International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Image Encryption Using Arnold Cat Map and Henon Chaotic Encryption

Navyansh Kothari[1], Padmanaban R[2]

[1,2]School of Computer Science and Engineering Vellore Institute of Technology Chennai, India

Abstract

The use of digital images in multimedia applications requires robust encryption techniques to protect sensitive visual information from unauthorized access. Traditional encryption methods like AES and RSA have limitations and vulnerabilities when applied to encrypting digital images, especially in scenarios with high computing demands. This abstract explores the fasci- nating world of image encryption, focusing on the utilization of the Arnold Cat Map and Henon Chaotic Encryption algorithms. The Arnold Cat Map, is renowned for its ability to produce intricate patterns with chaotic behavior. The Henon Chaotic Encryption algorithm, adds an additional layer of complexity to the encryption process. By using a nonlinear system of equations, this algorithm generates a series of pseudo random values. These values are then combined with the encrypted image, further enhancing its security. We also explore the advantages and limitations of these techniques, highlighting their potential in securing sensitive visual data in various domains, including military operations, medical imaging, and digital forensics. This abstract aims to inspire further research and development in this exciting field, contributing to the protection of digital information in an increasingly interconnected world.

Keywords: Chaos maps, Chaotic systems, Nonlinear dy- namical systems, Arnold cat map, Henon map, AES, RSA, Computational complexity, Pseudorandom properties, Ergod- icity, Non-periodicity, Digital image security, Unauthorized decryption.

1. INTRODUCTION

Image encryption is the process of encoding an image in such a way that only authorized parties can access it. Chaotic systems, which are a sub-type of nonlinear dynamical systems, have been widely used in image encryption algorithms due to their sensitive dependence on initial conditions and ability to generate pseudo-random sequences. Chaos maps, also known as chaotic maps or functions, are equations or rules that specify how a dynamic system evolves with time. These maps are used to generate chaotic sequences for confusion and diffusion in image encryption algorithms. In this project, the implementation of image encryption involves using various chaos maps, including the Arnold cat map and Henon map. These maps are utilized to encrypt the plaintext image, with the aim of breaking the redundancy and transforming the sta- tistical characteristics of the original image. The merits of the encryption algorithms are compared based on key sensitivity, adjacent pixel autocorrelation, and intensity histograms. The quality of image encryption can be assessed through various methods, including ciphertext image histogram analysis. A good encryption technique should generate a cipher image with a uniformly distributed intensity histogram, transforming the original image into a random and incomprehensible form. Additionally, the correlation between adjacent pixels in a specific direction, such as horizontal, vertical, or diagonal, can be

analyzed. A good encryption algorithm should parade a arbitrary correlation plot with no perceptible pattern. crucial sensitivity is another important metric for encryption performance. An ideal encryption algorithm should be extremely sensitive to the secret key, meaning that an insignificant change in the key should produce a fully different translated image. To test crucial perceptivity, the plain image is translated using the three enforced algorithms, and also decryption is tried with a slightly changed key. Traditional encryption mechanisms like AES and RSA have certain downsides and sins when it comes to cracking digital images, similar as high computational time and power conditions for large images. As a result, there is a need for better techniques for image encryption. Chaos-based algorithms offer a good combination of speed, high security complexity, and low computational overhead. These algorithms leverage the sensitive dependenceon initial parameters, pseudo random properties, ergodicity, and non-periodicity of chaotic systems to encrypt images ina way that increases the difficulty of unauthorized decryption. Overall, image encryption using chaos maps provides a meansof securing digital images by transforming their statisticalcharacteristics and increasing the randomness of the cipher text. The use of chaos-based encryption algorithms offers advantages in terms of security, computational efficiency, and resistance to unauthorized decryption attempts.

2. LITERATURE SURVEY

In this literature review[1] they introduced a novel secure communication system that combines traditional encryption methods with chaotic encryption mechanisms, resulting in significantly enhanced anti-attack capabilities as supported by analytical findings and experimental data. Additionally,a new approach to chaotic synchronization is proposed, en- suring rapid synchronization during transmission and main-taining high-security performance using a simple mixed dis- crete chaotic signal. In contrast to the conventional one-time- one-key design in cryptography, this work develops a one- time-one-algorithm design by integrating chaos theory with traditional encryption. This approach allows for the public disclosure of encryption techniques while keeping the keysas the sole repository of secrets. A general theory is provided

for creating clock keys, substitution boxes, permutation boxes,and operational sign functions for the one-time-one-algorithm scheme. Furthermore, a system is devised to manage the trade-off between encryption method security and speed.

Literature review[2] explores recent advancements in chaos-based image cryptosystems, particularly focusing on designsincorporating diffusion and substitution phases. It identifiesvulnerabilities in conventional architectures, where confusionand diffusion are segregated, leading to excessive operation rounds for a desired security level. To address this, a proposedmodification introduces diffusion effects within the substitu-tion phase through add-and-shift operations, aiming to enhanceencryption efficiency and resilience to attacks. Emphasizingthe importance of addressing flaws in existing systems, the review offers insights into improving security and operationaleffectiveness through design changes. Additionally, a novelimage encryption technique utilizing three chaotic maps is pre-sented, involving block-based shuffling and chaotic sequencesgenerated via logistic and cat maps. Experimental results demonstrate strong encryption, large key space, and sensitivityto secret key changes, with desirable characteristics such aslow correlation coefficients, high information entropy, andrandom-like distribution of grey values in encrypted images. In this paper[3] they discussed the utilization of chaoticmaps has demonstrated effectiveness in establishing imageencryption methods. Previous studies have presented variousfunctional architectures that incorporate diffusion and confu-sion processes, typically treated as

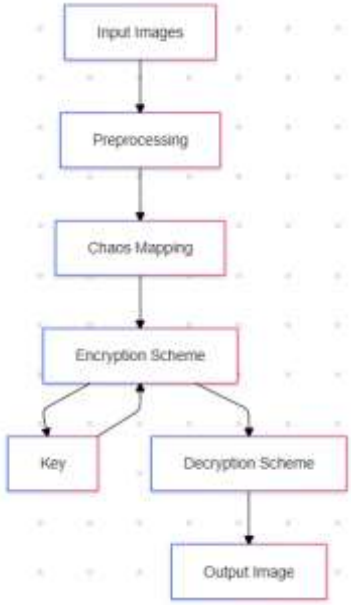
separate phases requiring pixel scanning. The proposed method utilizes fundamental operations like confusion and diffusion, employing a cascade of 3D standard and 3D cat maps. This process involves creating a diffusion template using a 3D standard map, ro-tating the image using the red and green plane, shuffling the color planes using a 3D cat map and standard map, and finally encrypting the image with an XOR operation. Computer simulations and theoretical analyses, including sta-tistical analysis and information entropy analysis, validate the algorithm's effectiveness, minimizing the risk of brute force attacks for decryption while ensuring practical image encryp-tion speed. Early developments in chaos-based encryption in the 1990s led to the implementation of a digital picture encryption technique combining chaotic systems, employing symmetric key cryptography for secure image encryption at a tolerable pace. The method combines a standard linked map with a one-dimensional chaotic map, demonstrating high- security encryption capabilities with a substantial key size. Additionally, recent literature explores advancements in chaos- based cryptographic algorithms, particularly in secure image encryption. A proposed scheme introduces chaotic logistic maps and dynamic modifications, utilizing an 80-bit external secret key to enhance security. Experimental results validate the approach as an efficient and secure method for real-time image encryption and transmission, showcasing its robustness through dynamic key alterations after encrypting each block of pixels.

This literature review[4] introduces a picture encryption tech-nique using three chaotic maps. It breaks the picture into 8x8 blocks, shuffles them using 2D chaotic maps, and encrypts with a one-dimensional Logistic map. Experimental findings confirm strong encryption, large key space, and sensitivity to key changes. Simulation analysis reveals low correlation coefficients, high information entropy, and a random-like dis- tribution of grey values in encrypted pictures.

This study[5] presents a method for image encryption using chaotic maps, merging diffusion and confusion processes for efficiency. It employs a cascade of 3D standard and 3D cat maps to create a diffusion template, rotate the image, shuffle color planes, and perform encryption via XOR operation. Sim-ulations and analyses confirm its effectiveness against brute force attacks, ensuring rapid and practical image encryption. In this paper[6], a digital picture encryption technique based on a combination of chaotic systems is implemented and presented. This study employs symmetric key cryptography as a chaotic cryptography approach. This approach, whose pace is tolerable for high degree security picture encryption, combines a standard linked map with a one-dimensional chaotic map. The security analysis and implementation of the suggested method are covered in depth. The suggested strategy and its implementation are deemed successful based on the experimental results obtained from a combination of chaotic maps. The benefits of huge key are demonstrated in this mixed application of chaotic maps.

The literature survey[7] explores recent developments in chaos-based cryptographic algorithms, focusing on their ap- plication in secure image encryption. The proposed image encryption scheme introduces a novel approach using chaotic logistic maps, an 80-bit external secret key, and dynamic modifications to enhance security. The initial conditions for logistic maps are derived from the secret key, and eight different operations are employed for pixel encryption based on the logistic map outcomes. The secret key is altered after encrypting each block of sixteen pixels, contributing to the scheme's robustness. Experimental and statistical analyses confirm the proposed approach as an efficient and secure method for real-time image encryption and transmission.

3. PROPOSED METHODOLOGY



The above proposal can be implemented in the following
way: Arnold cat map Arnold's Cat chaotic mapping of two dimensions can be used to change the position of the image's pixel without removing any information from it. The pixel image can be assumed by:
S= (x, y) — [x,y = 0, 1, 2 ... N -1]
A. The 2- D image of Arnold's cat chart can be written as
x)(y) = A *(x)(y) *(modn) 1 pq(pq 1) *(x)(y) *(modn) Where p and q are positive integers, the determinant(A) = 1.(x', y') isthe new position of the original pixel position(x, y), when Arnold's Cat Chart algorithm performed formerly.

```
import cv2
import numpy as np
def ArnoldCatTransform( img, num) rows, couloirs, ch = img.shape n = rows arnoldimg = np.zeros(( rows, couloirs, ch)) for x in range( 0, rows) for y in range( 0, couloirs) arnoldimg( x)( y) = img(( x y)  return arnoldimg def ArnoldCatEncryption( imageName, crucial) img = cv2.imread( imageName) for i in range( key) img = ArnoldCatTransform( img, i) cv2.imwrite( imageName.split( '. ')( 0) ' ArnoldcatEnc.png ', img) return img
```

Algorithm to encrypt an image of size m: Using this map we generate two random sequences savex1, savey1 and savex2, savey2 of size m2 where savexi and saveyi contain the x and y values generated from the function where each ith set has started from a different initial value of x andy.

```
x1 = -0.04
y1 = 0.2
for i in range(1, m2):
x1next = y1
y1next = -0.2*x1 + 2.75*y1 - y1**3savex1 = x1next
savey1 = y1nextx1 = x1next
y1 = y1next
```

Similar iterations are run for initial values x2 = 0.23 andy2 = -0.13 but saved to savex2 and savey2.

```
for i in range(0, m2):
```

h1[i] = 0 if savex1 < savex2 else 1h2[i] = 0 if savey2 < savey1 else 1
encryptedimage = bitwisexor(h1, h2, imagematrix)decryptedimage = bitwisexor(h1, h2, imagematrix)
h1 and h2 can be found by knowing the initial values x1, x2, y1,y2, which makes them the secret keys for this encryption.

A. Henon map:

It's a 2- D dynamic system. Two different chaotic sequences are generated by the Henon chaotic chart. These sequences are also applied to the row and column permutations of the original/ plain image. XOR models are used to produce pixel values prolixity by unimodal skew roof chart.
Hussain's negotiation box is used to substitute each pixel into a new arbitrary pixel in the last stage of the algorithm. Consider xi 1 = yi 1 1 × x2
yi 1 = xi. Where, the initialpointis(x0, y0) and are the original parameters. Each point(xn, yn) is counterplotted to a new point(xn 1, yn 1) through the Henon chart.

- **Algorithm for Henon map implementation::**

for i in range(m2):
x[i + 1] = y[i + 1] + 1 * x2y[i + 1] = x[i]
bit = 0 if x[i] <= 0.4 else 1
((Only the value of x is used. This is appended as rows of lists of 8-bit numbers, so that we can have a bitwise xor with the image).
Encryptedimage = bitwisexor(imagematrix,bitmatrix for R, G, B values in each pixel of imagematrix)
decryptedimage = bitwisexor(imagematrix,bitmatrix for R, G, B values in each pixel of imagematrix)
The bit matrix can be generated by knowing the initial values applied in the Henon map, making them the secret keys in this operation.
Proposal including modified paper implementation: Arnold-Henon composite map
Based on the paper "A Chaotic Cryptosystem for Images Based on Henon and Arnold Cat Map" by Ali Soleymani, Md Jan Nordin, and Elankovan Sundararajan, a modified version of the scheme proposed in the paper has been implemented as part of this project.
Algorithm:
Use Henon map to generate two secret images A and B based on the secret key (i.e initial value of the Henon map) where the x values make up A and y values generated makeup B and this is done m2 times, so that it can correspond to each pixel in the original image using:
pixA.append(abs(math.floor(xN*paramlambda)) pixB.append(abs(math.floor(yN*paramgamma))where paramlambda=math.floor(x*m*5000) paramgamma=math.floor(y*m*5000)
paramlambda and paramgamma can be found using x y,or the initial values, and therefore are not part of the secret key, as they can be derived from it. Simultaneously, we record values in arrays Pvalues and Qvalues as follows: Pval-ues.append(abs(math.floor(savethexmat[i]*math.pow(10,14)))
where alpha=26010 beta=15080
Here, 26010 and 15080 were randomly chosen because they were the dates for Republic Day and Independence Day. Thus,alpha and beta too come under the secret key. Runthe Arnold- Cat map m/3 times on the original image with the matrix multiplication algorithm mentioned earlier in the paper, but with different values of P and Q based on the iterator i, with the values being taken from the lists Perform a bitwise XOR ofsecret images A and B, and then run the Arnold Cat algorithm on the xor-ed imaged 5m/7 times.

Note: m/3 and 5m/7 are values chosen to be part of the alogirthm as the algorithm was found to be most robust for these values. As such, these can be found through knowing the image size and are public knowledge in terms of the values of m/3 and 5m/7 and do not form part of the secret key. Performa bitwise XOR of the final images obtained in the previous step and the step before it. This is the encrypted image.

4. EVALUATION METRICS

A. Histogram Analysis

To measure the effectiveness and the security of the encryp-tion algorithms we have used three analyses-namely, Intensityhistogram analysis, Adjacent pixel autocorrelation test and thekey sensitivity tests.

The ciphertext image histogram analysis is one of the most straight-forward methods of illustrating the image encryption quality. A good image encryption method tends to encrypt a plaintext image to a random incomprehensible form. Thus, a good image encryption technique generates a cipher image thathas a uniformly distributed intensity histogram.

Figures show the histograms for the various encryption schemes discussed. The Arnold cat encryption system has an identical intensity histogram to the original image. This isbecause the Arnold Cat method essentially just shuffles the pixels but does not change any pixel values.

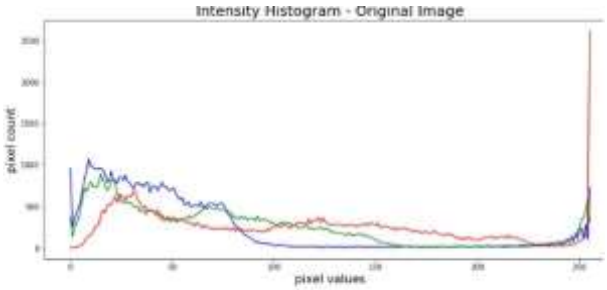


Figure 2: The intensity histogram for original image

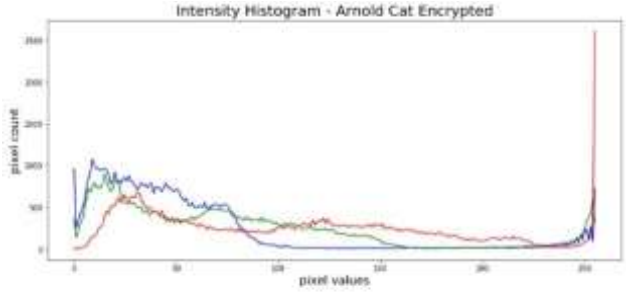


Figure 3: The intensity histogram for Arnold cat map

The intensity histogram for the Arnold cat map representsthe distribution of pixel intensity values in an image afterencryption using the Arnold cat map algorithm. It illustrates the frequency of occurrence of different intensity levels within the encrypted image. In the context of the Arnold cat map, a good encryption technique would result in a uniformly distributed intensity histogram, indicating that the encrypted image appears random and incomprehensible.

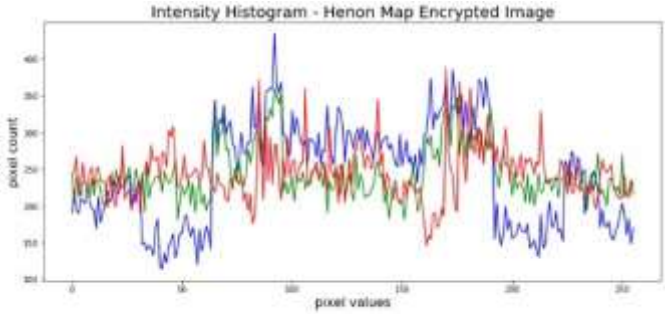


Figure 4: The intensity histogram for Henon map

The intensity histogram for the Henon map represents the distribution of pixel intensity values in an image afterencryption using the Henon map algorithm. Henon map isa chaotic system employed for image encryption. A desirable outcome for the intensity histogram of the Henon map would also exhibit a uniformly distributed pattern, suggesting thatthe encrypted image maintains a balanced distribution of pixelintensities, thereby enhancing security.

B. Key Sensitivity

An ideal image encryption algorithm should be sensitive with respect to the secret key i.e., a slight change in the key should produce a completely different encrypted image. To test the key sensitivity, we encrypt the plain image with three algorithms. We then try decrypting them with a slightly changed key. The figure shows us that for the Arnold cat algorithm, while a change in key does not decrypt the image correctly, the resultant image has discernible features that appear like the plain image. This is because on applying a certain number of Arnold Cat transformations, the initial image can be easily recovered. By applying brute force,it becomes possible for a person without a key to decrypt an image encrypted using Arnold cat maps. This proves that the Arnold cat algorithm, owing to its periodicity, is unsafe for practical use.Arnold cat chaotic encryption have lower tolerance to key perturbations compared to Henon chaotic encryption. Slight changes in the encryption key could result in significantly different encrypted outputs in Arnold cat encryption. While this high sensitivity enhances security against brute-force attacks, it also requires carefulmanagement of encryption keys to ensure accurate decryption.

Figure 12: Key sensitivity for Arnold Map

The adjacent pixel autocorrelation for the original image refers to the statistical relationship between the intensity valuesof neighboring pixels in the unencrypted (original) image. It measures how closely the intensity values of adjacent pixels are related to each other. In an unencrypted image, there may be correlations between adjacent pixel intensities dueto patterns or structures present in the image. On the other hand, the adjacent pixel autocorrelation for the encrypted image assesses the statistical relationship between the intensityvalues of neighboring pixels in the encrypted image. A good encryption algorithm aims to break these correlations, resultingin a randomized pattern of pixel intensities. Therefore, in an effectively encrypted image, the autocorrelation between adjacent pixels would ideally be minimized or

appear random,indicating successful encryption and enhancing security byreducing the predictability of the image content.

On the other hand, Henon chaotic encryption may exhibit relatively higher tolerance to key perturbations.Small variations in the encryption key does not resultin drastic changes to the encrypted output. While this may offer some flexibility in key management, it could potentially introduce vulnerabilities if the systemrelies too heavily on a narrow range of key values.

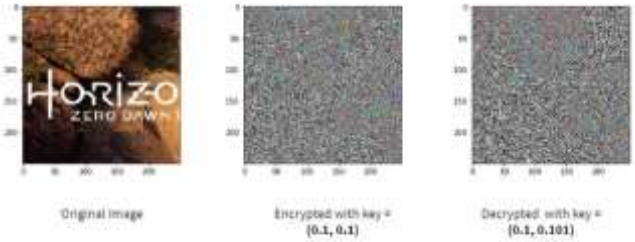
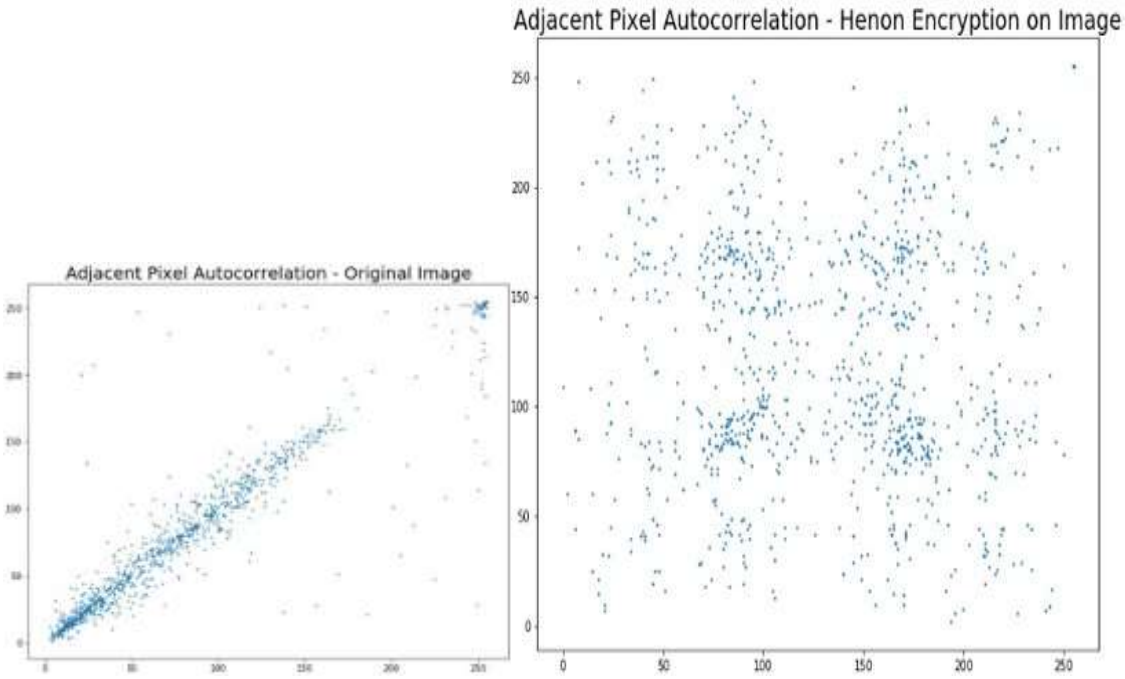


Figure 13: Key sensitivity for Henon Map

C. Adjacent Pixel Correlation Analysis



The adjacent pixel autocorrelation for the Arnold map evaluates the statistical connection between neighboring pixel intensities in an image encrypted with the Arnold cat map algorithm. This assessment measures the disruption of cor- relations between adjacent pixels introduced by the chaotic mixing and diffusion of the Arnold cat map. In an effectively encrypted image, such correlations are minimized or appear randomly, showing successful encryption and increased security through reduced predictability in the image content.

The adjacent pixel autocorrelation for the Henon mapevaluates the statistical connection between nearby pixel intensities in an image encrypted using the Henon map algorithm. It examines how closely these intensities are related in the encrypted image. The Henon map introduces chaos to disrupt any correlations

between neighboring pixel intensities in the original image. Thus, in a properly encrypted image using the Henon map, the adjacent pixel autocorrelation should ideally be minimized or appear random, enhancing security by reducing predictability in the image content.

D. Security Strength

Arnold cat chaotic encryption relies on the mixing proper- ties of the chaotic map, while Henon chaotic encryption relies on the sensitivity to initial conditions and parameters. The security strength of each method depends on factors such as key size, the quality of randomness, and the implementation details.

E. Resource Requirements

Henon chaotic require more computational resources or memory compared to Arnold cat chaotic encryption due to the complexity of the Henon map equations. Arnold cat chaotic encryption is lightweight in terms of resource requirements but it is slower due to the iterative nature of the encryption process.

F. Robustness to Attacks

Both methods may have vulnerabilities to certain types of attacks, such as statistical attacks or chosen-plaintext attacks. The robustness of each method depends on factors such as the specific implementation, key management practices, and the ability to withstand known cryptographic attacks.

G. Implementation Complexity

Arnold cat chaotic encryption may involve more complex implementation due to the iterative nature of the encryption process and the need for precise control over initial conditions.

Henon chaotic encryption, while simpler in terms of mathe- matical operations, may still require careful implementation to ensure security and efficiency.

5. CONCLUSION

The document on Image encryption using Chaos-Maps concludes by highlighting the potential of Chaos-based image encryption as a robust alternative to traditional methods like AES and RSA. It emphasizes the improved security, speed, and complexity of advantages offered by Chaos-based en- cryption techniques. The study also acknowledges the chal- lenges that need to be addressed, such as selecting suitable chaotic maps, optimizing control parameters, and enhancing resistance to various attacks. Overall, Chaos-based image encryption shows promise in providing a balance between security and efficiency, making it a valuable approach for securing digital images. The convergence of chaotic theory and cryptography has spurred advancements in chaos-based image cryptosystems, with a particular focus on addressing the challenges unique to image encryption. Recent literature underscores the vulnerability of conventional architectures that rely solely on separate confusion and diffusion stages, high- lighting the need for enhanced security measures. In response, proposed modifications introduce diffusion effects within the substitution stage, aiming to bolster resistance against attacks while improving encryption efficiency by reducing operation rounds. The significance of addressing weaknesses in existing systems is paramount, as emphasized by the literature survey. By integrating chaotic dynamics into encryption algorithms, researchers aim to create robust systems capable of securing digital images against unauthorized access. The exploration of encryption techniques grounded in chaotic maps reflects a growing recognition of the complexities involved in image encryption, distinct from traditional text encryption methods. Furthermore, the emphasis on encryption quality assessment, demonstrated through ciphertext image histogram analysis and correlation analysis between adjacent pixels, underscores the importance of evaluating encryption techniques beyond theo- retical constructs. A good encryption method should transform plaintext images into random, incomprehensible forms while breaking

information redundancy, as indicated by uniformly distributed intensity histograms and random correlation plots. Ultimately, the choice between Arnold cat chaotic encryption and Henon chaotic encryption should be based on a thorough analysis of factors such as security requirements, resource constraints, and the specific characteristics of the data and application environment.

In summary, the literature survey provides valuable insights into recent developments in chaos-based image cryptosystems,highlighting the ongoing efforts to enhance security and op- erational efficiency. By addressing weaknesses and proposing innovative modifications, researchers aim to pave the way for more robust and reliable image encryption techniques in the realm of information security.

REFERENCES

1. L. Min, P. Fei, Q. Shuisheng and C. Yanfeng, ”Implementation of a new chaotic encryption system and synchronization,” in Journal of Systems Engineering and Electronics, vol. 17, no. 1, pp. 43-47, March 2006, doi: 10.1016/S1004-4132(06)60008-X.
2. G. Zhao, G. Chen, J. Fang and G. Xu, ”Block cipher design: Generalized single-use-algorithm based on chaos,” in Tsinghua Science and Technology, vol. 16, no. 2, pp. 194-206, April 2011, doi: 10.1016/S1007-0214(11)70030-X.
3. Wong, KW. (2009). Image Encryption Using Chaotic Maps. In: Kocarev, L., Galias, Z., Lian, S. (eds) Intelligent Computing Based on Chaos. Studies in Computational Intelligence, vol 184. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-95972-416
4. Ahmad, Musheer Alam, M.. (2010). A New Algorithm of Encryption and Decryption of Images Using Chaotic Mapping. International Journal on Computer Science and Engineering.
5. ”New Approach for Fast Color Image Encryption Using Chaotic Map” written by Kamlesh Gupta, Sanjay Silakari, published by Journal of Information Security, Vol.2 No.4, 2011
6. N.K. Pareek, Vinod Patidar, K.K. Sud, Image encryption using chaotic logistic map, Image and Vision Computing, Volume 24, Issue 9, 2006, Pages 926-934, ISSN 0262-8856, https://doi.org/10.1016/j.imavis.2006.02.021.
7. S. Behnia, A. Akhshani, H. Mahmodi, A. Akha- van, A novel algorithm for image encryption based on mixture of chaotic maps, Chaos, Solitons Fractals, Vol- ume 35, Issue 2, 2008, Pages 408-419, ISSN 0960-0779, https://doi.org/10.1016/j.chaos.2006