Journal of Integrated
SCIENCE & TECHNOLOGY

Henon Maps based selective image encryption approach for enhanced control and security

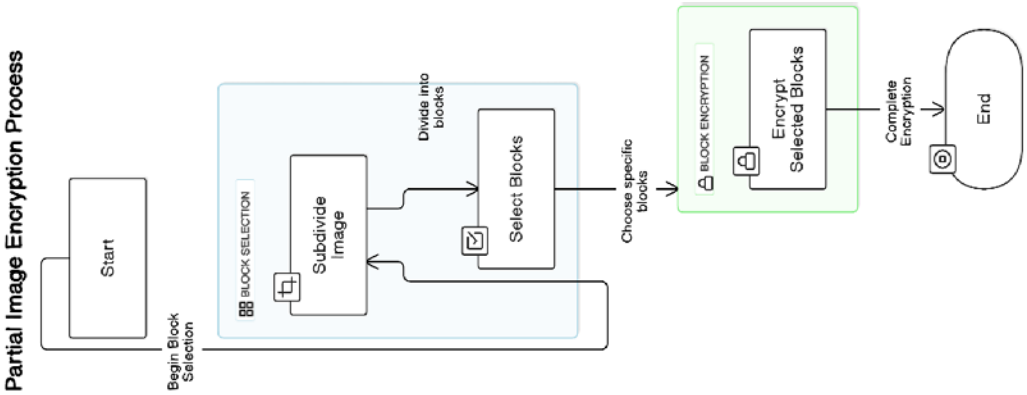
Sudheesh K V[1], Benaka Santhosha S[2*], Kiran Puttegowda[1]

[1]Department of ECE, Vidyavardhaka College of Engineering, Mysuru, Visvesveraya Technological University, Belagavi, Karnataka, India. [2]Department of CSE, Dayananda Sagar University, Harohalli, Bengaluru, Visvesveraya Technological University, Belagavi, Karnataka, India

Submitted on: 02-Aug-2024, Accepted and Published on: 23-Oct-2024

Article

ABSTRACT In the modern world where the use of hard drives and networks cannot be underestimated, the protection of information is of equal importance and especially so with images. Encryption remains as an introductory safeguard that helps to protect the privacy of the image data and obscure specific data. Nevertheless, encryption of images implies encrypting every pixel in the image or, in other words, encrypting entire images can sometimes take longer time than expected to compute; therefore, it can be disadvantageous when it comes to real-time activities. Partial image encryption comes out as a solution, one that only encrypts the areas of an image that needs protection while greatly lessening the number crunching requirements. In this regard, we present a block based partial image encryption scheme. Using the Henon Map as a basis, we randomly encode image blocks to meet the specified requirements of further encryption. Increasing or decreasing the level of encryption is performed by means of modifying the control threshold value. Research data in the field shows that encryption time experiences a significantly low value in comparison to full image encryption, which makes this technique work as an effective option for real-time applications. The proposed approach presented in this paper demonstrates advantages of increasing the security of digital images while incurring low computational costs, making it a possible line of protection for digital images in flexible operational environments.



Keywords: Selective encryption, Henon Map, Control threshold, image Security

INTRODUCTION

In recent years, multimedia technology and internet usage has grown exponentially and hence require larger storage capacity and higher levels of security provision. As with this surge, we are faced with numerous risks that put the privacy of transmitted and stored content at risk. However, protection of images in the digital environment remains as one of the biggest challenges in this digital world. Encryption comes out as the most dominant approach in safeguarding information from unauthorized invasion by attackers. However, much needed computation in encryption and decryption of digital images becomes a drawback especially in real-time applications. Encryption methodologies are broadly categorized into two domains: There are methods of full image encryption and selective (partial) image encryption, using basic ciphers such as AES, DES, as well as cipher streams.[1,2]

Due to the high time consumption required for encrypting and decrypting digital images, many researchers have pursued partial image encryption. This approach is designed not only to improve security, but also to address the issue of computational overhead. Partial image encryption means the encryption of specific segments of an image that might contain relevant information in certain regions of image bits, blocks or pixels, using position shifting,

*Corresponding Author: Benaka Santhosha S, Department of CSE, Dayananda Sagar University, Harohalli, Bengaluru. Email: benaka.santhosh-cse@dsu.edu.in

Cite as: *J. Integr. Sci. Technol., 2025, 13(2), 1034.*
URN:NBN:sciencein.jist.2025.v13.1034
DOI:10.62110/sciencein.jist.2025.v13.1034

swapping or both. In recent research undertakings, several novel selective encryption techniques have been developed to some image encryption issues.[3,4]

The subsequent sections of this paper provide an overview of the Henon map utilized in the proposed methodology, followed by the detailed explanation of the proposed approach in Section III. Experimental analysis and concluding remarks are presented in Sections IV and V, respectively.

LITERATURE SURVEY

M. Packirisamy et al.[5] introduced An adaptive-selective image encryption method which offers enhanced user control and security by utilizing JSMP map, OPT, and dynamic permutation matrix, catering to varying encryption levels efficiently. Qamar Natsheh et al.[6] introduces an automatic selective encryption approach for DICOM images, enhancing security by encrypting important regions differently, reducing processing time significantly, and maintaining robustness against attacks. Tariq Khan et al.[7] put forward a selective encryption method, a flexible, generic and reusable architecture for securely conveying only that subset of the control information which is deemed by the process engineer of a constrained environment critical for the smooth operation of the overall process, to the controller with restricted access to its own memory with purposes and security of the communicated information certified at the target control environment. Cheng Wei et al.[8] introduced a new multi-dimensional hyperchaotic system develop from logistic map and ICMIC based on closed-loop coupling (LICC) hyper-chaotic systems and it is employed in selective image encryption. Qiqi Cun et al.[9] proposed a new one-dimensional map with higher Lyapunov coefficients and dynamic performance and optimized the local graph structure algorithm to select the image area More suitable, and use the chaotic map created in this paper generate pseudo random sequences for dynamic encoding and manipulation of the selected DNA area. Ali Soleymani et al.[10] also proposed the Ecc and chaotic maps combined system which identifies face(s) in the image and then encrypt only 5% of the whole image and only confidential areas of the image not the whole image. L salman et al.[11] has come up with a selective image encryption method in the paper that improves on efficiency by selectively encrypting sections of an image using polynomial based secret image sharing and a chaotic map. Oulaya Berrak et al.[12] describes a a new selective mode of image encryption by selected cascade of interesting regions and the use of stream cipher encryption is being proposed hence comparison has been done in accordance with the parameters such as histogram, correlation coefficient, entropy value and PSNR value.

Hassan N. Noura et al.[13] provides format-compliant compression-selection cipher, which can be incorporated together with lossless as well as lossy image compression techniques. And the cipher variants introduced in the paper utilize the compressed data properties including randomness and uniformity compared to uncompressed data and thereby make the proposed solution different from the previous ones. Lahieb Mohammed Jawad et al.[14] proposes a novel selective image encryption approach using GLCM texture features and Faster R-CNN for object detection, enhancing security by encrypting specific regions based on object roughness criteria. Wang et al.[15] as mentioned in the proposed a secure scheme for social image dissemination on social media platform, which establish a map between the tree structure haar (TSH) transform and the hierarchical community structure of a social network. Apoorva Aggarwal et al.[16] proposed algorithm integrates Modified Moth Flame Optimization and Logistic Chaotic Map for enhanced image encryption, achieving high security with improved evaluation parameters and de-correlation of adjacent pixels. Hazem Al-Najjar et al.[17] introduced image encryption algorithms utilizing chaotic functions with pixel data, ensuring high sensitivity and enhanced security through complete image transformation with minimal alterations. Ram Ratan et al.[18] proposed an encryption technique which reveals that encrypting only the four most significant bit-planes in image encryption may not provide adequate security, especially in histogram equalised images.

The survey on selective image encryption reveals a variety of innovative approaches that have emerged to enhance the security, efficiency, and control of image encryption processes. Different methodologies like adaptive-selective encryption, automatic region-based encryption, chaotic maps, and cryptosystems combining ECC and chaotic functions were developed to selectively encrypt sensitive image regions while minimizing computational overhead. Proposed approach increase the efficiency and flexibility of selective image encryption, making it highly applicable to real-time and resource-constrained environments.

HENON MAP

The Henon map, as described by V. Rathore et.al.,[19] is a tool to produce non-sequence random values for two-dimensional chaotic systems. These maps are much more useful in defining sequences that are inherently dynamic, showing significant sensitivity to conditions within the sequence at its onset and exhibiting unpredictable attributes in their overall behavior. The Henon map works under the iterative form with the following two equations to refresh the x and y values. This iterative character guarantees that the sequences generated are not only random but also free of repeating patterns a fairly large number of times – necessary for many practical applications that require strong security measures, including encryption in medical image analysis. Because of the characteristics of the Henon map, this paper seeks to prove that it is an optimal map for achieving randomness when securing sensitive medical data. Equation 1 gives Henon map System.

$$x_{n+1} = 1 - ax^2{}_n + y_n \qquad (1)$$
$$y_{n+1} = bx_n$$

PROPOSED METHODOLOGY

The proposed partial image encryption method, illustrated in Figure 1, employs the Henon map and consists of two primary stages: one of them are block selection and the other one is the block encryption. In the block selection stage, the image is subdivided into some number of blocks, then for encryption purposes, only particular blocks will be selected for such a process against the remaining ones, making the process selective in the sense that it only gets to work on a section of the image. This approach entails

lower computation costs while at the same time affording a reasonable degree of security.

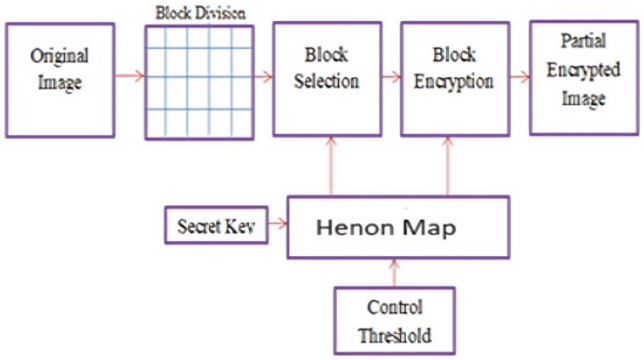


Figure 1. Proposed selective encryption scheme

The proposed partial image encryption method, illustrated in Figure 1, utilizes the Henon map and involves two main stages: block selection and block encryption.

Stage 1: Block Selection:

Selective encryption commences by selecting blocks and the usual approach of partitioning an original image of size P*Q into 16 * 16 blocks called macro blocks. This segmentation makes the image simpler and the features to which encryption must be applied can be applied selectively. It is done purposely for the block selection, to be random, a logistic sine map is used on the selected macros. This map type has a default set of initial parameters by which it generates random numbers. These random numbers are then used to choose precise 16×16 macro pixels inside this picture. The level of encryption is regulated by a threshold value unknown. This means that high threshold selects many blocks to be encrypted and so the security of the image increases while a low threshold will encrypt few blocks and so the image security and computational time are balanced. This makes the encryption process flexible to different security considerations to embrace the ideal solution.

Stage 2: Block Encryption:

In the encryption process the key image originating from the LSM is also quantized into 16x16 macro blocks. For each macro block randomly chosen in the original image, the pixel value of the macro blocks undergoes a bitwise XOR with the pixel in the key image block. This operation helps to only encrypt a portion of the image, resulting in a partially encrypted image. This method is efficient and secures the images because they do not employ general image encryption, instead they work on block-level encryption. This way of eliminating domains lowers the required number of computational procedures while ensuring sufficient levels of security.

As previously explained, the decryption process is the reverse of the encryption process. The encrypted image is for input into the decryption algorithm as shown in figure 2 below where the image is divided into a macro block of the size 16×16 in size. Consequently, logarithmic tendency numbers decided by the control threshold of the logistic sine map select random macro blocks for decryption. The selected random block of the LSM is then compared to the key image for a key image block where the pixel values for the pixels in the selected random blocks are bitwise XORed against the pixel values in the key image blocks. This operation serves to reverse the encryption and yield back the decrypted image.

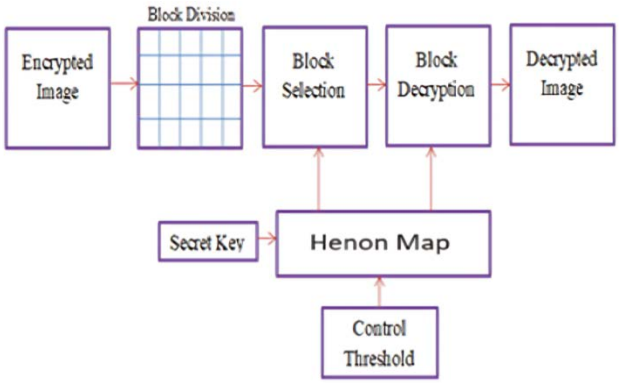
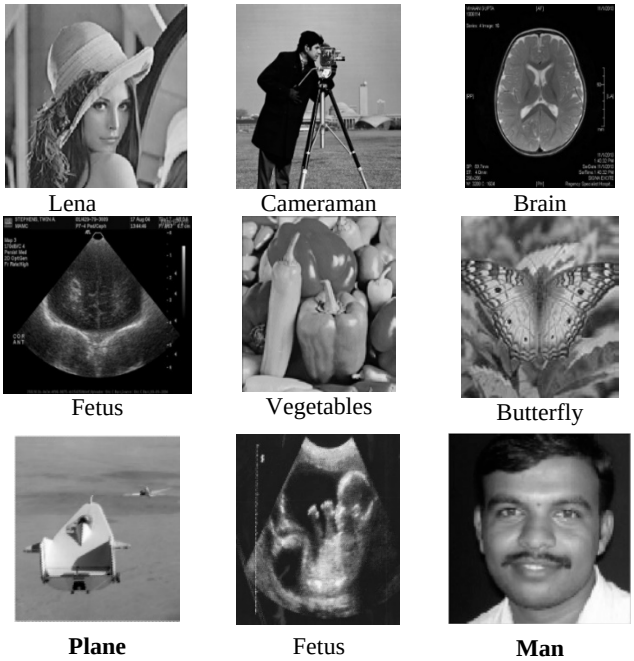


Figure 2. Proposed selective decryption scheme

PERFORMANCE EVALUATION

In this section, we validate and evaluate the performance of the proposed methodology using MATLAB 2022b for simulation purposes. Table 1 presents the set of test images utilized in the simulations, all standardized to a size of 256 × 256 pixels. The proposed algorithm leverages secret keys (r=3.74361) and ($x(1) = 0.587923$) for the Henon map. To thoroughly assess the effectiveness of the proposed method, various performance metrics are employed. These metrics include measures of encryption quality, computational efficiency, and robustness against attacks, ensuring a comprehensive evaluation of the methodology's capabilities. The subsequent sections will detail these performance metrics and the corresponding results obtained from the simulations.

Table 1. Datasets used for current work



Histogram analysis

The image histogram refers to a graphical representation of the pixel density within an image depending on their frequency. Of all the graphical analysis techniques, especially in high security encryption technique, the histogram of the cipher image should perfectly be uniform. Perfectly distributed Histogram proves that the pixel values of the encrypted image are distributed uniformly on all levels of intensity and is presented in Table –VI. Such throughout consistency indicates that the pixel values have indeed been randomized by encryption so that hostile forces cannot decipher structures or gain insights out of the encrypted form of the image.

Therefore, evaluating the security of an encryption technique involves analyzing the histogram of the cipher image. A uniformly distributed histogram signifies a robust encryption process, which enhances the overall security of the encrypted data by ensuring no statistical information about the original image is revealed.

Entropy Analysis

Entropy is often time applied in image processing as a way of determining the amount of randomness in data contained within images. The formula for entropy, often cited in literature [13], is typically expressed as:

$$H(S) = \sum_{i=0}^{2^M-1} P(si) \log_2 \frac{1}{P(si)} (2)$$

And in image analysis, especially the cryptographic and security aspect of it, the entropy value of a random image with the of 8 bits per pixel should in fact be 8. This value represents the amount of noise or uncertainty within image to its optimum. When entropy is less than or equal to 8 this implies that it points to the fact that there may be trends prevailing which might pose a danger to the efficiency of encryption or data compression algorithms by posing some certainty. Discouragingly, low entropy leads to an increased foreseeability or predictability of the pattern or figure within the image.

Mean Square Error

The Mean Squared Error (MSE) measures how much the pixels values of the plain image are on average squared deviant from the pixels value of the encrypted image. The formula for MSE, cited from reference [13], is expressed as:

$$MSE = \frac{1}{MXN} \sum_{i=1}^{M} \sum_{j=1}^{N} [X(i,j) - Y(i,j)]^2 (3)$$

Number of Pixel Change Rate (NPCR)

The NPCR (Number of Pixel Change Rate), used to measure the change in pixel values between a simple image (C1) and its encrypted image (C2). The formula for NPCR, referenced from [13], is defined as:

$$NPCR = \frac{\sum_{i,j} D(i,j)}{MXN} X100\% (4)$$

Where D is bipolar array.

$$D(i,j) = \begin{cases} 1, C1(i,j) \neq C2(i,j) \\ 0, \quad otherwise \end{cases}$$

Peak Signal to Noise Ratio (PSNR)

Peak Signal-to-Noise Ratio (PSNR) is among the quality assessment parameters that compare the quality of an image with that of a reference image. It is usually expressed in decibel (dB) and has been found to be inversely proportional to the Mean Squared Error (MSE). The formula for PSNR, as cited from reference [13], is defined as:

$$PSNR = 10 \log_{10} \frac{255}{MSE} (5)$$

Unified average changed intensity (UACI)

The UACI (Unified Average Changed Intensity) is employed to calculate the intensity rate difference between plain image and its cipher form [13].

$$UACI = \frac{1}{N} \left[\sum_{i,j} \frac{|C1(i,j) - C2(i,j)|}{255} \right] (6)$$

Key space analysis

The key space means to describe a set of different keys that an algorithm can use in the processes of encryption and decryption. The best encryption is achieved when an algorithm has a key space of more than $2^{\wedge 128}$. Two pairs (x0, r) are used in the block selection of the proposed algorithm as well as in the block encryption process.

In our scheme, each key parameter of the henon map utilizes a key space of $10^{\wedge 15}$. Therefore, the key space for the proposed algorithm is calculated as $10^{\wedge 15} * 10^{\wedge 15} * 10^{\wedge 15} * 10^{\wedge 15} = 10^{\wedge 60}$, which significantly exceeds the threshold of $2^{\wedge 128}$. Additionally, the control threshold value can also function as a key. Overall, the proposed algorithm offers a substantial key space, ensuring efficient security measures.

Table 2. Control threshold 50% for encryption process

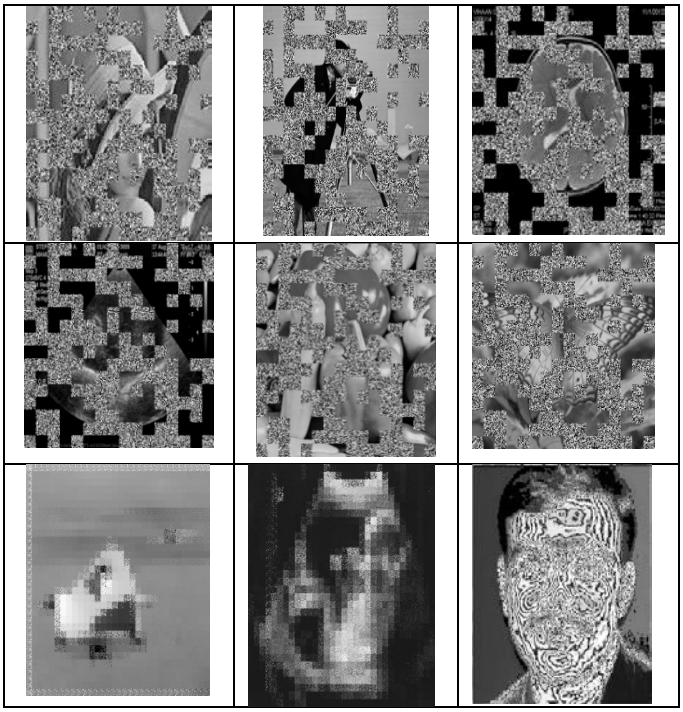


Table 3. Control threshold 75% for encryption process

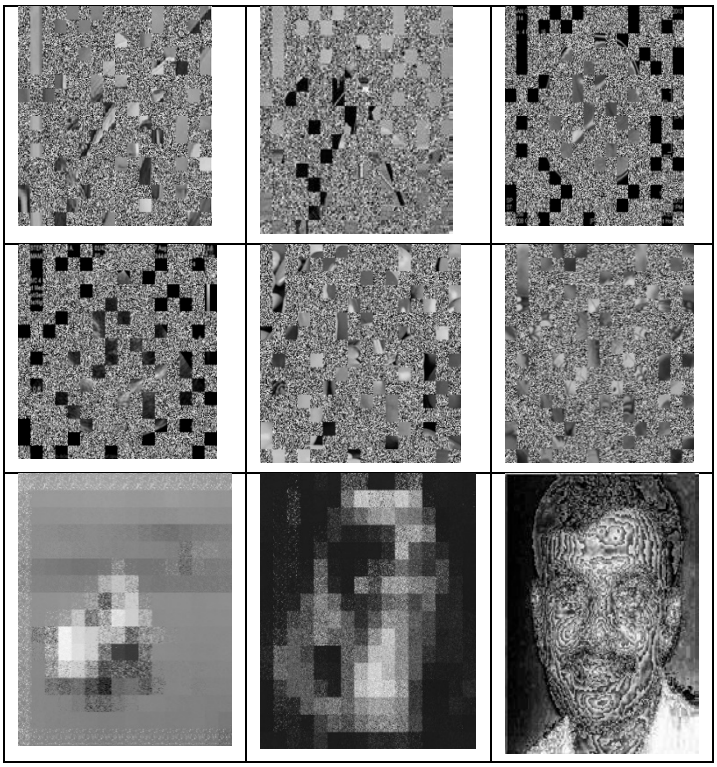


Table 4. Control threshold 100% for encryption process

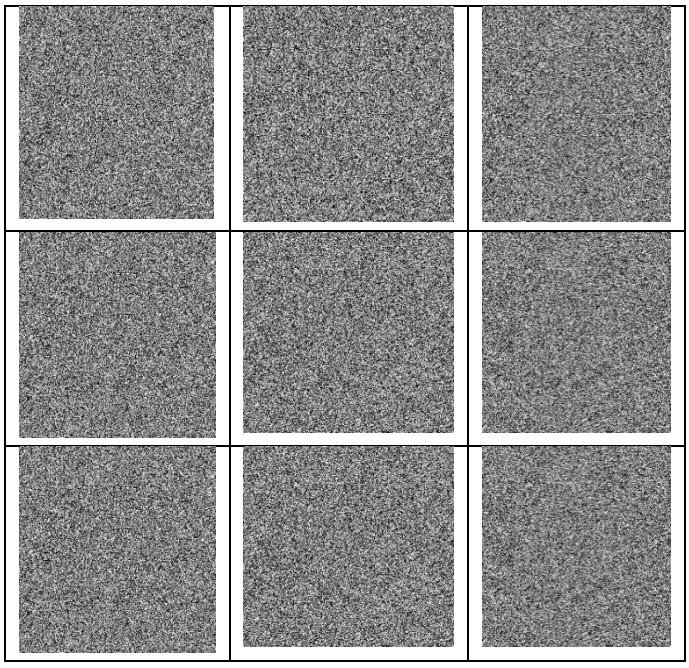
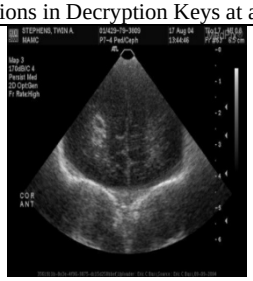
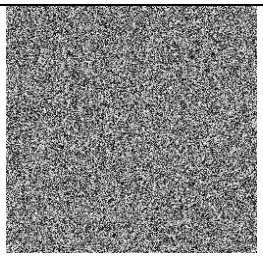


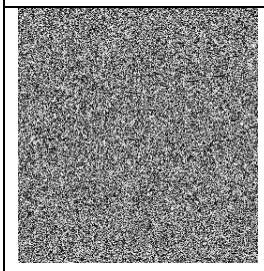
Table 5. Partially Decrypted MRI Images Displayed with Slight Variations in Decryption Keys at a Control Threshold Value of 100%



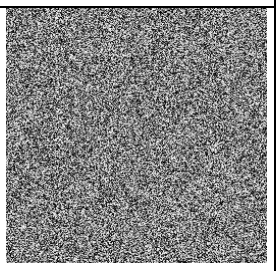
r=3.74361, x(1)=0.64432



r=3.74362, x(1)=0.64432



r=3.74363, x(1)=0.64432



r=3.74363, x(1)=0.64432

Table 6. Variation in Lena Image Histogram Analysis Across Various Control Values

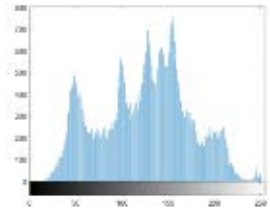
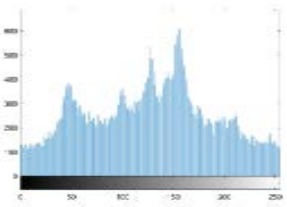
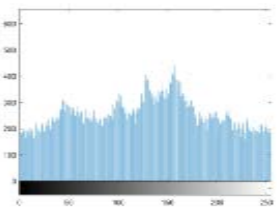
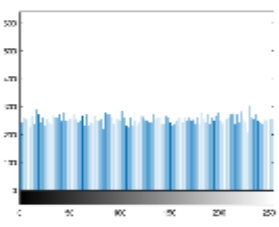
Histogram of original Lena	
50% threshold of Cipher Histogram	
75% threshold of Cipher Histogram	
100% threshold of Cipher Histogram	

Table 7. Performance Metrics Analysis at Various Control Threshold Levels

Parameters\Images	Lena			Brain			Vegetables		
	50%	75%	100%	50%	75%	100%	50%	75%	100%
Entropy-input(bit)	7.5110			5.1748			7.5808		
Entropy-output(bit)	7.9927	7.9346	7.9873	7.6791	7.8313	7.8970	7.8100	7.8774	7.897
MSE	45.29	74.52	93.23	38.18	37.21	45.34	42.79	62.95	129.45
PSNR (dB)	28.32	27.15	29.36	29.12	31.47	26.51	29.87	31.84	31.72
NPCR (%)	50	75	100	50	75	100	50	75	100
UACI (%)	22.36	31.82	31.03	30.35	26.21	33.76	23.15	31.16	26.39

Table 8. Comparative Analysis of Execution Time Across Various Control Threshold values

Images	Execution Time (secs)		
	50%	75%	100%
Lena	0.072	0.095	0.089
Cameraman	0.200	0.201	0.079
Brain	0.070	0.082	0.090
Fetus	0.061	0.74	0.086
Vegetables	0.082	0.086	0.083
Butterfly	0.071	0.081	0.097
Plane	0.072	0.076	0.073
Fetus	0.062	0.066	0.053
Man	0.052	0.056	0.063

Table 2, 3, 4 has the performance result of all the tested images at different control threshold values. With the increase of the control threshold values, the level of encryption is also high. Every control sequence requires the encryption of certain blocks depending on the control threshold value. Interestingly, the experimental results show that the proposed method can encrypt all the control threshold values to 100% as shown in table 4. The tables present various MRI decrypted images derived from the slight modifications in the secret keys as shown in Table 5. The fact that only with the help of the same secret keys it is possible to precisely decrypt the original image, can be mentioned, however, even if one decimal value is changed in chosen secret key, the encrypted image turns to be quite different. This clearly shows that the proposed algorithm is very sensitive to the secret keys proving the efficiency of the encryption method. Table 6 shows histograms of Lena original image and corresponding cipher images for different control thresholds values. This is because it is seen that histogram of the encrypted image has a uniform distribution when the threshold value is 100, this shows that the encrypting is high. For the other kinds of threshold, such as 50 and 75, the histogram seems to be slightly stochastic rather than uniform, reflecting partial encryption. In partial image encryption techniques, the key factor of concern is the execution time which dictates the feasibility of real-time solutions. Table 7 provides Performance Metrics Analysis at Various Control Threshold Levels provides a comprehensive overview of how different control threshold settings impact the performance of the system being evaluated. This table likely includes metrics such as entropy of input, output images, MSE, PSNR and range of threshold values. By examining these metrics, one can assess how well the system performs under varying conditions and determine the optimal threshold for balancing trade-offs between sensitivity and specificity. The complex evaluation allows concluding about the existence of the best working threshold, which establishes the level of efficacy and dependability corresponding to the given criteria. Table 8 contains the set of time results obtained while executing different images with different control threshold values. As clearly observed, when there is a lower value for control threshold, the execution time is far less as compared otherwise, but the quality of the output image is partially encrypted. This proves that the authors' suggested method has a compromise between low computational velocity and decreased algorithmic density, which is suitable for application in real-time computation requiring fast computation methods. With reference to the control threshold, the proposed method provides a mechanism to balance both the security level and the procedure's execution speed in real-life applications.

Table 9. Comparison of Encryption Times: Proposed vs. Existing Selective Encryption Schemes

Schemes	**Encryption time (sec)**
Proposed work	0.8954
[13]	1.4074
[14]	1.4943
[15]	1.202

Table 9 presents quantitative results of computational time for the proposed selective encryption compared with different existing encryption methods. This comparison shows how the proposed scheme performs concerning security and speed that is essential when it comes to real time applications like video processing or, in the large-scale image encryption.

Proposed Scheme: The table probably demonstrates that the encryption time of the proposed method is much higher or at least comparable to the existing methods. This shows how effective the approach is especially when using selective encryption that applies

to areas of interest in an image or data set since less data is encrypted.

Existing Schemes: Some of the existing schemes [13-15] may employ encryption algorithm based on chaotic maps, ECC or other such methods. These schemes may take relatively longer time to encode due to encryption of large sections of the image or the whole image depending on the selective encryption of only areas of special interest. Therefore, faster encryption times in the proposed method suggests that the proposed method is more appropriate for real-time application, for example, in feed video transmission since it combines aspects of both speed and security. Existing schemes, while being significantly more secure than schemes described above, might be slower and more computationally intensive because of their full encryption strategies, or simply because their algorithms are not as efficient.

However, when applying the proposed selective image encryption method as described above, several weaknesses and threats are apparent. Firstly, the high sensitivity of the encryption method to secret keys shown by the significant differences of the encrypted images when the secret keys are slightly changed emphasizes that there might be an issue associated with the secret keys management. This same sensitivity makes it absolutely imperative that key management and protection are carried out with the utmost of care; should the secret key be somehow compromised or lost then all data encrypted is at risk of being fully revealed. Moreover, the partial encryption approach of encrypting some blocks of images depending on control threshold might be vulnerable to attacks on the non-encrypted image areas. One threat that we can derive from this attack model is called partial information disclosure, which means that an attacker may try to guess or reconstruct parts of the image within the partially encrypted sections with the help of cryptanalytic approaches. Furthermore, being able to vary the effectiveness of encryption at different threshold values as demonstrated in the histograms the memory may be exploitable through statistical analysis or pattern recognition attacks, in the event that the data encryption method is not randomized sufficiently at some partially obscured threshold values. Finally, the performance advancement of the method maintaining the balance of the encryption level and processing time are the performance metrics and the execution times that can be considered as the signs of potential side-channel attack in which variations in the processing time may contain information on the process of encryption or a key. In all generality, the selective encryption method is still a weak link that requires a thorough assessment and optimization to avert these risks and prevent future attacks.

Conclusion and Future Work

The idea of selective image encryption using Henon Map is designed by selecting blocks and then applying diffusion process to the 16 x 16 macro block randomly. The flexibility of the degree of encryption is easily controlled by changing the control threshold values which makes it easy to meet the need of the various applications of the encryption. Based on experimental tests it has been found that the computational time for image encryption when using a symmetric cipher is a function of the threshold control value and images properties. The findings also indicate that the time taken to encrypt, thus at least for the selective encryption methods on static visual images is greater than full encryption. The selective encryption method discussed in this paper, with the help of the Henon Map, is suitable for applications in which the necessary computation should be carried out as quickly as possible while achieving acceptable levels of protection. Future work will focus on extending this methodology to dynamic image data, such as video sequences, to evaluate its effectiveness in real-time streaming applications. Additionally, exploring the integration of other chaotic maps and enhancing the robustness of the encryption process against various types of cyber-attacks will be crucial. Further studies will also aim to optimize the balance between encryption efficiency and security, ensuring the method's applicability in diverse telemedicine and multimedia contexts.

Acknowledgments

This work is supported by VTU Belagavi, Karnataka and Deapartment of Electronics and Communication Research centre, Vidyavardhaka College of Engineering, Mysuru, Karnataka.

Conflict of Interest Statement

Authors declare that there is no conflict of interest for publication of this work.

References

1. Kirankumarhumse, K. Prabhavathi, R. Lakshmi, et al. Optimized Medical Image Encryption with Multiple Chaotic System Approaches. In 2nd IEEE International Conference on Networks, Multimedia and Information Technology, NMITCON 2024; IEEE, **2024**; pp 1–7.
2. P. Parikh, N. Patel, D. Patel, P. Modi, H. Kaur. Ciphering the Modern World: A Comprehensive Analysis of DES, AES, RSA and DHKE. Proceedings of the 18th INDIAcom; 2024 11th International Conference on Computing for Sustainable Global Development, INDIACom 2024. **2024**, pp 838–842.
3. Kiran, B.D. Parameshahcari, S. V. Sandeep, et al. Secure Image Transmission with Efficient Resource Constraints Using Multiple Chaotic Systems. In 2023 IEEE 3rd Mysore Sub Section International Conference, MysuruCon 2023; IEEE, **2023**; pp 1–5.
4. Kiran, D.S.S. Kumar, K.N. Bharath, et al. Optimized Encryption Technique for Securing E-Health Images. In International Conference on Computer Vision and Robotics; Springer Nature Singapore, Singapore, **2023**; pp 131–141.
5. M. Packirisamy, J.S. Muthu, P.M. Kumar. An adaptive-selective image encryption with JSMP map and square-wave shuffling. In Machine Learning and Cryptographic Solutions for Data Protection and Network Security; IGI Global, **2024**; pp 390–424.
6. Q. Natsheh, A. Sălăgean, D. Zhou, E. Edirisinghe. Automatic Selective Encryption of DICOM Images. *Appl. Sci.* **2023**, 13 (8), 4779.
7. S. Banerjee, T. Khan, J.H. Castellanos, G. Russello. Selective Encryption Framework for Securing Communication in Industrial Control Systems. In IEEE International Conference on Communications; IEEE, **2023**; Vol. 2023-May, pp 4125–4130.
8. C. Wei, G. Li. A selective image encryption scheme using LICC hyperchaotic system. *IET Image Process.* **2022**, 16 (12), 3342–3358.
9. Q. Cun, X. Tong, Z. Wang, M. Zhang. Selective image encryption method based on dynamic DNA coding and new chaotic map. *Optik* (Stuttg). **2021**, 243, 167286.
10. S.M. Darwish. A modified image selective encryption-compression technique based on 3D chaotic maps and arithmetic coding. *Multimed. Tools Appl.* **2019**, 78 (14), 19229–19252.

11. L.A. Salman, A.T. Hashim, A.M. Hasan. Selective Medical Image Encryption Using Polynomial-Based Secret Image Sharing and Chaotic Map. *Int. J. Saf. Secur. Eng.* **2022**, 12 (3), 357–369.
12. O. Berrak, A. Belmeguenai, S. Boumerdassi. An approach based on concatenation the areas of interest for selective image encryption. In 2020 10th International Symposium on Signal, Image, Video and Communications, ISIVC 2020; IEEE, **2021**; pp 1–6.
13. H.N. Noura, O. Salman, R. Couturier, A. Chehab. Efficient and secure selective cipher scheme for MIoT compressed images. *Ad Hoc Networks* **2022**, 135, 102928.
14. L.M. Jawad. A Novel Region of Interest for Selective Color Image Encryption Technique based on New Combination between GLCM Texture Features. In Proceedings - 2021 IEEE 4th National Computing Colleges Conference, NCCC 2021; IEEE, **2021**; pp 1–6.
15. C. Ye, S. Tan, Z. Wang, B. Shi, L. Shi. Hybridized Hierarchical Watermarking and Selective Encryption for Social Image Security. *Entropy* **2023**, 25 (7), 1031.
16. W. Alexan, Y.L. Chen, L.Y. Por, M. Gabr. Hyperchaotic Maps and the Single Neuron Model: A Novel Framework for Chaos-Based Image Encryption. *Symmetry* (Basel). **2023**, 15 (5), 1081.
17. H. Al-Najjar, N. Al-Rousan. Enhancing Image Security with Rossler Attractor-Based Encryption. In 2nd International Conference on Cyber Resilience, ICCR 2024; IEEE, **2024**; pp 1–7.
18. R. Ratan, A. Yadav. Security Analysis of Bit plane Level Image Encryption Schemes. *Def. Sci. J.* **2021**, 71 (2), 209–221.
19. V. Rathore, A.K. Pal. An image encryption scheme in bit plane content using Henon map based generated edge map. *Multimed. Tools Appl.* **2021**, 80 (14), 22275–22300.