Journal of Current Research in Engineering and Science
Bi-Annual Online Journal (ISSN: 2581 - 611X)
Volume7-Issue2, January 2024
Paper: 6

An image encryption based on hyperchaotic sequence using AES – CBC

Sri Rishitha B V, Rahul Subbiah Ganesan, Afra Nahar A, and Dr.J. Selvakumar

Department of Electronics and Communication Engineering,

SRM Institute of Science and Technology, Kattankulathur, Tamil Nadu, India – 603203.

sb2560@srmist.edu.in , rs9761@srmist.edu.in , aa6937@srmist.edu.in

Abstract: In an age of rapid technological innovation, protecting sensitive visual data during transmission and storage is critical. In order to address the limitations of conventional methods, this work provides a revolutionary image encryption methodology that combines Hyperchaotic systems with CBC-AES (Cipher Block Chaining-Advanced Encryption Standard). Our hybrid technique improves the security of CBC-AES by utilizing the chaotic character of Hyperchaotic systems and adding a high-dimensional key space for more unpredictable and complex encryption. The method effectively uses CBC-AES for robustness and speed in picture block encryption. A thorough analysis, encompassing parameters like encryption speed, key sensitivity, and resilience to frequent attacks, confirms the efficiency and excellence of our suggested method for protecting image data.

Keywords:ImageEncryption,AdvancedEncrptionStandards(AES),CBC(CipherBlockChaining), Hyperchaotic systems, SHA512,Pixelshuffling,Performance analysis.

1. INTRODUCTION:

THIS focuses on developing an image encryption scheme that combines the widely used Cipher Block Chaining (CBC) mode of the Advanced Encryption Standard (AES) algorithm with the chaos theory-driven hyperchaotic system.[3][5][6] By leveraging the inherent unpredictability and complexity of hyperchaotic systems, this hybrid approach aims to enhance the cryptographic strength of the encryption process, thereby fortifying the protection of sensitive visual information. The hyperchaotic system, characterized by a higher degree of complexity compared to traditional chaotic systems[3], introduces a new dimension of unpredictability[7], which is crucial for thwarting sophisticated attacks. Paired with the CBC-AES algorithm, which provides a secure and efficient block cipher operation, this amalgamation seeks to create a robust and adaptable image encryption framework.

The CBC-AES algorithm operates on blocks of data, ensuring that each encrypted block depends on the previous one, effectively eliminating patterns and enhancing the overall security of the encrypted image. The integration of hyperchaotic dynamics into this process aims to further amplify the chaotic behavior[13], introducing a layer of non-linearity and randomness that significantly strengthens the encryption scheme against potential adversaries.

1. Theoretical methodology

1.1 The hyperchaotic system: The hyperchaotic system is a nonlinear dynamic system that is employed in the permutation and scrambling operations of encryption techniques [6][8][4]. The system is defined by a system of differential equations called the Rossler attractor [1], which are as follows:

Journal of Current Research in Engineering and Science
Bi-Annual Online Journal (ISSN: 2581 - 611X)
Volume7-Issue2, January 2024
Paper: 6

$$dx/dt = -y - z \quad \ldots\ldots(1)$$
$$dy/dt = x + a * y \quad \ldots\ldots(2)$$

$$dz/dt = b + z * (x - c) \quad \ldots\ldots(3)$$

where a, b, and c are the system's parameters. When three parameters are tuned to values 14 for c, 0.1 for b, and 0.1 for a The system behaves in a hyperchaotic manner.This hyperchaotic state of the system is indicated by positive Lyapunov coefficients, a measure of its chaotic behavior. The NIST test [14], which it passed, further attests to its high degree of security. By employing the Runge-Kutta technique to iterate the system with a step size of 0.001, phase diagrams are generated that show the behaviour of the system.

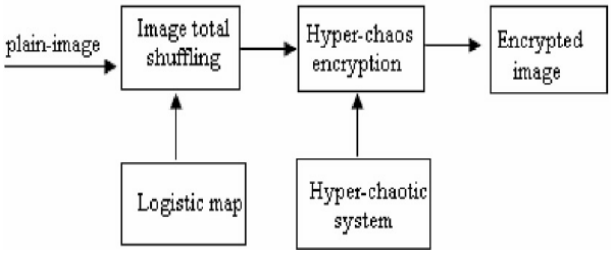


Fig 1: Hyperchaotic System

1.2 Changing the picture's greyscale format: The method transforms an input image into a grayscale representation in this stage [7]. Only shades of grey are used to represent each pixel in a grayscale image, simplifying the data while maintaining the key elements of the image. The picture data's complexity is decreased in this stage [7].

1.3 Making a hyperchaotic sequence with the Rossler system: One kind of chaotic dynamical system with three differential equations is the Rossler system [1]. Its behavior is complex and unpredictable, which is what makes it useful for creating sequences that seem random. The algorithm generates a hyperchaotic sequence by utilizing the Rossler system. You can think of this sequence as a stream of values that are somewhat random [1].

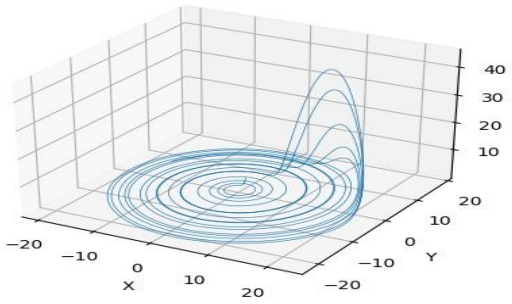


Fig 2: Rossler diagram

1.3 Using SHA-512 to compute a hash from the hyperchaotic sequence: The hyperchaotic sequence is subjected to the SHA-512 cryptographic hash function by the procedure [7][10]. This stage creates a fixed-length, secure hash from the continuous hyperchaotic sequence. In addition to acting as a representation of the sequence, the hash may be used to generate a key for further

Journal of Current Research in Engineering and Science
Bi-Annual Online Journal (ISSN: 2581 - 611X)
Volume7-Issue2, January 2024
Paper: 6

encryption processes.

1.4 Using a random number generator seeded with the hashed key: A random number generator (RNG) uses the hashed value from the previous phase as its seed. Based on this seed, the RNG will generate a series of pseudo-random numbers. The same sequence of pseudo-random numbers is produced each time the procedure is run using the same picture if a consistent seed is used.

1.5 Using the random number generator, shuffle the indices that indicate the locations of the pixels: The approach shuffles the indices, which indicate the pixel locations in the grayscale image, using a pseudo-random number generator. Rearranging [10] the indices causes the pixels to seem to be rearranged randomly, producing a permutation that may be utilized to change the order of the pixels [3].

1.6 Using the shuffled indices to reorder pixels to create a new image: The technique reorganizes the grayscale image's pixels using the shuffled indices [3]. The outcome is a new picture with rearranged pixels according to the pseudo-random number generator's random-like permutation [10]. The new picture is basically the grayscale original image with encryption applied. The same seed and set of processes would need to be repeated in reverse to shuffle and unshuffled the pixel locations to decode the picture.

In summary, the "Hyperchaotic System" algorithm converts an image to grayscale, creates a hyperchaotic sequence, hashes the sequence to produce a key, rearranges the pixels to create an encrypted version of the original image, and applies chaos theory and cryptography techniques to transform and secure an image [3][10].

2. SECURITY ANALYSIS BY STATISTICAL APPROACH

Advanced cryptographic techniques, like Hyperchaotic dynamics, are being integrated with the Advanced Encryption Standard (AES) algorithm's Cipher Block Chaining (CBC) mode in the rapidly changing field of image encryption[4][5], has gained significant attention. To ensure the robustness and efficacy of the proposed encryption scheme, a comprehensive statistical analysis is imperative. This research focuses on employing a range of statistical methods to evaluate the cryptographic strength and security of an image encryption system based on Hyperchaotic dynamics and CBC-AES algorithm. the paper.

2.1 Key Space Analysis: The encryption method generates the encryption key using the SHA-512 technique [7][10]. The given key space for SHA-512 is 2^256. The hyperchaotic system furthermore has four starting values with key spaces of 10^30 each. Consequently, the encryption algorithm's total key space is computed to be 1.157×10^107.

Journal of Current Research in Engineering and Science
Bi-Annual Online Journal (ISSN: 2581 - 611X)
Volume7-Issue2, January 2024
Paper: 6

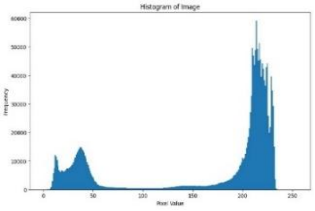
2.2 Sensitivity Analysis of Encryption Keys: During the encryption process, the sensitivity of the encryption key is evaluated. Key sensitivity is the degree to which small changes in the key cause large changes in the cipher.. Equations are used to quantify NPCR [2] and UACI [2]. For NPCR and UACI [2], the predicted values are 100% and 33.4635%, respectively. A cameraman, Fruits and Pepper picture is used in the example to show how significant differences in NPCR and UACI values can result from even a tiny key change, on the order of 10^-12, between the original and cipher image. This illustrates how sensitive the encryption algorithm is to variations in the encryption key. The test known as Number of Pixel Change Rate, or NPCR, is used to quantify the avalanche effect in image encryption [11].The average intensity of the differences between the plain and encrypted images is shown by the Unified Average Change Intensity (UACI) [12].

2.3 Sensitivity Analysis of Decryption Keys: Numerous metrics, including pixel change rate (NPCR) [11][2], pixel average change intensity (UACI) [10][11], The summary excludes specific mathematical formulas that are used to quantify these measures. This section essentially emphasizes the significance of determining key sensitivity throughout the decryption process and use these metrics to compare the altered and decrypted pictures**.**

2.4 The Histogram Analysis: Histograms are used as statistical markers in photos, displaying the distribution of pixel values. The original mxn (m,n are the dimension of original images) original images and their histograms are compared with the corresponding cipher pictures in this section. The pixel value distributions of the original photographs are relatively concentrated, exhibit statistical properties, and are susceptible to brute force assaults. On the other hand, the cipher pictures' pixel values display a more consistent distribution, defying the statistical characteristics rule. This indicates great resistance to statistical assaults by making it difficult for attackers to retrieve the original image using statistical information. The chi-square ($\chi 2$) distribution is used to quantify the distribution law of the pixel histogram [7] [11], and a formula for computing this distribution is given.

IMAGE 1:

Original image 1 Histogram of original image

Encrypted image Histogram of encrypted image

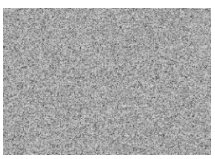
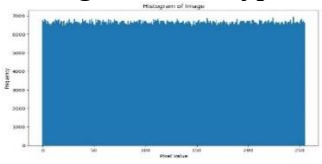
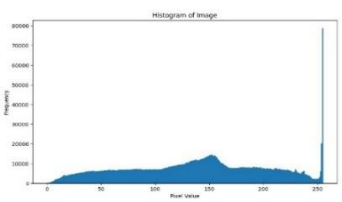



IMAGE 2:

Original image 2 Histogram of original image

Journal of Current Research in Engineering and Science
Bi-Annual Online Journal (ISSN: 2581 - 611X)
Volume7-Issue2, January 2024
Paper: 6

Encrypted image Histogram of encrypted image

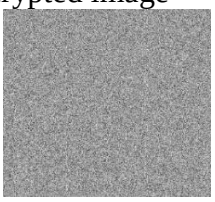
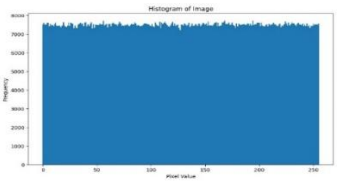
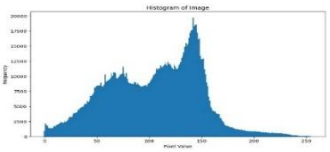



IMAGE 3:

Original image 3 Histogram of original image

Encrypted image Histogram of encrypted image

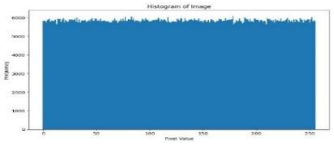



Fig 3: The Histograms of the original image and encrypted image

2.5 Entropy Analysis: This section explores the idea of information entropy analysis [11], which is used to measure and assess information within the context of pictures. The unpredictability and uniform distribution of pixel values inside a picture are measured using information entropy. Every pixel in a grayscale picture has 256 potential states, and each state has a chance of 1/256. The optimal information entropy for a totally random picture is 8. Equation [12] gives the information entropy formula, in which "p(i)" stands for the probability of each pixel [13].

Entropy and correlation: Let m be an image of size N.

The entropy of m is given as,

$$H(m) = \sum_{0}^{M-1} p(m_i) \log \frac{1}{p(m_i)}, \quad (4)$$

where m is the number of grey levels that repeat themselves and p(mi) = n/N is the correlation of the pixel mi.

TABLE I. Entropy of the original and encrypted images using the suggested and AES encryption techniques, respectively.

Images	**Encrypted Images**		
	Original image	***AES Encryption method***	***Proposed Encryption Method***
IMAGE 1	7.0097	7.9966	7.9971
IMAGE 2	7.5691	7.9974	7.9975
IMAGE 3	7.6284	7.9984	7.9986

Journal of Current Research in Engineering and Science
Bi-Annual Online Journal (ISSN: 2581 - 611X)
Volume7-Issue2, January 2024
Paper: 6

3. Modified Methodology

Developing a hyperchaotic image encryption methodology using the AES-CBC (Cipher Block Chaining) mode involves the creation of a sophisticated system for image encryption and decryption, integrating the Rossler hyperchaotic system and SHA-512 hashing to ensure heightened security. The Rossler system, defined by parameters a, b, and c, acts as the underpinning mechanism for generating a hyperchaotic sequence through numerical integration. This dynamic sequence serves as the cornerstone for constructing a robust cryptographic key, employing the SHA-512 hashing algorithm to enhance its security characteristics. During the encryption phase, the grayscale image undergoes a complex shuffling process, intricately tied to the generated key. The result is an encrypted version of the image, strategically securing its contents from unauthorized access.

Importantly, this encryption and decryption methodology is designed for implementation on an FPGA (Field-Programmable Gate Array), adding a layer of formality and efficiency to the system. Leveraging FPGA technology allows for hardware-based acceleration, enhancing the computational speed and efficiency of the encryption process. This implementation on an FPGA platform aligns with industry trends seeking to optimize cryptographic operations through hardware acceleration, ensuring a more robust and swift response to the increasing demand for secure image communication and storage. The combination of hyperchaotic dynamics, SHA-512 hashing, and FPGA implementation underscores a commitment to a comprehensive and efficient approach to image encryption in a security-conscious environment.

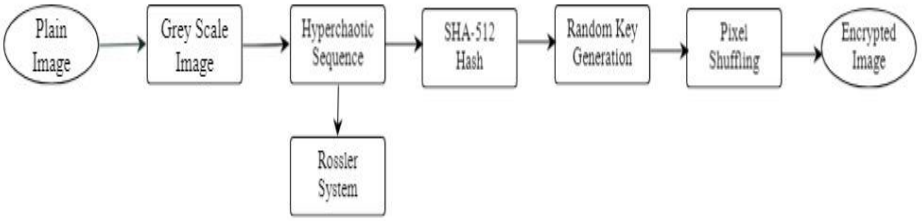


Fig 4: Block *diagram for proposed methodology*

TABLE II. Comparison of NPCR, UACI of AES-CBC encryption

Criteria (expected value)	**Original image vs Encrypted image**		
	name	***AES Encryption method***	***Proposed Encryption method***
NPCR(99.61%)	IMAGE 1	99.5911%	99.999%
	IMAGE 2	99.6155%	99.999%

Journal of Current Research in Engineering and Science
Bi-Annual Online Journal (ISSN: 2581 - 611X)
Volume7-Issue2, January 2024
Paper: 6

Criteria (expected value)	Original image vs Encrypted image		
	name	***AES Encryption method***	***Proposed Encryption method***
	IMAGE 3	99.6521%	99.999%
UACI(33.46%)	IMAGE 1	31.0664%	31.24440%
	IMAGE 2	30.5720%	30.83742%
	IMAGE 3	36.2764%	36.46578%

4. Conclusion

In conclusion, this study presents a meticulously designed hyperchaotic image encryption methodology implemented in AES-CBC mode. By seamlessly integrating the Rossler hyperchaotic system, SHA-512 hashing, and FPGA technology, a robust framework is established to elevate the security standards in image communication and storage. The dynamic sequence derived from the Rossler system's parameters forms a resilient cryptographic key, further fortified by SHA-512 hashing.
The encryption phase employs a refined shuffling process intricately tied to the generated key, ensuring a steadfast defense mechanism for the grayscale image's contents against unauthorized access. Importantly, the methodology is optimized for FPGA implementation, introducing a layer of formality and efficiency. FPGA technology, with its hardware-based acceleration, significantly enhances the computational speed and efficiency of the encryption process.
Aligned with current industry trends prioritizing cryptographic optimization through hardware acceleration, the convergence of hyperchaotic dynamics, SHA-512 hashing, and FPGA technology underscores a commitment to a comprehensive and efficient approach to image encryption within a security-conscious environment. As technology continues to advance, the ongoing exploration and refinement of such integrated systems are essential to proactively address evolving cybersecurity challenges and ensure the robust protection of sensitive image data in the ever-evolving technological landscape.

5. Acknowledgment

We would like to acknowledge the help provided by **Dr. J Selvakumar** for his direction, counsel, and unwavering support throughout this work as a lecturer in the Faculty of Electronics and Communication Engineering at the SRM Institute of Science and Technology. His support has been crucial to making this work a reality**.**

6. References

1. Christophe Letellier, Dr. Otto E. Rossler , " A Rossler attractor", 2006.

2. Y. Wu, S. Member, J.P. Noonan, and L. Member, "NPCR and UACI Randomness Tests for Image Encryption", Cyber Journals Multidiscip. Journals Sci. Technol. J. Sel. Areas Telecommun., no. APRIL 2011, pp. 31–38, 2011.

3. Huang, C.K., Liao, C.W., Hsu, S.L. et al. "Implementation of gray image encryption with pixel shuffling and gray-level encryption by single chaotic system.", 2013.
4. Xuanping Zhang · Yanbin Mao · Zhongmeng Zhao, " An efficient chaotic image encryption based on alternate circular S-boxes ", 20 May 2014.

5. Salim Muhsin Wadi · Nasharuddin Zainal," High Definition Image Encryption Algorithm Based on AES Modification ", 26 June 2014.

6. Asst. Prof. Dr. Alia Karim Abdul Hassan," Proposed Hyperchaotic System for Image Encryption ", 2016.

7. Vinita Shadangi1 , Siddharth Kumar Choudhary1 , K. Abhimanyu Kumar Patro1 and Bubhudendra Acharya, " Novel Arnold Scrambling Based CBC-AES Image Encryption ", 2017.

8. Abolfazl Yaghouti Niyat, Mohammad Hossein Moattar∗ , Masood Niazi Torshiz," Color image encryption based on hybrid hyper-chaotic system and cellular automata", 2017.

9. Heidilyn V. Gamido1 , Ariel M. Sison2 , Ruji P. Medina3, " Implementation of Modified AES as Image Encryption Scheme ", September 2018.

10. Manjit Kaur1 • Vijay Kumar1, " A Comprehensive Review on Image Encryption Techniques ",24 November 2018.

11. X. Zhang, L. Wang, Z. Zhou, and Y. Niu, "A chaos-based image encryption technique utilizing hilbert curves and h-fractals," IEEE Access, vol. 7, pp. 74734–74746, 2019.

12. Chih-Hsueh Lin 1 , Guo-Hsin Hu 1,2, Che-Yu Chan 1 and Jun-Juh Yan 3," Chaos-Based Synchronized Dynamic Keys and Their Application to Image Encryption with an Improved AES Algorithm",2021