encryption

of the picture. This experiment is conducted in two phases i.e. the encryption phase and the decryption phase.

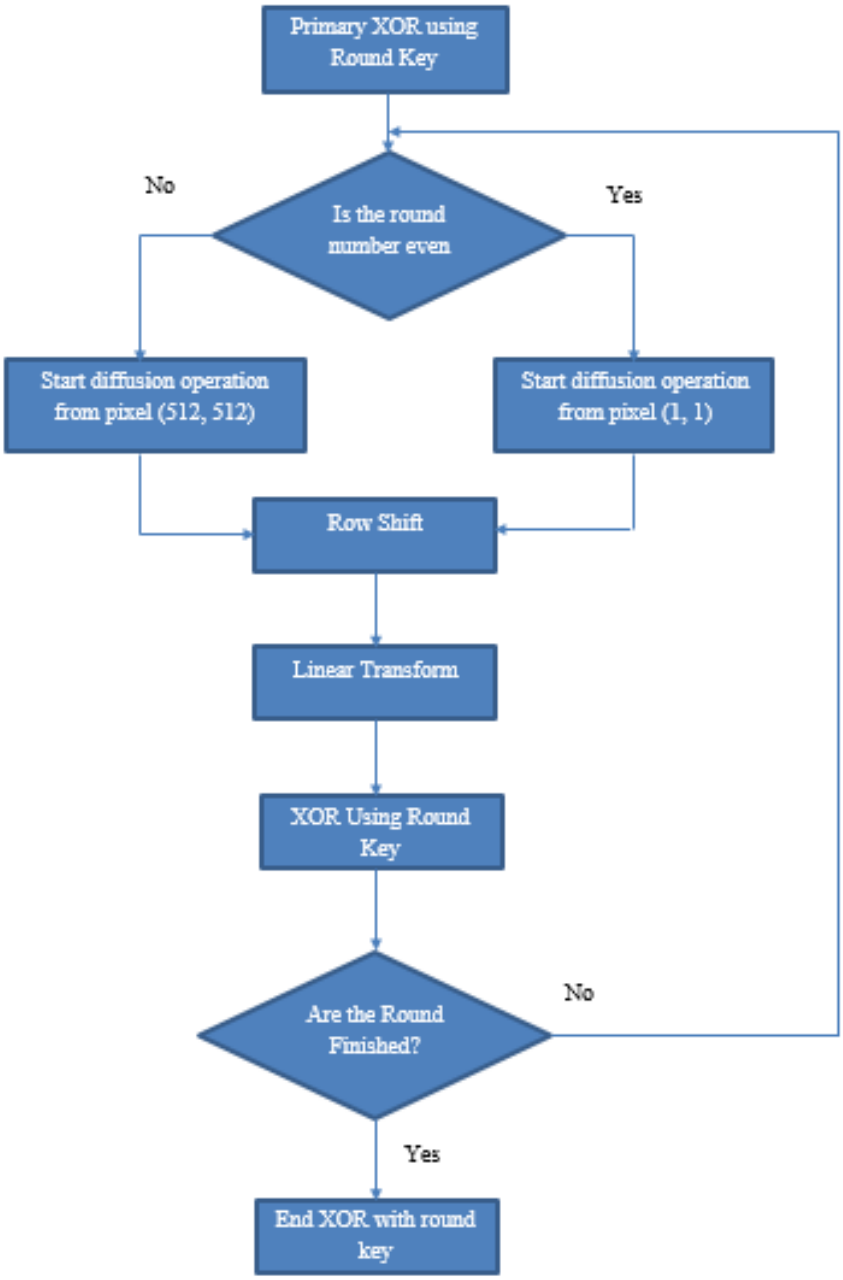


Figure 1: Illustrates the flow diagram of the proposed picture encryption algorithm

3.2 Instrument:

This experiment was performed on MATLAB R2018b software installed in a personal computer having a 64-bit operating system and 6GB RAM. MATLAB has become one of the most useful

and user-friendly software during the last many years for its attractive features. Numerous useful tools within MATLAB provide rational features to resolve various types of problems. There are various researchers who prefer MATLAB in comparison to other software due to its simple user interface and less computational complexity. The MATLAB software is utilized for various applications like deep learning, machine learning, neural networks, image processing and several others.

3.3 Data Collection:

During the experiment there has been taken various images formats of different pixels and test results were validated with a high precision in order to validate the proposed modified AES algorithm for the encryption of the images. Some of the essential formulas are given here for the calculation of the various parameters such as NPCR, UACI.

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

$$UACI = \left[\sum_{i=1}^{M} \sum_{j=1}^{N} \frac{|C1(i,j) - C2(i,j)|}{255} \right] \times \frac{100\%}{M \times N}$$

Another critical constraint is the correlation coefficient to ensure that the encryption algorithm is very accurate. The expression is given below.

$$r_{x,y} = \frac{C(x,y)}{\sqrt{D(x)}.\sqrt{D(y)}}$$

Where $C(x,y), D(x)$ and $D(y)$ may be evaluated by utilizing the following equations [6].

$$C(x,y) = \frac{\sum_{i=1}^{K} (x_i - E(x))(y_i - E(y))}{K}$$

$$D(x) = \frac{1}{K} \sum_{i=1}^{K} (x_i - E(x))^2$$

$$D(y) = \frac{1}{K} \sum_{i=1}^{K} (y_i - E(y))^2$$

3.4 Data Analysis:

In this paper, a modified version of the standard AES algorithm is utilized for pictures encryption from secrecy perspectives during transmission over wireless communication media. There are numerous algorithm for the encryption of the various images format form security perspective but some of these existing algorithms have more computational complexity which is a huge problem. The authors modified the standard AES algorithm in two segments during the experiment. One

modification was done by replacing the proposed propagation to the permutable operation in the original AES algorithm. The steps of the modified AES algorithm are given below.

Algorithm:

Step 1: First read the input picture and further encode this picture by utilizing base 64.

Step 2: Second read the code file and initialize AES 256 bit by applying the SHA256.

Step 3: Third encryption of the picture by applying the base 64 coded text and hash sequence originated in previous steps.

Step 4: Fourth originate a novel picture C of a dimension (p, q) with pixel data

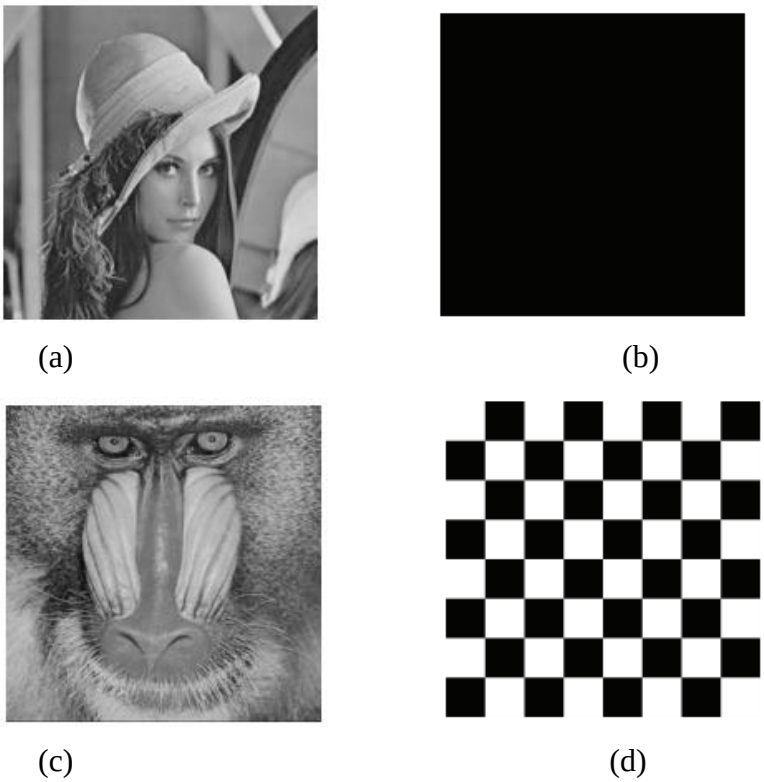
Step 5: Every row r in the height of the picture encore.

(i) Assume s be the ASCII code of the rth character within the code file.
(ii) Fill initial j pixels of picture inside picture within the rth row.

Step 6: Originate the N (=2) picture of the similar size and same pixel data.

Step 7: Output encrypted coding of every picture.

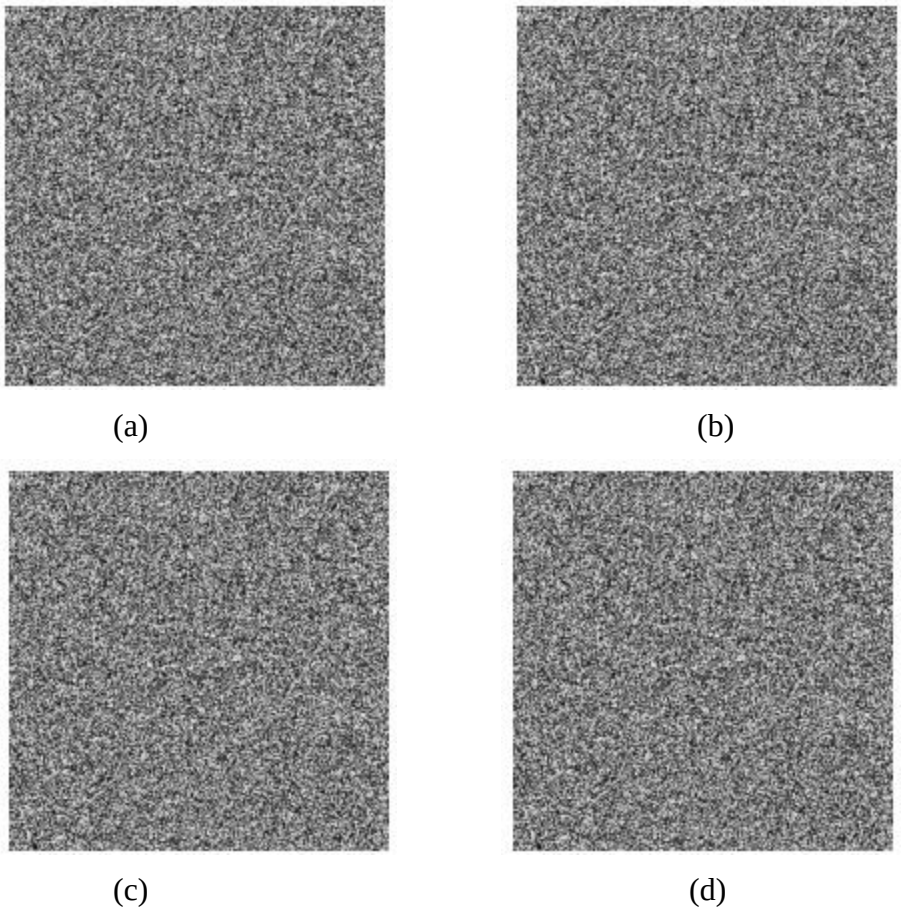
RESULTS AND DISCUSSION



(a) (b)

(c) (d)

Figure 2: Illustrates real test pictures selected for experiment. Plain pictures of (a) Lena; (b) Black; (c) Baboon; (d) Chessboard

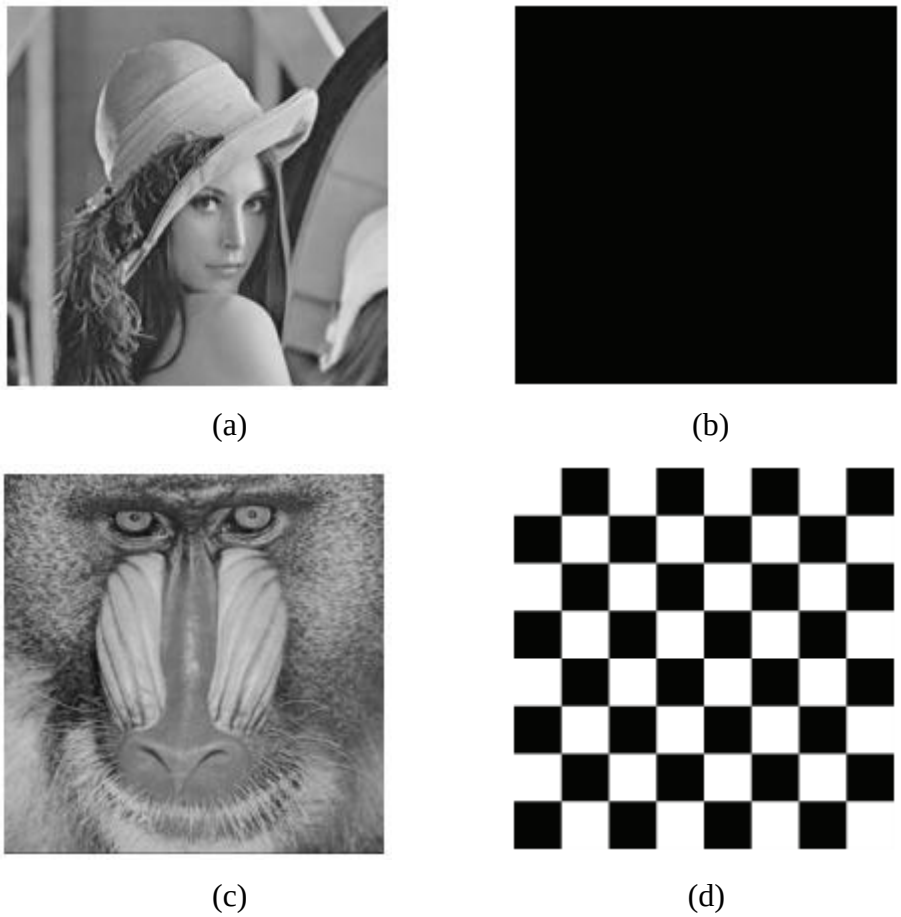


(a) (b)

(c) (d)

Figure 3: Illustrates encrypted pictures of (a) Lena; (b) Black; (c) Baboon; (d) Chessboard;

Figure 2 shows the real test pictures which were selected for this experiment. For this experiment four diverse images were taken and validated with the help of the proposed modified AES algorithm. For the optimum validation of the proposed AES algorithm three different pixel sizes were taken i.e. 128×128, 256×256, 512×512 for every image. The selected four pictures are Lena, Black, Baboon and Chessboard. The Figure 3 shows the encrypted images of all selected images i.e. Lena, Black, Baboon and the Chessboard. The encryption of all images were done by applying the proposed modified AES algorithms in order to get the more secure and fast results in comparison to ordinary methods. This Figure 4 shows the corresponding decrypted images of all images on the receiving side. This modified AES algorithm were applied for the encryption and decryption procedure because it provides the pragmatic results according to the requirements. Table 1 shows the observed NPCR as well as the UACI amount of each selected picture. The pictures of Lena, Black, Baboon and the Chessboard having the NPCR and the UACI values 99.6812, 99.7013, 99.7215, 99.7617 and 33.3011, 32.3120, 33.4688, 33.3164 respectively.



(a) (b)

(c) (d)

Figure 4: Illustrates decrypted pictures of (a) Lena; (b) Black; (c) Baboon; (d) Chessboard

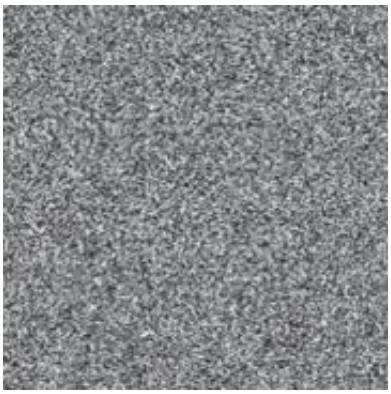
Table 1: Illustrates the NPCR as well as UACI amount of selected experiment pictures

Sl. No.	Picture(s)	NPCR (%)	UACI (%)
1.	Lena	99.6812	33.3011
2.	Black	99.7013	32.3120
3.	Baboon	99.7215	33.4688
4.	Chessboard	99.7617	33.3164

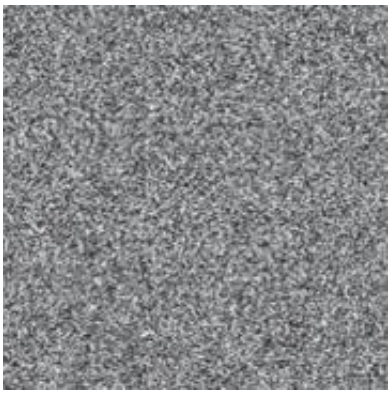
Table 2: Illustrates information entropy with local entropy of selected pictures for experiment.

Sl. No.	Picture(s)	Plain-picture	Cipher-picture	Local Shannon
1.	Lena	7.17186	7.92171	7.97551
2.	Black	7.16156	7.95672	7.97272
3.	Baboon	7.27185	7.93193	7.97183
4.	Chessboard	7.40114	7.91984	7.97564

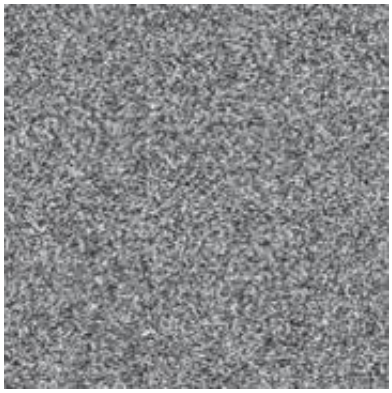
(a) Real picture



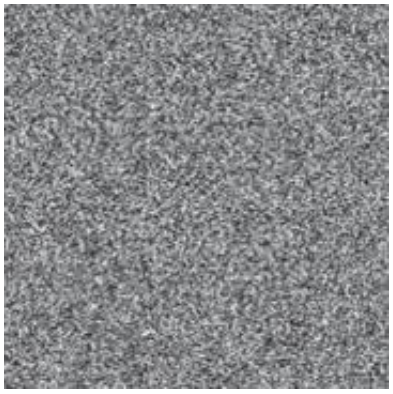
(b) Encrypted picture Using code c1



(c) Encrypted Picture Using code c2



(d) Difference picture of (b) & (c)



(e) Decrypted picture using Wrong code c1

(f) Decrypted picture using right code c2

Figure 5: Illustrates original and corresponding decrypted selected picture of Chessboard. The selected Chessboard picture were encrypted by two different code words c1 and c2.

The privacy of the pictures is one of the primary concerns during image transmission over communication channels. The privacy of the pictures is becoming more difficult at present due to multifarious reasons. This modified AES algorithm provides high secrecy for multifarious picture formats by applying the separate code word to various pictures to puzzle the strikers. Figure 5 shows the original picture and the corresponding decrypted selected picture of the Chessboard and herein the selected Chessboard picture was encrypted by two separate codewords c1 and c2 to puzzle the strikers. Table 2 shows the information entropy with local entropy of selected pictures for this test. This table depicts the diverse values of plain-picture, cipher-picture, local Shannon for all selected test images as illustrated in Table 2.

CONCLUSION AND IMPLICATION

Image security and privacy are a primary concern now a days to secure confidential data during the transmission over the communication network. There have been investigated numerous approaches to secure confidential data from the strikers by investigating various image encryption algorithms. In the past, various researchers validated many image encryption algorithms for image security but these traditional algorithms have certain limitations for all image formats and pixel sizes. Moreover, these existing algorithms have more computational complexity which demands more attention towards this problem. In this study, the authors investigated another novel picture encryption method by utilizing the modified AES algorithm. This explored picture encryption method is more appropriate for modern communication systems as it has very little computational complexity. The measured results are more appropriate and validated with a high degree of precision with a personal computer having a configuration of 64-bit with 6GB RAM in window 10. For this experiment MATLAB R2018b software was used and the measured results are validated with a high degree of precision. The NPCR and UACI amounts for every selected picture are 99.6812, 99.7013, 99.7215, 99.7617 and 33.3011, 32.3120, 33.4688, 33.3164 respectively. These measured results show that this algorithm is more fast and reliable in comparison to the traditional algorithms. Although much research work has been done regarding image encryption by investigating novel algorithms there is a pragmatic scope of more research in this domain to find the solution to the existing problems.

REFERENCES

[1] G. Chen, Y. Mao, and C. K. Chui, "A symmetric image encryption scheme based on 3D chaotic cat maps," *Chaos, Solitons and Fractals*, 2004, doi: 10.1016/j.chaos.2003.12.022.

[2] Y. Wang, K. W. Wong, X. Liao, and G. Chen, "A new chaos-based fast image encryption algorithm," *Appl. Soft Comput. J.*, 2011, doi: 10.1016/j.asoc.2009.12.011.

[3] C. Li, G. Luo, K. Qin, and C. Li, "An image encryption scheme based on chaotic tent map," *Nonlinear Dyn.*, 2017, doi: 10.1007/s11071-016-3030-8.

[4] M. A. Murillo-Escobar, C. Cruz-Hernández, F. Abundiz-Pérez, R. M. López-Gutiérrez, and O. R. Acosta Del Campo, "A RGB image encryption algorithm based on total plain image characteristics and chaos," *Signal Processing*, 2015, doi: 10.1016/j.sigpro.2014.10.033.

[5] M. Khan and T. Shah, "A Literature Review on Image Encryption Techniques," *Autoimmunity Highlights*. 2014, doi: 10.1007/s13319-014-0029-0.

[6] S. Liu, C. Guo, and J. T. Sheridan, "A review of optical image encryption techniques," *Opt. Laser Technol.*, 2014, doi: 10.1016/j.optlastec.2013.05.023.

[7] Y. Li, C. Wang, and H. Chen, "A hyper-chaos-based image encryption algorithm using pixel-level permutation and bit-level permutation," *Opt. Lasers Eng.*, 2017, doi: 10.1016/j. optlaseng.2016.10.020.

[8] E. Setyaningsih and R. Wardoyo, "Review of Image Compression and Encryption Techniques," *Int. J. Adv. Comput. Sci. Appl.*, 2017, doi: 10.14569/ijacsa.2017.080212.

[9] M. Panda, "Performance analysis of encryption algorithms for security," 2017, doi: 10.1109/SCOPES.2016. 7955835.

[10] R. K. Rajinder Kaur, "Image Encryption Techniques:A Selected Review," *IOSR J. Comput. Eng.*, 2013, doi: 10.9790/0661-0968083.